Australian Government
Australian Transport Safety Bureau

Runaway and derailment of TasRail freight train no. 604

Devonport, Tasmania, on 21 September 2018

ATSB Transport Safety Report
Rail Occurrence Investigation (Systemic)
RO-2018-014
Final – 18 November 2022

Cover photo: Tasmania Police

Released in accordance with section 25 of the *Transport Safety Investigation Act 2003*

Publishing information

Published by: Australian Transport Safety Bureau
Postal address: PO Box 967, Civic Square ACT 2608
Office: 12 Moore Street Canberra, ACT 2601
Telephone: 1800 020 616, from overseas +61 2 6257 2463
Accident and incident notification: 1800 011 034 (24 hours)
Email: atsbinfo@atsb.gov.au
Website: www.atsb.gov.au

Addendum

Page	Change	Date

Executive summary

What happened

On the morning of 21 September 2018, a train driver was using remote control equipment (RCE) to control and position TasRail train no. 604 so that it could be loaded with cement powder at a siding in Railton, Tasmania. The driver was outside the train and no-one else was on board.

Having overshot the intended location to load the last 2 wagons, the driver attempted to use the RCE transmitter to reverse the train. However, the train did not respond to their commands. The driver attempted procedures to recover the RCE from known failure modes in order to restore control, however these were unsuccessful.

As the driver began to walk towards the locomotive to attempt to reset equipment, they noticed the train start to move. They attempted several methods to command the train to stop by using the RCE transmitter, but these were unsuccessful. Instead, the train, which was on a downhill grade, continued to roll away, leaving the siding and entering the main line toward Devonport.

The driver notified TasRail network control of the runaway, and they in turn notified emergency services. Network control also organised for the points at the entrance to Devonport Yard to be set to divert the train from the main line, which continued past this location, into a dead-end siding within the yard.

The train travelled through 10 active and 3 passive public level crossings, beneath a highway overpass, and through 5 sets of points, mostly at speeds greater than the maximum track speed. It reached a maximum recorded speed of 87.5 km/h.

About 23 minutes after the train rolled away from Railton, it collided with a concrete footing and surrounding fences at the end of the silo siding in Devonport Yard. The derailment caused significant damage to the train's locomotive and 7 wagons, as well as damage to the end of the siding and fences. Fence debris struck 2 pedestrians who had been walking in the area, resulting in minor injuries to both.

What the ATSB found

Key parameters related to the remote control equipment (RCE) were not recorded. This hindered internal and external safety investigations of events involving use of the RCE, both for this accident and previous events. However, the ATSB was able to determine that the RCE entered a spurious fault condition (involving the application of emergency braking) that was almost certainly associated with rapid movement of the RCE transmitter's direction controller by the driver. This likely initiated an unintended interaction between a safety feature (the dual direction fault interlock) and braking systems on the locomotive, which resulted in an emergency-level brake application.

At about this time, the RCE ceased to respond to driver commands. Instead, the initial brake application was released, then 2 further emergency brake applications and releases occurred. These did not replicate any documented fault condition behaviour for the RCE. A short time later, while still unresponsive to driver commands and with the train's brakes still released, the train started to roll away.

When a driver was operating the train from outside the train (such as during loading and unloading), there was no way for them to stop the train if the RCE ceased to respond. Also, the TasRail cement loading facility at Railton had a downhill grade to the main line, and no devices to protect against runaway.

The RCE receiver was designed to apply the train's brakes when it was outside of radio communication range with the transmitter, but this did not occur when the train rolled away from Railton. Instead, the train proceeded to roll away with the brakes remaining released until it derailed in Devonport Yard.

When network control was notified of the runaway, TasRail staff and emergency services conducted a prompt and effective response. This included routing the train away from the main line into the yard and protecting some level crossings; actions that minimised the risk exposure of the public. However, the successful response on this occasion was not assured, as TasRail's processes for responding to emergency situations fundamentally relied on the experience and knowledge of NCOs and did not include the provision of procedures, tools and checklists detailed enough to support the effective management of specific types of incidents that require a time-critical response.

The ATSB examined a range of topics associated with the development of the RCE, and its use more broadly. At the time of the runaway, TasRail were using the third generation of RCE developed and manufactured by Air Digital Engineering (ADE) to remotely operate the cement train. The generation 3 RCE had been commissioned for use in February 2018 and incorporated several changes from the previous generation used by TasRail. However, the generation 3 RCE had several safety-related design and integration problems, including the potential for unintentional activation-and-release of emergency braking on the locomotive and opposition to externally-initiated emergency brake applications. These issues existed at the time of the accident but had not been identified during the testing and commissioning processes.

The RCE was used as the primary driver control interface to control the train, both when loading/unloading with the driver outside and during transit when the driver was either in the locomotive or the driver's van. As such, the function that the RCE performed was safety critical. However, although ADE had safety as a design objective and safety elements were included in the RCE, systems safety assurance activities appropriate to its application were not conducted.

TasRail had operated the cement train service successfully using previous generations of the RCE for about 19 years without any accidents attributable to the RCE, which likely contributed to a high level of confidence in the RCE and overall operation. Nevertheless, the development and integration of new equipment is not solely the responsibility of the equipment manufacturer; the organisation using the equipment also has a duty to ensure it is safe. In this case, TasRail commissioned the manufacture of the new equipment without fully engaging with the development process or understanding the extent of design changes since the previous generation of RCE, identifying and imposing safety requirements, or verifying that the overall system met a specified level of safety.

The ATSB also found that there were problems associated with TasRail's management of change. Most activities that were required by TasRail's procedures for a significant change were not performed during the project to develop and implement the generation 3 RCE. Furthermore, the change management process, while detailed, had limited capability to assure that activities, approvals, and documentation that were identified as being required were completed. The process also had limited capability to reliably determine whether the change being considered had the potential to impact safety or identify what safety assurance activities were needed to manage the change.

In addition, there were broader safety issues identified relating to TasRail's remotely-controlled train operations, separate to the implementation or use of the generation 3 RCE. TasRail had not identified or fully assessed the safety implications of remotely-controlled train operations or those of its specific implementation. TasRail also did not have a reliable process to systematically identify, track and analyse reported faults on its remotely-controlled train or to identify their potential safety implications.

The ATSB also identified that, at the time, there was limited practical guidance specifically for the Australian rail industry for the application of system safety assurance processes to the development of complex and safety-critical rail systems. Although standards, legislative requirements, and guidance for rail safety were recognised and applied in Australia, they were of limited value in the development and operation of complex systems.

There was also no explicit regulatory requirement for developers of rail equipment to demonstrate an objective evaluation of design safety or apply system safety principles during development. If a rolling stock operator or equipment developer intended to apply system safety principles, there were numerous challenges in attaining justified confidence in its success, which were difficult even for experts to overcome. Overall, the standards and guidance for system safety available at the time of the runaway were too abstract, complex, costly and/or impractical for widespread recognition and acceptance by the Australian rail industry.

Separately, there is a requirement for rolling stock operators to notify ONRSR when they intend to make certain changes. A change to a safety critical component, such as the RCE, should be considered the type of change which should be notifiable to ONRSR, so that regulatory oversight may occur. However, TasRail did not submit a notification of change for the generation 3 RCE and this was likely because an accepted view had formed within TasRail that it was 'like-for-like' replacement and therefore minimal change was occurring.

Guidance material prepared by ONRSR relating to the regulatory requirements for notifying change included limited detail about the extent or type of changes that necessitated a notification. One category that was identified as requiring notification was 'a safety critical element of rolling stock'. However, the guidance did not provide an interpretation of 'safety critical' or the applicability of the requirement to equipment that may not be inherently part of rolling stock (such as RCE). In this case, a notification of change had not been provided to ONRSR, but the reasons for this were not found to be related to the interpretation of the regulation.

What has been done as a result

Following the accident, TasRail immediately suspended remotely-controlled train operations. In November 2020, TasRail completed installation of a catch point at the western end of the Railton siding to prevent runaway rail vehicles from entering the main line. TasRail also:

- extensively revised its processes and guidance on change management, project management, engineering design
- enhanced processes for fault tracking and analysis
- implemented checklists to help ensure consistent and sound decisions during time-critical emergency responses.

ADE advised that it would re-evaluate the generation 3 remote control equipment under system safety design principles if it were to be used for future operations.

ONRSR advised that it planned to provide additional guidance about interpreting the conditions that describe when a notification of change to ONRSR would be required.

Other safety actions have also been taken that help address safety issues identified by the ATSB (although were not initiated as a direct result of this accident):

- In November 2018, the Rail Industry Safety and Standards Board (RISSB) finalised Australian Standard (AS) 7472 (*Railway operations - management of change*), to assist rail transport operators in fulfilling change management responsibilities. (This standard was in development prior to the accident.)
- ONRSR published a safety message in March 2019 titled *Importance of a System Engineering Approach* and 2 related fact sheets in 2020 that emphasised the need for a systems engineering approach in rail projects and drew attention to the relevant standards. The safety message stated that rail transport operators 'should demonstrate that they use appropriate systems engineering processes and safety assurance processes… in their design and procurement approach.'
- In 2020, RISSB issued standard AS 7473 (*Complex system integration in railways*) to support a systems engineering approach in Australian rail projects.

- In 2021, RISSB issued standard AS 7474 (*Rail industry – System safety)* to 'provide a clear standard for management of System Safety that addresses Australian legislative requirements and is readily scalable for the scope of rail projects undertaken within Australia.'

In addition to providing an overview of the relevant methods, AS 7473 and AS 7474 referred to other more detailed systems and safety engineering standards to enhance their visibility and application across the Australian rail industry.

Safety message

Rolling stock operators and equipment developers both have duties to ensure the design and modification of rolling stock and other equipment is safe for its intended use. This accident reinforces the need for such organisations to identify what systems are performing safety-critical functions and manage the risks of systems failure by ensuring the system has appropriate levels of reliability and/or by using secondary safety components that can override a failed system. This is especially true of complex systems such as those that implement software, due to the potential for these systems to fail in ways that are hard to predict.

Systems for the management of change need to reliably assure the determination of whether a change had the potential to impact safety and identify the need for relevant safety assurance activities. When a new system is implemented, or changes occur to a system, effective safety management needs to be a joint effort between the operator and the developer in order to effectively identify safety hazards and ensure that associated risks are managed. Operator involvement at this stage is important to fully account for the safety implications of the broader system.

Overall, it is important to ensure that systems have a compelling argument for their safety. Developing such an argument is not a simple task but there are numerous standards and guidelines available for a range of applications, including (more recently) specifically for the Australian rail industry. The ATSB strongly advises rolling stock operators and developers of rail systems to apply system safety methodologies so that they can have a high level of confidence in the overall safety of the system. The ATSB additionally encourages the continuing development of guidelines and standards to enhance the accessibility and practical application of system safety principles for all rail operations.

In addition, this investigation has also highlighted that rolling stock operators should ensure that event recorders are recording sufficient parameters for optimal outcomes of safety investigations, including those conducted by the operator.

Contents

The occurrence

Overview

TasRail operated train services between Railton and Devonport, Tasmania, for the purpose of transporting cement powder. The trains were operated by a single driver using remote control equipment (RCE).[1] The trains consisted of a TR class locomotive, cement wagons and a driver's van.

When a train was being loaded with cement at the Railton loading facility, the driver was outside the train and no-one else was on board. The driver operated both the RCE and the loading equipment to transfer the cement powder from silos via chutes into the train's wagons.

At 0846[2] on 21 September 2018, train no. 604 was being loaded. While the train driver was attempting to manoeuvre the last 2 wagons into position for loading, the train did not respond to remote control commands from the driver. The train (which was on a downhill grade) then rolled away from the facility without any train crew on board and in an uncontrollable state. The train driver informed the network control officer (NCO) about the runaway train, and then arrangements were made for it to be rerouted away from sensitive infrastructure.

The train travelled for about 20 km before reaching a dead-end siding in Devonport at 0909. The train collided with the end of the dead-end siding, and travelled in a derailed state for about 60 m into a public area.

Operations before the occurrence event

At 0130 on 21 September 2018, the driver signed on at Devonport Yard to work the service between Devonport and the Railton cement loading facility, taking over from another driver who had worked the preceding shift. The drivers performed a handover at the cement silos at Devonport where train no. 512[3] was being unloaded, with the previous driver advising that there were no faults or issues with the train or the RCE.

At 0220, the driver departed with the empty train from Devonport for Railton, where the 16 wagons were to be loaded. The train returned to Devonport to unload, before returning to Railton at 0740 to load again. During these cycles between Devonport and Railton, the RCE and train continued to perform as expected, with no faults or issues identified.

On arrival at Railton, the driver alighted from the train in preparation for checking the wagon doors prior to loading the train (now train no. 604). The Railton cement siding was located on the southern side of the main line between Devonport and Railton Yard. The loading facility (consisting of 2 cement powder silos) was situated on the siding (Figure 1). From the loading facility, the track had a downhill grade of 1 in 139[4] westward towards Devonport. Access to the main line was through a set of trailable electric points.

---

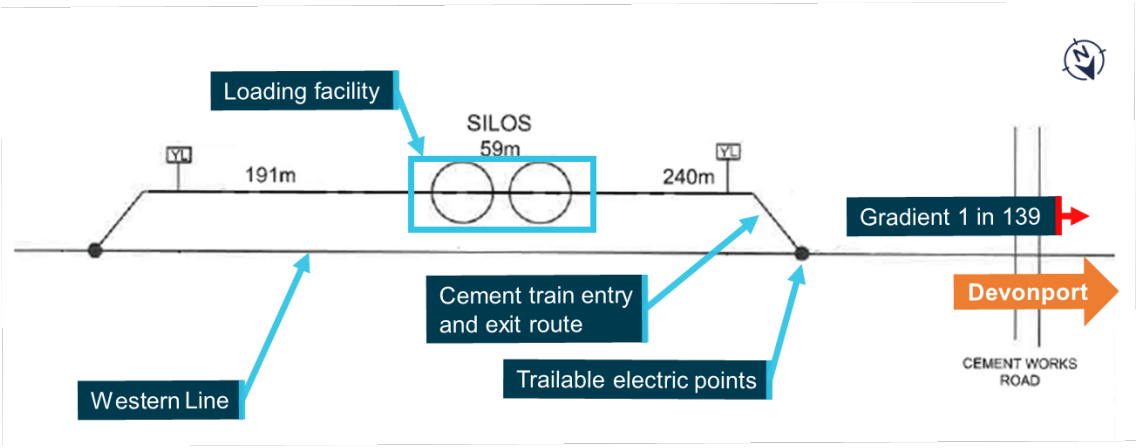
1 RCE was always used while operating the cement train, including when travelling on the main line and when loading and unloading.

2 All time references in this report are in local time (Eastern Standard Time).

3 Each train service on the TasRail network was allocated a unique identifying number. For the cement train, this changed sequentially at Railton and Devonport. Even numbered trains operated from Railton to Devonport, odd numbered trains operated from Devonport to Railton.

4 That is, 1 m drop in elevation for every 139 m travelled.

Figure 1: Railton cement siding and loading facility



Source: TasRail, modified by the ATSB

Loading train no. 604

At about 0746, after checking the bottom discharge doors on the wagons as the train passed through the loading facility towards Railton Yard, the driver aligned wagons 1 and 2 under the silos in preparation for loading. As the loading process was designed to be a single person operation, the driver then entered the loading facility and proceeded to the upper level where the loading control panel was positioned (see *Train loading process*).

The driver removed the key from the RCE transmitter and placed it into the loading control panel to allow operation of the panel's loading controls.[5] The driver then commenced loading of the first 2 wagons with cement powder.

Once the 2 wagons were full, the driver removed the transmitter key from the loading control panel and placed it back in the RCE transmitter, allowing driver commands to be sent to the RCE receiver on the locomotive. The driver then moved the train forward towards Devonport using the transmitter, aligning the next pair of wagons for loading. This process continued for the first 14 wagons (that is, the first 7 placements).

At about 0841, the driver removed the transmitter key from the loading control panel and placed it into the RCE transmitter to facilitate the next train movement forward to load the final 2 wagons. Using the transmitter, the driver released the automatic (train) brake, placed the direction controller in forward, released the independent (locomotive) brake, and applied light traction power. As the train came to a stop, the driver noticed that they had misjudged the wagon alignment, overshooting the stopping mark[6] by about 20 cm.

Remote control equipment failure

The driver recalled that, after the train came to a stop, they requested the direction to change (via the RCE transmitter) in preparation to reverse the train. The data recorded on the locomotive showed that the direction went immediately from forward to reverse without registering in neutral.

The driver informed the ATSB that, after releasing the train's brakes, they applied traction power to facilitate the rearward realignment of the wagons. After about 1 minute, allowing for the train's brakes to settle and traction power to take effect, the driver noticed that the train was still not moving. The driver stated that the RCE transmitter display screen was showing the text 'Connecting 9863 v1.4', instead of the usual system status information.

---

5 For more detail about the transmitter and other components of the RCE, see *Remote control equipment*.

6 The stopping mark was a welded indicator on a handrail near the driver's position in the loading facility, used to visually align the wagons when they were being loaded.

On observing the displayed message, the driver believed that the RCE had a communications failure,[7] so they configured the RCE transmitter controls for a reset (direction in neutral, throttle idle, independent brake fully applied, and automatic brake set) and pressed the train set button to reset the fault. The displayed message did not clear as it normally would.

Given the lack of response, the driver then believed that the RCE was experiencing a control fault.[8] They reported following the procedure to reset the control fault mode, which was to:

- retain the transmitter configuration as described above
- turn the transmitter's key switch off, wait about 10 seconds
- turn the transmitter key switch on again and press the train set button to return to 'run' mode.

The displayed message immediately reappeared on the transmitter display screen, so the driver repeated the process. Immediately after the second attempt at a control fault mode reset, the same message reappeared, so the driver determined a 'cold start' reset would be required to clear the fault. This required the driver to proceed to the rear of the locomotive (14 wagons away) to disconnect and reconnect the multiple unit cable[9] between the RCE receiver and the locomotive.

The driver informed the ATSB that the transmitter display screen continued to display the message 'Connecting 9863 v1.4' throughout the initial occurrence sequence. This indicated that the driver's RCE transmitter did not have a communication connection to the RCE receiver on the locomotive.

The runaway

At 0846:42, just as the driver had started to walk along the loading platform (while carrying the RCE transmitter) to perform an RCE reset at the locomotive, they noticed the train start to move forward. As the independent (locomotive) brake was still applied on the RCE transmitter, the driver thought that the train was momentarily 'bunching' coupler slack[10] on the downhill grade against the stationary locomotive.

The driver quickly realised that the train was moving past the expected extent of a bunch movement and they applied a full-service automatic (train) brake application on the RCE transmitter. When that did not work, they turned off the transmitter key switch to cause a communication failed mode automatic brake application. When the train still did not respond, the driver tilted the RCE transmitter[11] and then removed the battery as further attempts to command a brake application, which were also ineffective.[12] The driver also stated that they thought they had tried to use the 'emergency stop' switch on the RCE transmitter but did not recall when in the sequence this occurred.

The driver observed the driver's van at the rear of the train exit the Railton loading facility in the direction of Devonport. Believing that the RCE's vigilance function[13] would automatically apply the brakes, the driver crossed the loading platform bridge and walked down the stairs to observe the train's stopping position. The train continued to roll out of the cement siding and onto the main line

---

7 Communication failed mode: a fault mode that occurred when the RCE detected interrupted messages between the transmitter and receiver and was shown to the driver on the transmitter as 'COMF'. On entry into this mode, the RCE receiver was designed to command the removal of traction power and apply the train's brakes.

8 Control fault mode: a fault mode that occurred when a command from the RCE failed to enact correctly and was shown to the driver on the transmitter as 'CNF'. On entry into this mode, the RCE receiver was designed to command the removal of traction power and apply the train's brakes.

9 The action of disconnecting the multiple unit cable resulted in power loss to the RCE receiver, effectively turning it off.

10 That is, the train was entering a compressive state.

11 The RCE transmitter (when switched on) was designed to command a brake application if it was tilted at an angle of 50° or more past its normal upright orientation for 10 seconds. This was called the tilt function.

12 Removing the RCE transmitter battery (when switched on) would normally result in a brake application when the RCE would enter communication failed mode.

13 Vigilance function: to protect against driver incapacitation; if the driver did not acknowledge a periodic vigilance alarm, the RCE transmitter was designed to command the RCE receiver to apply a full-service brake application.

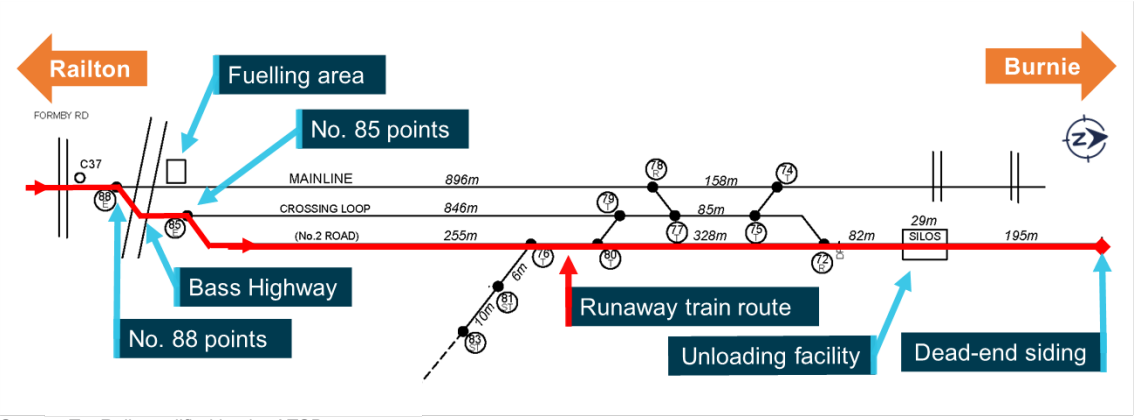
out of the driver's view. With no further method to stop the train available, the driver immediately rang the network control centre to report the runaway train.

Emergency response

At 0848:05, the network control officer (NCO) answered the driver's phone call and was advised that there was a runaway train. The NCO immediately checked the section of track from Railton to Devonport was clear and discussed with the driver where the train was likely to stop. It was determined that this could be prior to Devonport at Horsehead Creek, due to a rising grade and 40 km/h curves. In a scenario where the train continued to roll past Horsehead Creek, background conversations of other TasRail staff in attendance determined that the best course of action was to set the points to divert the runaway train into Devonport Yard, away from the main line and several level crossings. There it would derail at a dead-end siding, away from the township.

To facilitate the switch in points, the general manager freight services (who had been alerted to the runaway and was able to assist) contacted the shunter based at Devonport at 0852 and instructed them to set the points (no. 85 and no. 88) for no. 2 road Devonport (silo siding) (Figure 2). When the shunter advised this had been done, the general manager instructed the shunter to warn local businesses near the yard to evacuate.

Figure 2: Devonport Yard showing the route taken by the train to the dead-end siding



Source: TasRail, modified by the ATSB.

At 0853:52, 1 minute after the phone call with the driver concluded, the NCO contacted emergency services. The NCO advised Tasmania Police of the runaway event and the location of major level crossings between Spreyton and Devonport that would require police protection, with derailment now deemed likely to occur at the end of Devonport Yard.

The TasRail rolling stock asset manager had been alerted to the runaway. They logged into a computer in a room near to but separate from the network control centre to view the train's GPS speed and location information to allow monitoring of the train in real time. They relayed this information verbally to the network access manager, who was present in the network control centre at the time the runaway train was reported by the driver.

At 0858:41, the network access manager took over from the NCO communicating with the police to streamline the relay of messages. Over the next 11 minutes, the network access manager liaised with emergency services to deal with the emergency, including:

- providing regular GPS train speed and location updates
- advising likely derailment points between Latrobe and the entry to Devonport Yard
- discussing the possibility of a derailment at no. 88 points near the Bass Highway causing a bridge pylon strike
- requesting fire services and ambulances to attend Devonport Yard
- advising the final stop location after the train had derailed.

The train travelled through 10 active and 3 passive public level crossings, beneath a highway overpass, and through 5 sets of points,[14] mostly at speeds greater than the maximum track speed at each location. It reached a maximum recorded speed of 87.5 km/h. A summary of the train's location and speeds during key events of the runaway sequence are summarised in *Track features*.

At about 0900, Tasmania Police despatched 20 police units to respond. The police response focussed on protecting the public in front of the train by alerting pedestrians and vehicles to the danger through activation of lights and sirens on all attending police vehicles and the closure of level crossings. However, not all road-rail interface points could be protected in time, including the Bass Highway overpass.

The derailment

At 0909:29, the cement train collided with a concrete footing and fences at the end of the silo siding in Devonport Yard. The train derailed, and then came to a stop adjacent to the Mersey River Torquay Ferry pontoon in Pioneer Mariner's Park.

Shortly before the derailment, 2 pedestrians who were walking in the area heard the police sirens and looked up and saw the oncoming train. Although they quickly moved away, they were both struck by fence debris, resulting in minor injuries.

In addition to the damage to the end of the silo siding, fences and park surrounds, 7 cement wagons and the locomotive were significantly damaged, with wagon wreckage blocking the main line between Devonport and Burnie (Figure 3).

Figure 3: Derailment site in Devonport, Tasmania

Image shows the location of the injured pedestrians at the time of the derailment, as well as the cement train consist configuration.
Source: ATSB

Following the accident, TasRail suspended RCE operations. The cement train service recommenced 2 days after the accident with a locomotive at both ends and with a 2-person crew

[14] Three sets of points were facing (onto diverging tracks) and 2 sets of points were trailing (onto a converging track).

configuration. The main line between Devonport and Burnie reopened to trains at about 2300 on 24 September 2018.

Additional occurrence sequence information

The ATSB's analysis of information relating to the accident sequence (including during loading, the runaway, and the derailment) is presented in Appendix A. The analysis drew on information from multiple sources, including data recorded on the locomotive, the driver's recollection, and both data and observation of system behaviour obtained during subsequent testing.

The TR class locomotive and the driver's van[15] were fitted with data recording devices (see *Event recorders* for more information). The RCE had no data recording capability, which limited the investigation's ability to identify or understand some of the key events.

Based on the available evidence, including the data recordings, the ATSB analysis identified that the following occurred during the accident sequence:

- The RCE became unresponsive to driver commands at the point of, or soon after, a fast direction change from forward to reverse.
- The RCE initiated a momentary emergency vent of the brake pipe, likely due to a momentary 'dual direction fault' being detected. The emergency vent resulted in the locomotive's VX vent valves and emergency magnet valve (EMV) activating to exhaust the brake pipe further, which the RCE tried to oppose after the fault state cleared by supplying pressurised air from main reservoir no. 1 to the brake pipe.
- The RCE triggered 2 further emergency brake applications and releases.
- The RCE ultimately entered an unsafe state with the brakes on the train and locomotive fully released, allowing the train to roll away on the downhill grade towards Devonport.
- The RCE did not command a 'communication failed mode' or apply the train's automatic brake, either when the transmitter and receiver were unlinked, or once the receiver was out of radio range of the transmitter.
- The emergency brake applications and releases, and subsequent state with brakes released without a radio link, were not consistent with any documented fault condition behaviour.
- The RCE remained in an unsafe state, which caused the brakes on the train and locomotive to be maintained in a fully-released condition, until the train's brake pipe was ruptured in the derailment.

After comprehensive testing and analysis, the ATSB also determined that:

- The locomotive, including its control and safety systems, operated as designed.
- The locomotive electronic airbrake system operated as designed.
- There was no evidence of malicious interference to the RCE or train systems.

Given this pattern of evidence, the ATSB concluded that the RCE entered a spurious fault condition (which applied the emergency brake) when the driver rapidly commanded a direction change, and then entered a persistent unresponsive state in which the train's brakes were not applied.

This unresponsive state was not reproduced during post-accident testing activities and the specific mechanism involved was not identified. Nevertheless, the fact that the unresponsive state occurred on this occasion indicated that a latent failure mode existed within the RCE system that could not be readily diagnosed.

[15] Inputs recorded on the driver's van were limited to the headlight and horn.

The following sections provide further information regarding the cement train service, the train's braking systems, the RCE (which was being used to operate the train and its braking systems), the design process and in-service history of the RCE, and other relevant subjects.

Context

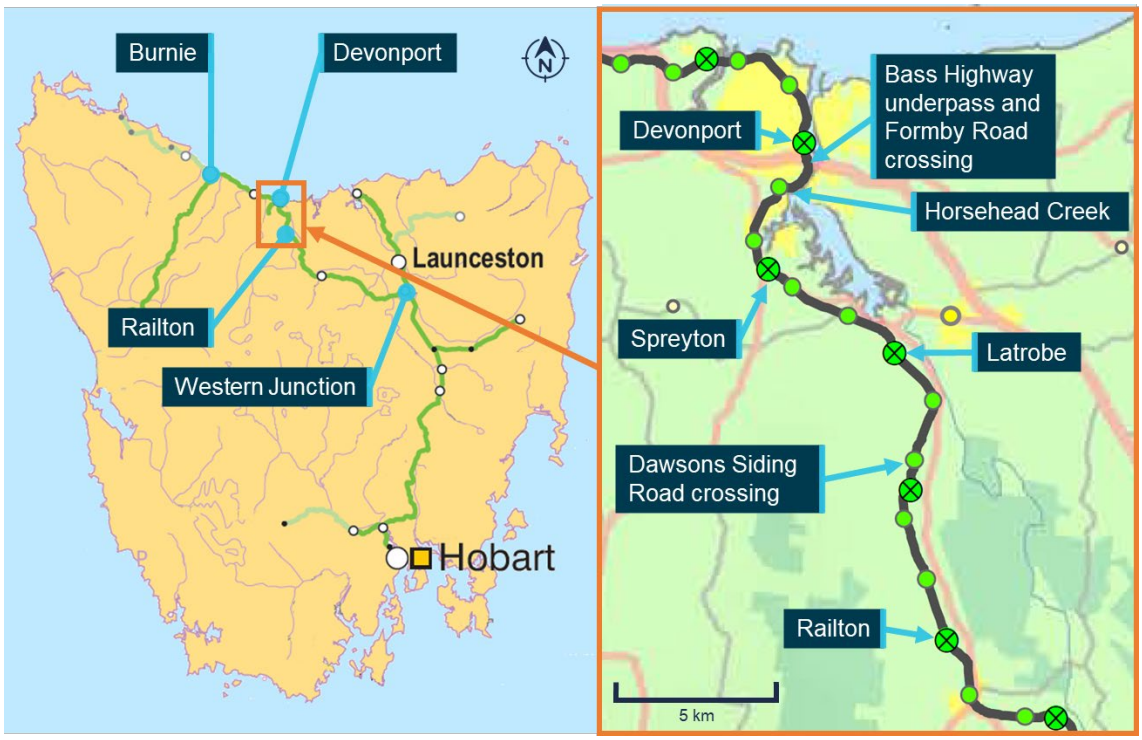
Track and network

General information

The Western Line (which included the track section from Railton to Devonport) consisted of 160 km of 1,067 mm narrow gauge railway between Western Junction and Burnie, Tasmania. TasRail was the rail transport operator (RTO)[16] accredited as the rail infrastructure manager for this track section.

Devonport, located on the northern coast of Tasmania, had a ship loading facility. Devonport Yard was located near the facility at an elevation of 3 m above mean sea level (Figure 4).

Figure 4: Map of TasRail network



Source: Australasian Railways Association and TasRail, modified by the ATSB

Railton, located 21 km to the south of Devonport, was the location of a cement plant with a train loading facility. It was at an elevation of about 59 m.

The track descended from Railton towards Devonport with brief rising gradients encountered at 3 locations, the most substantial being in the vicinity of Horsehead Creek (Figure 4).

The safeworking system[17] on the Western Line was the advanced network train control system (ANCS) track warrant (see *Network control*).

Railton loading facility

Access from the Railton loading facility to the main line was through a set of trailable electric points where the main line and the track to the siding converged (Figure 1). On approach to the

---

16 Rail transport operator (RTO): describes an organisation that is an accredited rail infrastructure manager or a rolling stock operator or both. TasRail was both the rail infrastructure manager (for example, track, signalling) and rolling stock operator (for example, locomotives, wagons).

17 Safeworking: an integrated system of operating rules and procedures that define the interaction between workers and engineered systems for the safe operation of a railway.

Railton cement siding with an empty cement train, a driver would (using the radio) remotely operate the points for entry into the siding. Once the train had entered the siding and was clear of the points, the points would automatically reset to the Western Line.

When departing Railton, the train would 'trail' through the points where the main line and track to the siding converged, which would automatically reset to the Western Line once the train was clear.

Onsite inspection by the ATSB at Railton on 22 September 2018 found no damage to infrastructure, including to the trailable electric points.

As previously noted, from the loading facility, the track had a downhill grade of 1 in 139[18] from the loading facility westward towards Devonport. There were no catch points or derailers fitted at the Railton cement siding (Figure 1). The purpose of catch points is to divert and derail an uncontrolled movement from a siding away from the main line. They are often installed on sidings with a downhill grade to the main line.

During March–April 2018, TasRail conducted a generic risk assessment for a runaway train across its entire network. An identified risk control was the provision of derailers or catch points at strategic locations based on a '…risk based approach of topography in yards to identify addition of catch points' (that is, those with descending gradients to the main line).

TasRail advised that, at the time of the 21 September 2018 accident, Railton had not been risk assessed for consideration of catch point installation.

Track features

The maximum track speed between Devonport and Railton was 60 km/h, with lower speeds of between 40 km/h and 50 km/h at 3 locations associated with track curves.

Between Railton and Devonport, the line passed through 13 public level crossings, 10 of which were actively protected by flashing lights, which were designed to activate 20 seconds before the arrival of a train travelling at maximum track speed. The remainder were passive level crossings protected by stop signs only, relying on sighting distance. There were also some private level crossings. Table 1 shows the time and speed that the runaway train passed through the level crossings and other locations, together with the track speed at these locations.

[18] That is, 1 m drop in elevation for every 139 m travelled.

Table 1: Location of runaway train and instances of excess speed (orange cells)

Track km	Time	Location	Track speed (km/h)	Recorded speed (km/h)
109.700	0846:42	Cement siding – Railton *(Commencement of runaway)*	Restricted[1]	0
109.900	0848:18	Cement Works Road level crossing (active)	Restricted	20
112.000	0851:41	Youngmans Road level crossing (passive)	60	51
116.100	0855:28	Dawsons Siding Road (active)	60 (exit 40)	76
118.000 (approx.)	0856:56	*Fastest recorded speed*	60	87.5
119.900	0858:18	Coal Hill Road (active) – Latrobe township	60	70
121.500	0859:48	Henslow Street (passive)	60	71
122.300	0900:22	Tarleton Road (active) – Tarleton locale	60	64
122.900	0900:54	Fosters Road (passive)	60	64
123.400	0901:23	Cornicks Road (active)	60 (enter 50)	65
125.100	0902:53	Sheffield Road (active) – Spreyton township	40	61
125.700	0903:29	Kelcey Tier Road (active)	40	56
126.500	0904:25	Stoney Rise Main Road (active)	40	54
126.900	0904:51	Durkins Road (active)	40	55
127.720	0905:13	Start of Horsehead Creek vicinity	40	60
128.520 (approx.)	0906:08	End of Horsehead Creek vicinity	40	43
128.870 (approx.)	0906:32	*Slowest recorded speed*	40	34
129.300	0907:47	Formby Road (active)	Restricted	47
129.380	0907:56	Devonport Yard entry (no. 88 points)	Restricted	48
129.440	0907:59	Bass Highway overpass	Restricted	49
129.530	0908:09	No. 85 points (adjacent fuel loading area)	Restricted	51
130.570	0909:06	Devonport cement silo	5	51
130.820	0909:29	Dead-end cement silos siding *(Train derailled)*	Restricted	47

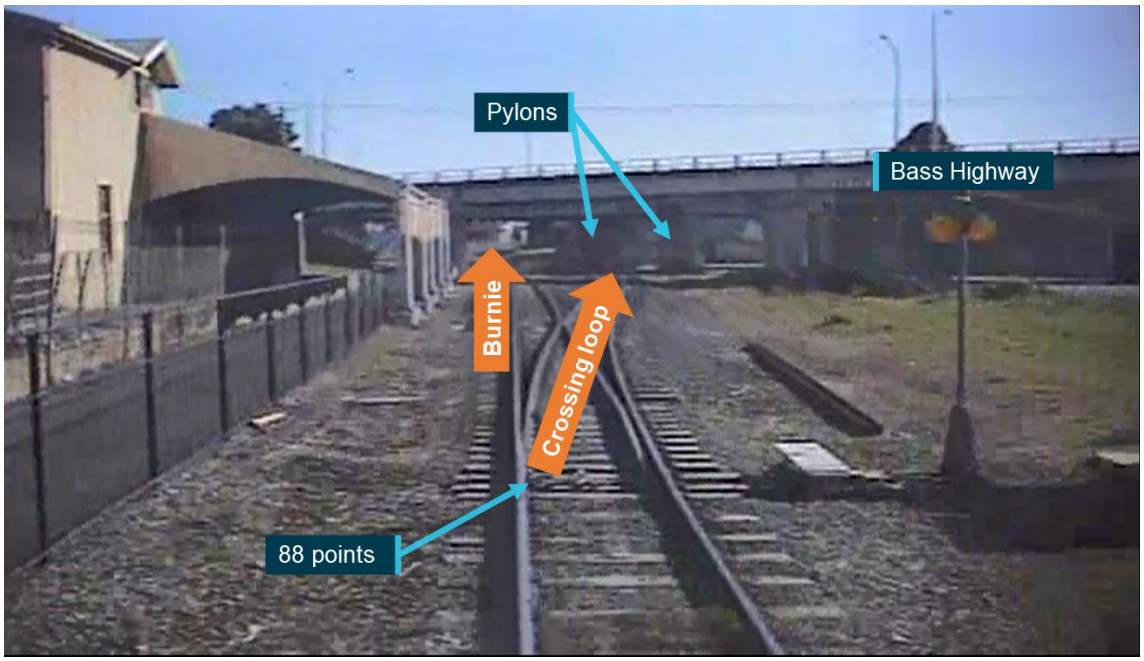
[1] Restricted speed required the train to be regulated to a maximum of 25 km/h and able to stop within half the distance of line of sight.

As the train travelled through most of these crossings at higher than the maximum track speed, the warning time was reduced. In the worst cases, the actual warning times were about 10 seconds at Formby Road crossing and 14 seconds at Dawsons Siding Road crossing (see Figure 4).

Train drivers were also required to have the train's headlight illuminated and sound the horn twice on approach to level crossings. In addition to the runaway train being uncontrolled, the locomotive's headlight (which increased visibility of the train to the public) was extinguished and the locomotive's warning horn could not be sounded.

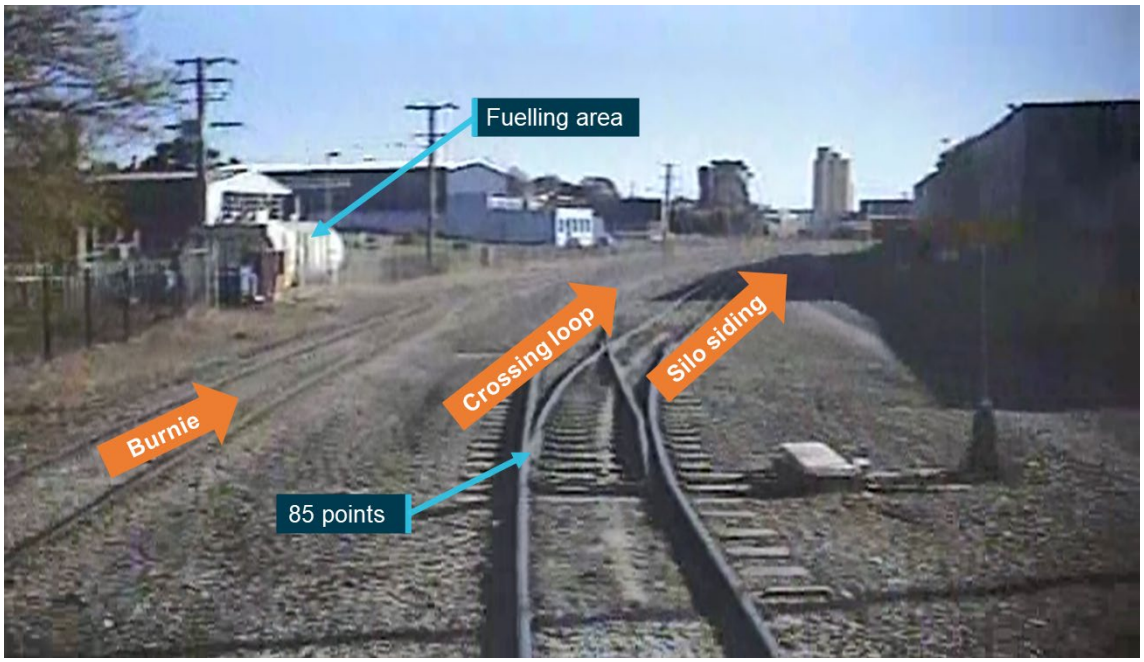
On entering Devonport Yard, the train was diverted from the main line towards no. 2 road (silo siding) for unloading, via radio-operated points no. 88 and no. 85 (Figure 2). The Bass Highway from Launceston to Marrawah (in north-west Tasmania) crossed over the line on an overbridge just to the north of no. 88 points (Figure 5). A fuelling area was located just past no. 85 points (Figure 6).

Figure 5: Devonport Yard, no. 88 points



Diversion point from the main line (towards Burnie) via no. 88 points into Devonport crossing loop. The Bass Highway passed over the line shortly after the points. The speed limit for no. 88 points was 'restricted speed' (maximum 25 km/h). The runaway train was travelling at 48 km/h at this point.
Source: TasRail, annotated by the ATSB

Figure 6: Devonport Yard, no. 85 points



Diversion point from the Devonport crossing loop via no. 85 points into no. 2 road (silo siding). A fuelling area was located on the left, shortly after the points. The speed limit for no. 85 points was 'restricted speed' (maximum 25 km/h). The runaway train was travelling at 51 km/h at this point.
Source: TasRail, annotated by the ATSB

Network control centre

Overview

Network control services for the entire TasRail network were conducted from the network control centre located within the head office building in Launceston, Tasmania. It consisted of a primary workstation under the control of the shift network control officer (NCO), with a secondary adjacent workstation available if required for backup or supervisory purposes.

During business hours, other network control centre staff that were present included the network access manager, a relief NCO and roster clerk. However, outside business hours the NCO would be the only staff member in attendance.

Network control centre personnel

The NCO who was on duty at the time of the runaway, and answered the emergency phone call from the cement train driver, had 6 years experience, having joined TasRail as a trainee NCO.

The network access manager who liaised with emergency services during the accident had previously been a driver, operations manager and NCO. In 1999 they were involved as the planning manager during the introduction of remote control equipment (RCE) operations for the cement train service (see *Operations with previous remote control equipment*).

Network control

Safeworking on the TasRail network was administered through the Advanced Network train Control System (ANCS). This system involved the issuance of GPS-tracked electronic track warrants and authorities to trains and track users, using digital radio technology. ANCS would use GPS to monitor both track warrant authority exceedances and train overspeed, providing an alarm to the network control centre in the event of detected breaches.

Yards were under local control, with the ANCS system deactivated once a train was registered within yard limits. This meant that, in the event of a runaway from a yard, the train would be invisible to the ANCS system and no alarm would be registered in the network control centre by the ANCS. Rather, the NCO was reliant on a report of the runaway from either the driver or a member of the public.

Additional Selcall[19] alarms could be sent to the network control centre from the train (independently of the ANCS). Conditions that activated a Selcall alarm included:

- emergency ‘cell call’ button on the TR class locomotive (this button provided the driver a direct means to activate the Selcall alarm)
- RCE- or locomotive-induced vigilance penalty
- RCE tilt function activation
- any event that caused an emergency reduction of brake pipe pressure when the train was travelling over 3 km/h.

Alarms received by the network control centre were presented for actioning by the NCO on the communications screen to the right of the workstation. Phone and radio communications were also managed through this screen.

No Selcall alarms were triggered by train no. 604 during the runaway sequence. This was because the driver was not in the locomotive cab, the vigilance function and tilt function required communications between the RCE transmitter and receiver, and the train was stationary when emergency brake applications were applied.

---

[19] Selcall: selective calling on a radio system, whereby receiving systems would selectively answer a radio transmission based on the sequential audio tone transmitted.

In addition, the TR class locomotive was fitted with a system for automated locomotive (SAL) computer control, an electronics and automation system that included recording of input and output data. An aspect of this functionality was the provision of a remote connection to the locomotive that provided one-way viewing access to real-time information of digital and analogue locomotive inputs and outputs, including GPS location and speed. This is the system that the rolling stock access manager utilised to monitor the train's position and speed during the runaway. Although access to this information (via the locomotive manufacturer's online portal) was available to all TasRail staff, knowledge of this access was limited. For example, the NCO who was on duty at the time of the runaway was not aware that they had access and the network access manager advised they had never tried to access it.

Emergency procedures for runaway events

When an RCE-induced alarm, locomotive alarm or emergency call was received by the network control centre, NCOs were to follow the procedure in NA-PRO-800 (*Emergency response*). If an emergency was confirmed, the NCO was to immediately protect the area from other trains and call emergency services, advising of the incident and any secondary hazards (for example, dangerous goods).

TasRail procedure SHE-PRO-201 (*Administering the incident and emergency response procedure*) required the NCO to conduct an evaluation of the potential magnitude of the event using the 'TasRail 6 x 6 risk assessment matrix'. This would inform the internal TasRail response (for example, appointment of an incident site controller, organising drug and alcohol testing, and reporting of the incident to external authorities). All incidents were to be recorded in the 'risk wizard' computer system for tracking and, where required, follow up.

The emergency response procedures did not contain any additional instructions for managing incidents that may have required a time-critical tailored response (for example, a runaway or track warrant authority exceedance).

Driver information

The driver of train no. 604 on 21 September 2018 had worked for TasRail since the early 1970s in various roles including as a driver, based at Devonport for almost all of this time. The cement train was exclusively operated with remote control equipment (RCE) since its introduction in 1999.

The driver was assessed competent as a train driver, with Australian Qualifications Framework qualification TLI42615 (*Certificate IV in train driving*) awarded to the driver in March 2017. The last reassessment of the driver's competence for 'safety critical competency units' of this qualification was conducted on 9 March 2018, with the driver deemed competent.

In relation to operation of the RCE, the driver was assessed as competent in the unit of competency TLIC3082A (*Operate a locomotive by portable remote control*) in February 2015. The last reassessment of the driver's competence for TLIC3082A was conducted on 22 February 2017 (using generation 2 RCE), with the driver deemed competent. Assessed observations included direction change, interpreting communication failed mode and control fault mode, resetting a communication failed mode occurrence, commanding and resetting an emergency stop application, and loading procedures at Railton.

There was no indication that the driver was in any way impaired at the time of the runaway accident. The driver reported they had been sleeping well prior to the shift and they did not report any issues with fatigue. They were about 7 hours into their work shift at the time of the accident. A drug and alcohol test was administered after the accident and returned a negative result (that is, no alcohol or drugs was detected).

Train information

General information

Cement train no. 604 was 220 m long and weighed about 1,132 t. It consisted of:

- a TR class locomotive (TR11) at one end
- 16 cement powder wagons (14 of which were loaded at the time of the accident)
- a driver's van wagon (DV1) at the opposite end.

The cement train was a regular bulk freight service that operated 24 hours per day, 7 days per week, completing about 6 service cycles between Railton to Devonport and return each day. TasRail was the rolling stock operator, and the cement train service was considered one of its most important, hauling more than 1 million tonnes of cement powder annually.

The cement train was operated as a driver only operation,[20] with motive power provided from the TR class locomotive, which was always positioned at the Devonport end of the train. This locomotive was always controlled by a driver using RCE:

- from Railton to Devonport, with the driver located in the cabin of the locomotive (the locomotive was hauling the consist as the leading vehicle)
- from Devonport to Railton, with the driver located in the cabin of the driver's van (the locomotive was propelling the consist as the trailing vehicle)
- with the driver outside of the train in the loading facility at Railton, while loading cement powder
- with the driver outside of the train in the unloading facility at Devonport, while unloading cement powder.

The loading and unloading operations took longer than the transits; therefore, the driver was outside of the train for the majority of an operational cycle.

The driver's van was a reclaimed Y class locomotive with no engine or traction motors. It was solely used for the driver to observe the track ahead while controlling a locomotive at the rear of the train using the RCE.

On a non-remotely-controlled train, the leading locomotive in the direction of travel has sole control authority over the train's airbrake systems. To enable this, the lead locomotive's braking system is conditioned to 'lead cut-in' mode. This controls the application and release commands of the braking systems. Trailing locomotives (under command of the lead locomotive) are conditioned to 'trail cut-out' mode, their response being similar to that of a trailing wagon.

For TasRail's remotely-controlled trains, the locomotive was conditioned to the trail cut-out mode, and so was essentially the equivalent to a trailing locomotive. The RCE took the place of a 'lead' locomotive, giving all electrical and airbrake commands to the physical 'trailing' locomotive.

Further information about the braking systems on the train is provided in *Train braking systems*.

The RCE on train no. 604 was the generation 3 RCE developed and manufactured by Air Digital Engineering (ADE) for TasRail. Further information about the RCE is provided in *Remote control equipment*.

Post-accident inspection

Onsite inspection of the accident scene in Devonport by the ATSB on 21 September 2018 found that the TR class locomotive and first 8 cement wagons were in a derailed state. The continuity of the brake pipe, operational status of the triple valve braking equipment (see *Automatic brake*) and condition of brake blocks on the rolling stock was examined, where possible.

---

[20] Driver only operation: a train crewing configuration where a single driver operated the train without the presence or assistance of any other on-board personnel.

It was observed that the RCE receiver was correctly connected to the TR class locomotive, with the locomotive brake pipe continuous to the first wagon. Derailment damage prevented verification of brake pipe continuity across wagons 1 to 5 and across wagons 6 to 7. Likewise, the operational status of the triple valve on wagon 4 and brake block condition on wagons 1–7 were unable to be verified due to accident damage. The status of all other brake pipe continuity points and triple valves on the train was found to be correct, and brake blocks present and within wear tolerances.

When the ATSB inspected the TR locomotive, it was shut down with the batteries turned off and with all circuit breakers in the 'off' position. However, TasRail advised the ATSB that these actions were performed as part of the emergency shutdown after the derailment and that all circuit breakers were correctly configured for operation when its personnel arrived at the site. All other cab switches and equipment were observed to be generally conditioned correctly for RCE operation. The following was also noted:

- the locomotive's automatic brake handle was in 'release' (no effect as in 'trail cut-out' mode)[21]
- the locomotive's independent brake handle was in 'release' (no effect as in 'trail cut-out' mode).

In summary, although anomalies were noted, the ATSB did not identify any locomotive configuration issue that would have caused the train not to respond to RCE commands from the driver. In addition, as previously discussed (see also Appendix A), analysis of available evidence identified that the locomotive, including its control and safety systems, operated as designed.

Operational inspections and maintenance

There was one train consist dedicated to the cement service between Devonport and Railton. The TR class locomotive was swapped every 30 days for servicing.

The cement wagons were inspected every 4 months at the East Tamar Junction wagon maintenance facility. Between these inspections, the driver of the cement service would perform a general inspection for obvious mechanical wear and damage. One side would be checked at Devonport after unloading and the other side at Railton prior to loading.

The driver's van was inspected at 2-monthly intervals at either East Tamar Junction or Burnie maintenance facility, with a general inspection undertaken in-between as with the cement wagons. Basic safety checks occurred every 7 days.

In-service tests of the train braking systems (noted on the brake test certificate) were valid for 7 days unless the train was idle for more than 4 hours or a shunt of the rolling stock had occurred.[22] Records showed that the last shunt of the consist had occurred on 10 September 2018, with the last terminal examination (including all relevant brake tests and a test of the RCE tilt[23] and vigilance[24] functions) conducted the day before the accident.

During its 30-day operational period, the locomotive was given a basic safety and operational check every 7 days, which was to include (among other things) provision of consumables, multiple unit functionality, sand, direction, traction power and brake tests. The record of the basic safety and operational check, completed for TR11 the night before the accident, did not mark off the multiple unit functionality, sand, direction, traction power and brake checks. A review of TR11's previous basic safety and operational checks found these items were not always recorded. TasRail reported that, as the train was operated almost continually, functions such as traction power and braking were effectively being checked on an ongoing basis. As previously noted, no problems with the serviceability of the locomotive were considered to be involved in the development of the runaway sequence.

---

[21] For cab handle unit positions and modes of operation, see *Train braking systems*.

[22] Tests included brake holding, brake pipe leakage, brake inspection, mechanical inspection, loading inspection and brake pipe continuity.

[23] See *Driver operation.*

[24] See *Vigilance function.*

Propelling operations

A unique aspect of TasRail's cement train operation was the use of a single motive power source, the TR class locomotive, at the rear of the consist (in a propelling configuration). This occurred when the train was operated in the empty direction, from Devonport to Railton, with the locomotive propelling (pushing) the train at track speed on the main line. This generated increased buff (compressive) forces and vertical loads in the couplings between wagons, particularly between the locomotive and first few wagons compared to a train that was being pulled by a locomotive.

Propelling was not a factor in the runaway accident sequence. However, as part of its investigation, the ATSB considered how RCE was integrated into the rail operation. TasRail's use in a propelling configuration on a main line from Devonport to Railton was permitted without restriction while being controlled from the driver's van. As far as could be determined, no other train service in Australia used a similar rear-propelling-only configuration.

Due to the increase in lateral force against the rail head and reduction in wheel load, excessive buff forces can be a cause of wheel lift and flange climb or jack-knife derailments.[25] Careful and gradual increase of buff forces by the driver is therefore required during propelling movements to minimise the chance of derailment. Although these effects are greatest with loaded wagons, they remain present with empty wagons.[26]

TasRail provided some train handling instruction to drivers, with emphasis on efficiencies of train movement (for example, reduction in fuel usage and brake block wear). It did not provide instructions related to the rear-propelling configuration used with its RCE, including at maximum track speed.

Further aspects of the use of the RCE with propelling operations are discussed in *Reduced effectiveness of automatic emergency brake*.

Train braking systems

General description

On non-remotely-controlled (or conventional) TasRail trains, a driver operated the controls from within a locomotive cabin at the lead of the train consist. With these controls, a driver could issue commands for tractive effort to move the train and braking effort to slow and stop the train. In addition, several safety features were available to the driver, such as the vigilance system and the emergency engine stop function (which shut off the diesel engine).

This section provides an overview of the braking systems on the TR class locomotive and how they are applied on a non-remotely-controlled train. The RCE, and the means of using it to control braking, is discussed in the next section.

There were 3 braking control systems fitted to the TR class locomotive:[27]

- automatic brake (a type of airbrake that controlled brakes on the entire train)
- independent brake (a type of airbrake that controlled brakes on the locomotive only)
- electrical dynamic brake on the locomotive.

---

[25] Nadal's formula is used to calculate the likelihood of derailment. See also RISSB 2014, *Derailment investigation and analysis guideline.*

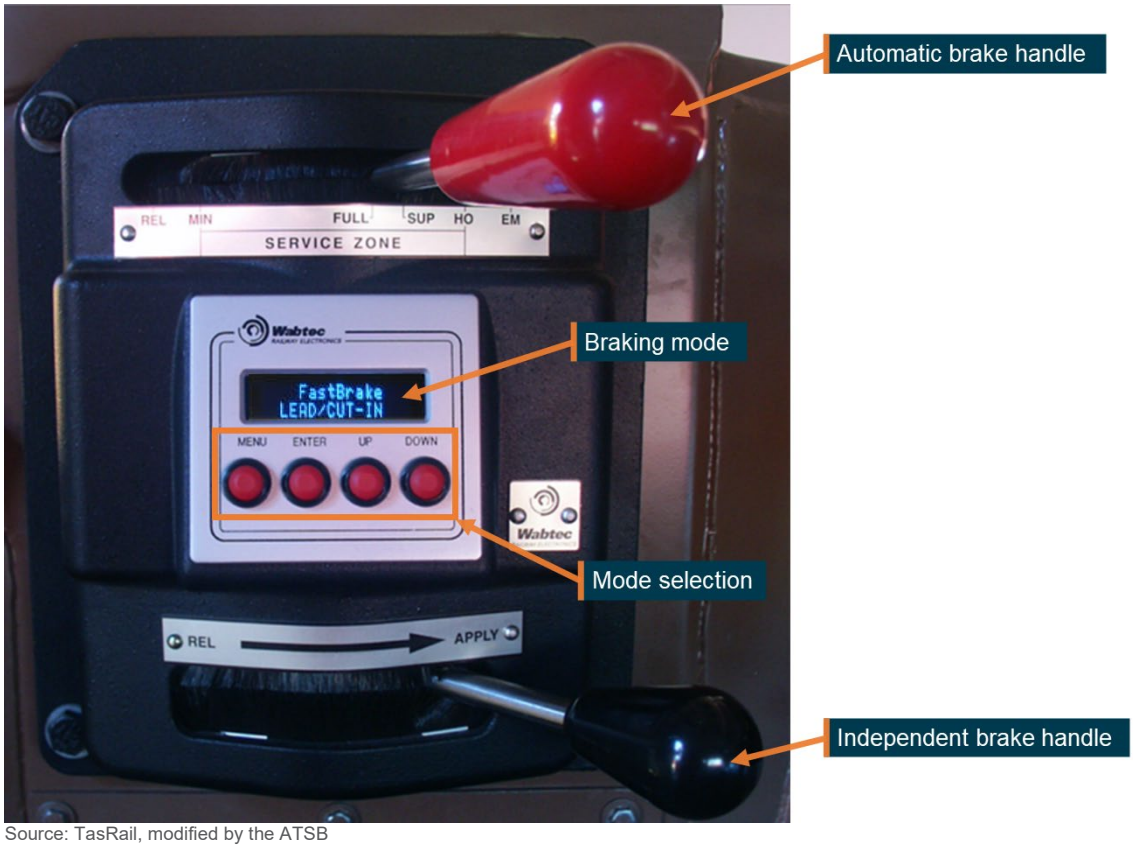
[26] Propelling with empty or lightly-loaded wagons between the locomotive and heavily-loaded wagons has a particularly high risk of jack-knife derailment; however, this type of consist was not used in TasRail's cement train operation.

[27] Parking brakes (or handbrakes) were also fitted to each locomotive and wagon.

The use of each of the 3 braking systems depended on the circumstance during which braking effort was required. For both airbrake systems, braking was achieved by the air-powered application of brake blocks[28] directly to locomotive or wagon wheels.

The 2 airbrakes (automatic and independent) were electronically-controlled and air-actuated on the leading locomotive. The airbrake system consisted of a driver's cab handle unit (CHU, Figure 7), which sent electronic commands to the pneumatic operating unit (POU) located in the locomotive engine room. The POU then controlled the pneumatic responses to slow or stop the train.

Figure 7: Cab handle unit in TR locomotive



Source: TasRail, modified by the ATSB

Compressed air for the airbrake system was provided by a compressor and stored in 2 main reservoirs, both of which were on the locomotive:

- Main reservoir no. 1 (MR1) air was supplied to other rolling stock by means of the main reservoir equalising pipe (MREQ).
- Main reservoir no. 2 (MR2) was supplied air pressure from MR1 via a one-way check valve. MR2 air was used by the POU to effect braking commands.

Automatic brake

Introduction

The automatic brake applied and released brakes on both the hauling locomotive(s) and any trailing rolling stock (that is, across the entire train). It was termed the 'automatic' brake because the brakes automatically applied when air pressure was lost, such as in a major derailment or train

[28] This is known as wheel-tread braking: where a brake block applies pressure to the wheel tread, causing friction to dissipate energy, thereby slowing the train.

separation.[29] In normal operation, the automatic brake was used as the main mechanism for slowing and stopping the train. The driver did this using the CHU automatic brake handle.

Integral to the function of the automatic brake was a continuous pipe of air that ran from the front to the rear of the train, known as the 'brake pipe'. Flexible rubber hoses at each end of a wagon allowed connection of the brake pipe with a locomotive or other wagons.

In simplified terms, air pressure in the brake pipe performed 2 functions:

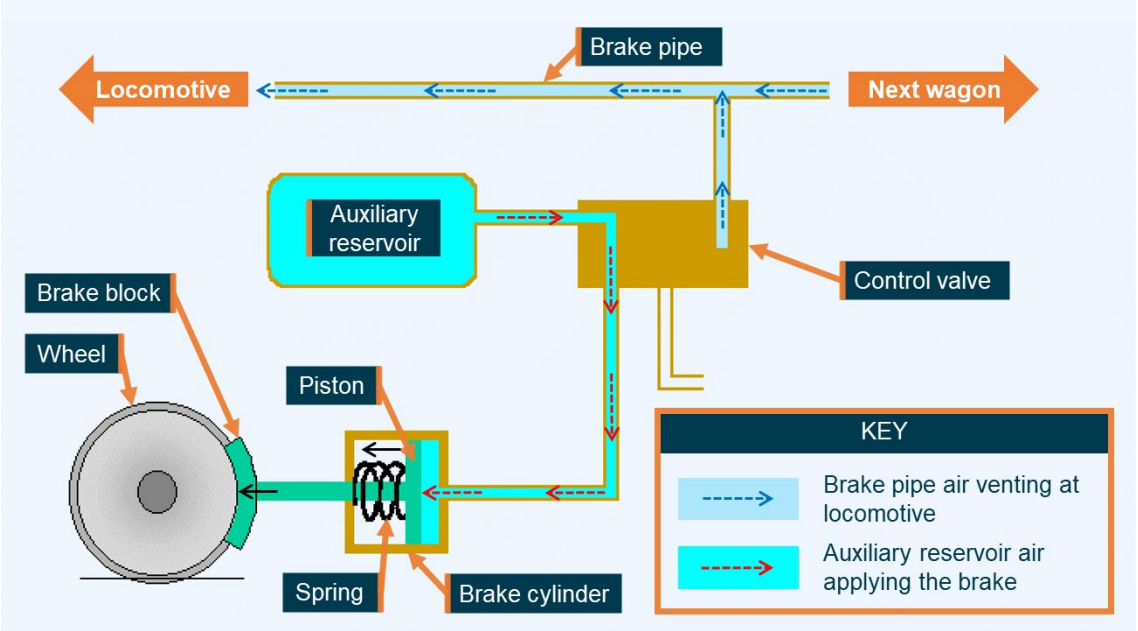
- acted as a signal to control brake application and release on both the locomotive(s) and the rest of the train
- provided a conduit for 'charged' (pressurised) air from the locomotive(s) to storage reservoirs in the wagons, which then provided the braking application force.

Decreases in brake pipe pressure applied proportional increases in pressure in locomotive and wagon brake cylinders, as long as there was enough air in the storage reservoirs to make the application. Increases in brake pipe pressure, above a small amount, fully released the brakes.

Means of operation

The lead locomotive charged the brake pipe with air from MR2 to an air pressure of 500 kPa when brakes were fully released. In addition to the brake pipe, each cement wagon[30] was fitted with a pneumatic control valve ('triple valve'), auxiliary (storage) reservoir, and brake cylinders.[31] The control valve responded to changes in pressure within the brake pipe. On sensing a reduction in brake pipe air pressure, the control valve would transfer air from the auxiliary reservoir to the brake cylinder, which would apply brakes. Figure 8 shows how this system worked in practice for a brake application.

Figure 8: Wagon airbrake application process



The image is a simplified representation of an airbrake application on a wagon. The control valve consisted of rubber diaphragms, springs and ports that responded to reductions in brake pipe air pressure to perform the required brake apply response.
Source: The Railway Technical Website, modified by the ATSB

[29] Train separation: where the rear of the train detached from the front of the train, either through coupler failure or uncommanded uncoupling.

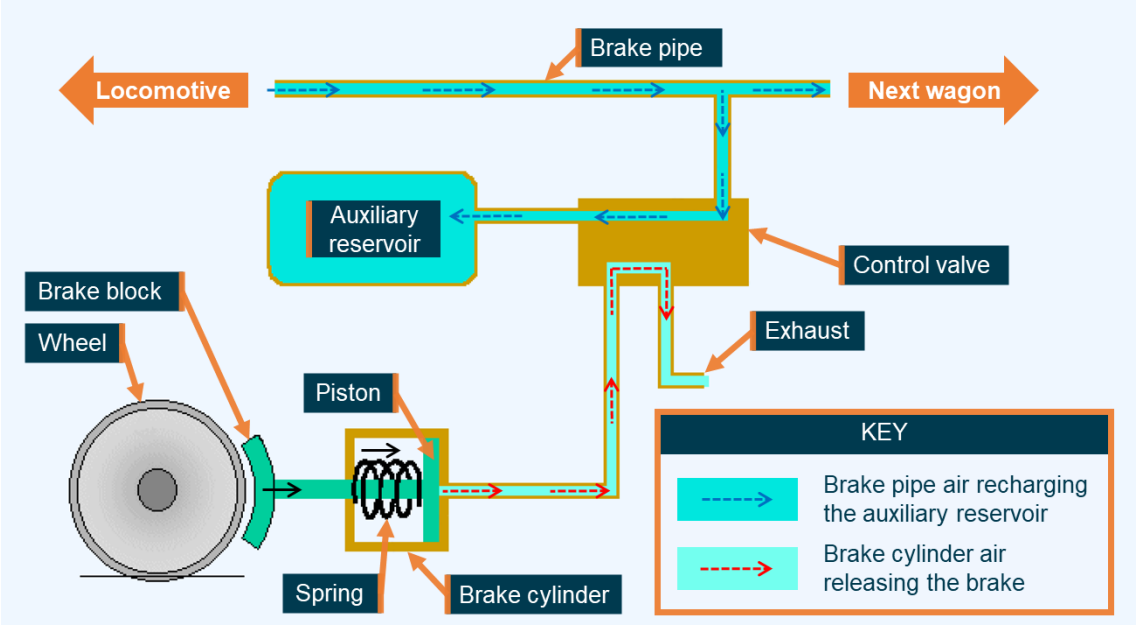
[30] Although different, the driver's van's braking components operated in a similar way to that of the cement wagons.

[31] Further braking components were present but have been omitted for relevance and simplicity.

A reduction in brake pipe pressure would similarly apply the brakes on the hauling locomotive. The locomotive's POU would read the brake pipe pressure and command a corresponding brake cylinder pressure of up to a maximum of 350 kPa on the locomotive.

Once the required speed reduction had taken effect, the driver would place the CHU automatic brake handle in release, which restored the brake pipe pressure to 500 kPa (Figure 9). On sensing an increase in brake pipe air pressure, the control valve would vent air from the brake cylinder to release the brakes, and also allow air from the brake pipe to recharge the auxiliary reservoir to 500 kPa.

Figure 9: Wagon airbrake release process



The image is a simplified representation of an airbrake release on a wagon. The control valve consisted of rubber diaphragms, springs and ports that responded to an increase in brake pipe air pressure to perform the required brake release response.
Source: The Railway Technical Website, modified by the ATSB

Driver controls

The CHU automatic brake handle had 6 detent positions for driver control (Figure 7):

- release (REL) – brake pipe charged to 500 kPa
- minimum service (MIN) – brake pipe reduced to 450 kPa at a service rate
- full service (FULL) – brake pipe reduced to 350 kPa at a service rate
- suppression (SUP) – brake pipe reduced to 350 kPa at a service rate (for penalty brake reset)
- continuous service / handle off (HO) – brake pipe reduced to 0 kPa at a service rate
- emergency (EM) – brake pipe reduced to 0 kPa at a rapid rate.

The operational area between minimum service and handle off detents reduced the brake pipe pressure at a steady service rate. The emergency position vented brake pipe pressure at a rapid rate. Maximum braking effort occurred when brake pipe pressure was reduced to 350 kPa, known as a full-service brake application. At this point, the brake pipe, auxiliary reservoir and brake cylinder pressures all equalised with each other at about 350 kPa. The ATSB was advised by the

airbrake manufacturer that a 350 kPa brake cylinder pressure on both wagons and locomotives was unlikely to result in wheel lock.[32]

Although the driver could graduate an increase in automatic brake effort by reducing brake pipe pressure incrementally between minimum-service and full-service positions, it was not possible to graduate a release. Once the control valve on the cement wagons sensed a pressure rise over 12.5 kPa in the brake pipe, it would release the brakes.

Brake pipe charging flow indicator

During an automatic brake release, MR2 air supply, which was fed from MR1, would recharge the brake pipe. The brake pipe charging flow indicator provided an indication of the flow rate from MR2 to the brake pipe. It was displayed to the driver on the TR class locomotive in-cab display screen. The purpose of the brake pipe charging flow indicator was to indicate:

- when the brake pipe (and thereby wagon auxiliary reservoirs) was fully charged. This avoided the circumstance of 'running out of air', whereby repeated brake applications with short release (brake pipe recharge) periods could result in loss of auxiliary reservoir air pressure. As a result, no air pressure would be available for the wagon brake cylinders.
- when tractive power could be applied from a standing start (that is, once the train's brakes were fully released). This avoided high locomotive tractive effort against the train's brakes causing high draft forces, resulting in possible coupling or draft gear[33] damage, train separation or rail burn.[34]
- uncommanded loss of brake pipe pressure. This could indicate a broken brake pipe hose, derailment or train separation event; all of which required an immediate driver response.

Indicators of main reservoir pressure were also available, and a driver could monitor for changes in these pressures for the same purposes.

Penalty conditions

In addition to the handle off position on the CHU automatic brake handle, there were a number of penalty conditions for a locomotive set to 'lead cut-in' mode that would result in a brake pipe pressure vent to 0 kPa (brake application) at a service rate. These included:

- Vigilance penalty: a penalty mode triggered by the vigilance system on the locomotive. The vigilance system was a protection against driver incapacitation. A penalty occurred if a driver did not acknowledge an audible warning light and alarm or make a control input within a periodic 15-second invitation period. This system was active when the locomotive was in lead cut-in mode and brake cylinder pressure was <170 kPa (that is, likely moving).
- Overspeed penalty: a penalty mode triggered by the detection of locomotive overspeed. The TasRail TR class locomotives were configured so that an overspeed penalty occurred if the locomotive speed reached or exceeded 88 km/h. The maximum speed on the TasRail network was 70 km/h.
- CHU to POU communications loss
- braking system power supply failure.

When the brake pipe pressure fell below 297 kPa, the locomotive would operate the power control switch (PCS). This would remove the locomotive's generator excitation, preventing further tractive

---

[32] Wheel lock occurs when there is insufficient wheel-to-rail friction to keep the wheel rotating, such as when excessive braking force is applied. In instances of wheel lock the friction of the wheel sliding along the rail head can result in flat spots on the wheel tread. These could result in further wheel damage, rail damage, or derailment where a severe flat spot impacted the rail head once the wheel rotates again.

[33] Draft gear: components that connected the coupling to the rolling stock structure. It also accommodated the dispersal of an amount of buff and draft forces.

[34] Rail burn: damage to the rail head caused by overheating through prolonged wheel slippage. It could result in chips or thermal cracks to the rail head.

power and dynamic brake from being generated. The driver reset the penalty condition by clearing the cause of the penalty and placing the CHU automatic brake handle in suppression, before returning it to release. The PCS would reset once the brake pipe pressure reached over 428 kPa.

Emergency brake

The driver could activate emergency braking by either the CHU automatic brake handle or by activating a separate emergency dump valve in the locomotive cabin. In addition, the brakes would automatically apply across the train in the event of a brake pipe rupture, such as during a derailment or train separation. In both cases, braking would be initiated by venting the brake pipe to 0 kPa.

On sensing a rapid (emergency) brake pipe pressure drop (that is, more than 69 kPa / second, either commanded by the driver or initiated by brake pipe rupture), the hauling locomotive POUs would energise the emergency magnet valve (EMV), increasing the rate of pressure drop. In the case of a leading locomotive set to lead cut-in mode, the POU would also prevent recharge of the brake pipe. The hauling locomotive would enact a PCS request and emergency sanding,[35] the latter if the train speed was over 3 km/h. As no further braking effort was achieved once the brake pipe reduced below 350 kPa (due to pressure equalisations), emergency braking only increased the rate at which brake application occurred. Emergency braking did not increase the level of braking effort.

For a locomotive configured to lead cut-in mode, a reset of an emergency brake application by the driver (after clearing the cause) required the CHU automatic brake handle to be placed in the emergency position for a minimum of 60 seconds. The purpose of this timeout was to ensure the train had come to a complete stop before a brake release. This prevented train separation from coupler breakage due to heavy braking at the rear of the train coinciding with releasing brakes at the front. On trailing locomotives configured to ‘trail cut-out’ mode, the POU’s EMV would self-reset after 20 seconds in preparation for a brake pipe recharge command from the lead locomotive.

Emergency vent valves

The TR class locomotive was fitted with 2 emergency vent valves, called ‘VX vent valves’ by the manufacturer. They were a pneumatic addition to the brake pipe at each end of the locomotive (see inset Figure 11), which was a requirement in the Australian Standard for locomotive braking systems.[36]

On sensing a rapid (emergency rate) reduction of brake pipe pressure, the VX vent valves released brake pipe air pressure, increasing the speed of brake pipe pressure drop in the event of an emergency. After the brake pipe pressure reduced sufficiently, the valve would internally equalise and reseat (stop venting). As VX vent valve operation was related to internal pressure equalisation, if air was still being supplied to the brake pipe when equalisation occurred, the VX vent valves would reseat, stop venting, and permit recharge at pressures above 0 kPa.

Vent valves were not fitted to the cement wagons or the driver’s van. Prior to using TR class locomotives, TasRail used DQ class locomotives. These also were not fitted with vent valves.

In summary, both the locomotive’s VX vent valves and EMV were designed to assist the rapid exhaust of the brake pipe on detection of an emergency brake command, either by the driver or through brake pipe rupture. Additionally, this ensured activation of the locomotive’s PCS, thereby removing traction power. Timeouts for EMV reset applied to prevent early emergency brake release and possible train separation.

---

[35] This delivered sand to the rail head in front of the leading wheels of each locomotive bogie, increasing friction between the rail and wheels which assisted in a rapid stop.

[36] RISSB 2014, *AS7510.1:2014 Braking systems – part 1 – locomotive rolling stock*, p. 18.

Independent brake

The independent brake applied and released brakes on hauling locomotives only, independently of any trailing rolling stock. The driver controlled this using the CHU independent brake handle to adjust pressure in a 'control pipe'. The braking could be graduated between the release (REL) and apply positions, the latter resulting in an air pressure charge (effected by the POU) of up to 350 kPa in the control pipe.

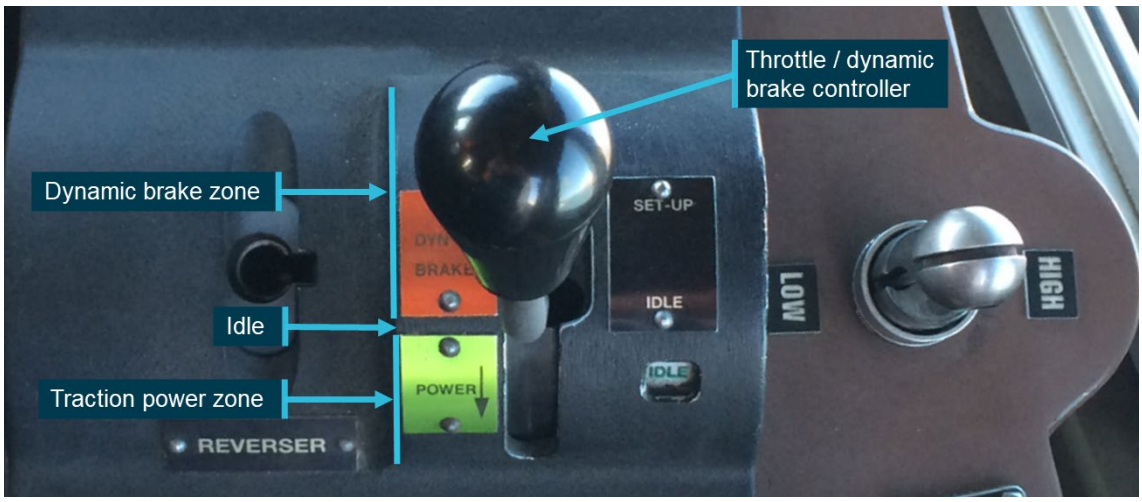
Flexible rubber hoses on each end of the locomotive were provided to allow connection of the control pipe with other locomotives. This provided a facility for one or more trailing locomotives (if used) to receive the control pipe pressure from the lead locomotive to effect independent brake applications on the trailing locomotive(s).

Dynamic brake

On the TR class locomotive, the traction motors could also be used to slow (but not stop) the train using the dynamic brake system. This reduced wear on braking components and reduced the risk of having insufficient air pressure to apply brakes after repeated applications and releases.

To engage the dynamic brake, the driver would return the throttle / dynamic brake handle to idle from the traction power zone then move it into the dynamic brake zone (Figure 10). This action would change the traction motor fields from a tractive power to a generator configuration. The subsequent power generated by the moving locomotive wheels was fed to resistor grids and dissipated as heat, resulting in a retarding force.

Figure 10: Driver's throttle (traction power) and dynamic brake controller



Source: TasRail, annotated by the ATSB

Post-accident inspection

As previously discussed (see also Appendix A), analysis of available evidence identified that during the accident sequence the RCE initiated a momentary emergency vent of the brake pipe, which resulted in the locomotive's VX vent valves and EMV applying to exhaust the brake pipe further. The RCE also triggered 2 emergency brake applications and releases, which did not replicate any fault condition behaviour documented for the RCE. The locomotive electronic airbrake system operated as designed.

Remote control equipment

Background

In about 1999, TasRail's predecessor, ATN Tasrail, altered the business operating model for its existing cement train service, changing from a 2-person crew configuration to a driver only operation configuration using RCE. In addition to reducing staffing costs and exposing fewer staff

to hazards during loading and unloading, this operating model allowed for the use of a single locomotive, without the requirement to either run-around or turn the consist at Devonport and Railton.

ATN Tasrail found during the tendering process that there was limited market availability of portable main-line RCE units.[37] Shortly afterwards, ADE proactively approached ATN Tasrail with its developmental RCE system. Based on the outcome of trials, in August 1999, the generation 1 RCE system was purchased by ATN Tasrail, being ADE's first RCE customer.

In about August 2010, the operator (now TasRail) replaced generation 1 RCE with ADE's generation 2 RCE. In turn, following issues with the ongoing reliability of generation 2 RCE and other factors, TasRail commissioned ADE to develop the generation 3 RCE, and it was introduced in February 2018 (see *Remote control equipment development*). Generation 3 RCE was fitted to train no. 604, and unless otherwise noted, references to RCE in this report relate to the generation 3 RCE.

ADE advised the ATSB that, in addition to TasRail, 5 Australian rail transport operators (RTOs) used the generation 2 RCE. However, all had ceased to do so by the time of the accident in September 2018. TasRail was the only RTO that used the generation 3 RCE.

TasRail primarily used the RCE for cement train services on the section of railway between Devonport and Railton. In addition, it permitted RCE operations for:

- emergency banking[38] purposes (assisting with heavy loads) over Don Hill between Devonport and Leith
- transfer of a locomotive and driver's van to Burnie for maintenance purposes
- transfer of cement wagons to East Tamar Junction for maintenance purposes.

System overview

The RCE comprised 3 main components:

- a transmitter, a portable unit carried by the driver
- a receiver, mounted on the locomotive, which interfaced with the locomotive's electrical systems via a multiple unit cable
- an air box, mounted on the locomotive, which interfaced with the locomotive's airbrake system via air hoses.

The RCE receiver received commands from the RCE transmitter, with communications between the 2 components linked on start-up of the RCE system. When operated by the driver, the transmitter sent remote control signals via radio to the receiver. The receiver then sent electrical signals to the air box to enact airbrake commands, or to the locomotive for throttle, direction, and other commands.

The RCE replicated most of the controls available on the locomotive, including automatic brake, independent brake, dynamic brake, engine, and direction controls. An emergency stop switch was intended to imitate the response to placing the locomotive's automatic brake handle in the emergency position (see *Emergency stop function*).

Interface with the locomotive

Generation 2 RCE's receiver and air box were located at the front of the previously-used DQ class locomotives. On introduction of the TR class locomotives, the location was changed to the rear of the locomotive, due to the absence of a footplate or handrails to allow mounting of the receiver and air box at the front of the locomotive. The rear location was continued with generation 3 RCE.

---

[37] ATN Tasrail required an RCE unit that allowed flexibility in removal from one locomotive to another, without being semi-permanently integrated into the electronics and pneumatics of the locomotive control systems.

[38] Banking: the use of a bank locomotive provided to assist rail traffic on a steep grade (bank).

In this arrangement, the receiver was placed on the rear locomotive footplate with the air box located on the right-side footplate (Figure 11).

Figure 11: Rear of TR class locomotive, showing interface with generation 3 RCE

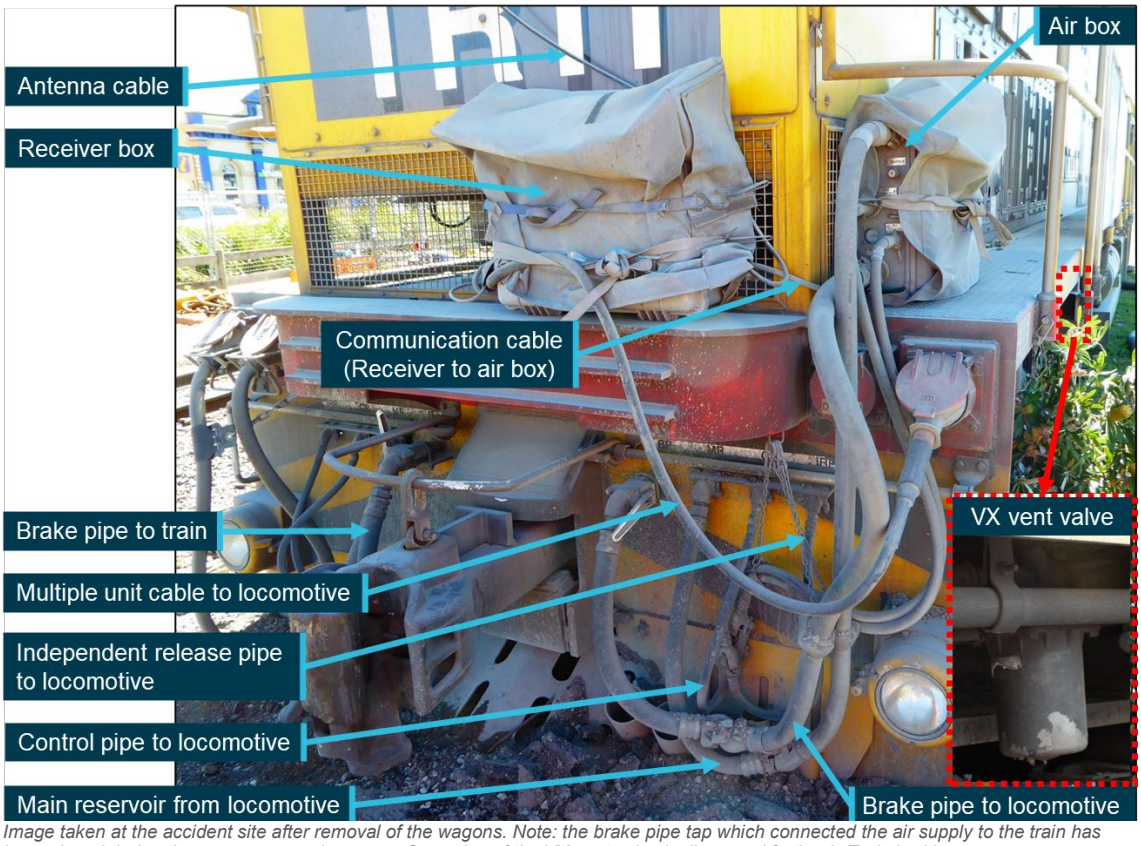


Image taken at the accident site after removal of the wagons. Note: the brake pipe tap which connected the air supply to the train has been closed during the wagon removal process. Operation of the VX vent valve is discussed further in Train braking systems.
Source: ATSB

The air box location affected some aspects of the braking system response, due to it being connected to the airbrakes at a different point in the pneumatic circuit (see *Remote control equipment emergency brake reset*).

A multiple unit electrical cable from the RCE receiver was plugged into the TR class locomotive's multiple unit socket to provide the receiver with a 74 V DC power supply. The multiple unit cable also carried electrical commands (for example, direction, throttle and dynamic brake settings, sand and horn) from the receiver to the locomotive.

A communication cable from the receiver to the air box carried electrical airbrake commands for the pneumatic system within the air box to enact. The air box was supplied with pressurised air from main reservoir no. 1 (MR1) by the main reservoir equalising pipe (MREQ). To allow this, the driver was required to condition the TR class locomotive's braking system to 'trail cut-out' mode. This gave control of the airbrake to the RCE, which could directly command:

- application of the train's automatic brake through brake pipe pressure reduction via a brake pipe valve and/or a separate emergency brake valve in the RCE air box
- release of the train's automatic brake by recharging the brake pipe with MREQ air (not MR2 air as on a TR class locomotive without RCE)
- release of the locomotive's brake cylinder pressure during an automatic brake application through charging the independent release pipe ('bail-off' function)[39]

[39] For train handling purposes, the brake cylinder pressure from an automatic brake application was usually released on hauling locomotives, without affecting the brake application on the trailing rolling stock. This was known as 'bailing-off' the automatic brake application and was achieved by the driver depressing the CHU independent brake handle.

- application of the locomotive's independent brake through charging the control pipe with MREQ air (not MR2 air as on the TR class locomotive without RCE)
- release of the locomotive's independent brake through exhausting the control pipe
- penalty brake applications.

Figure 12 shows the interface between the locomotive and the first wagon. The brake pipe connection shown allowed reductions and increases in brake pipe pressure by the RCE, enacted through the adjacent brake pipe connection (Figure 11), to be registered by the wagons and driver's van. The MREQ air hose connected to the first wagon provided MR1 air supply to the wagon roof hatches, which were operated for cement powder loading purposes at Railton.

Figure 12: Interface of RCE from rear of TR class locomotive to first wagon

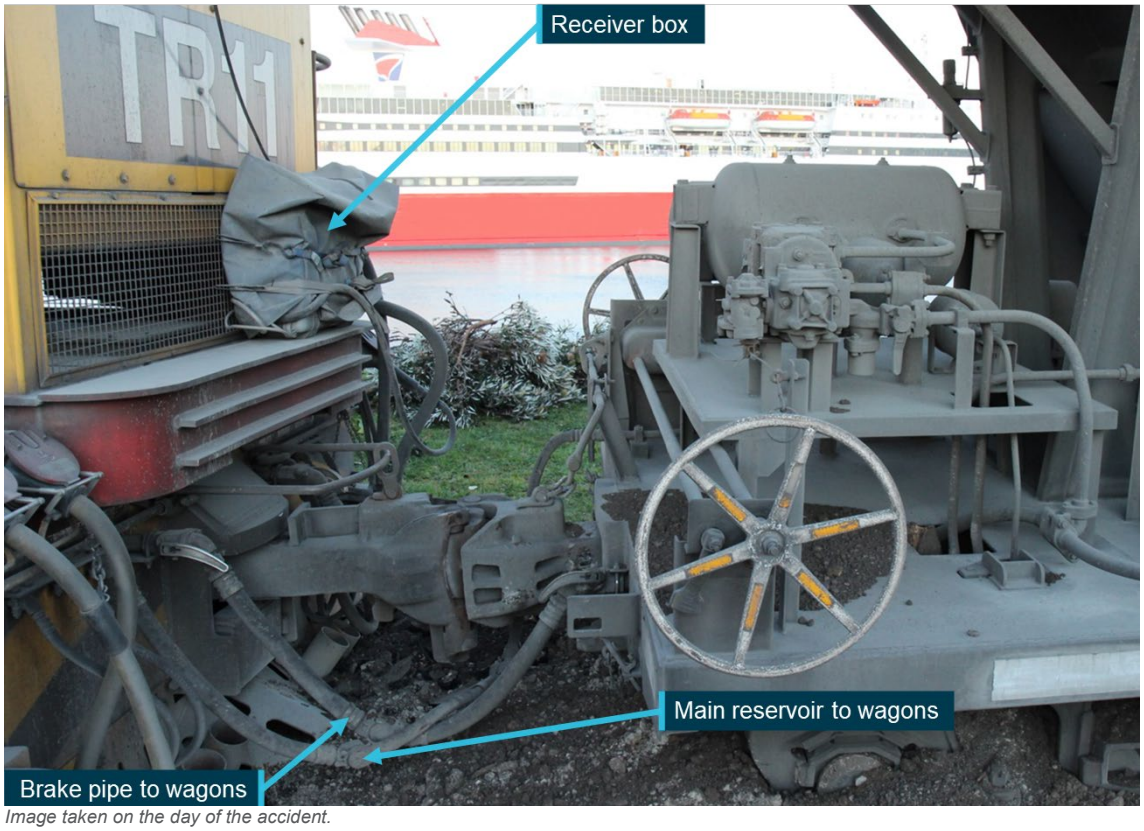


Image taken on the day of the accident.
Source: ATSB

Driver operation

The RCE transmitter (Figure 13) was designed to replicate several controls available to the driver as if they were operating a non-remotely-controlled train consist from the cabin of a locomotive. These were:

- direction controller
- throttle control
- brake controls (independent brake, automatic brake, dynamic brake and emergency stop)
- sand
- horn
- vigilance function
- generator field switch (by selecting a throttle notch while in forward or reverse)
- engine run switch (by entering 'run' mode).

Figure 13: Generation 3 RCE transmitter

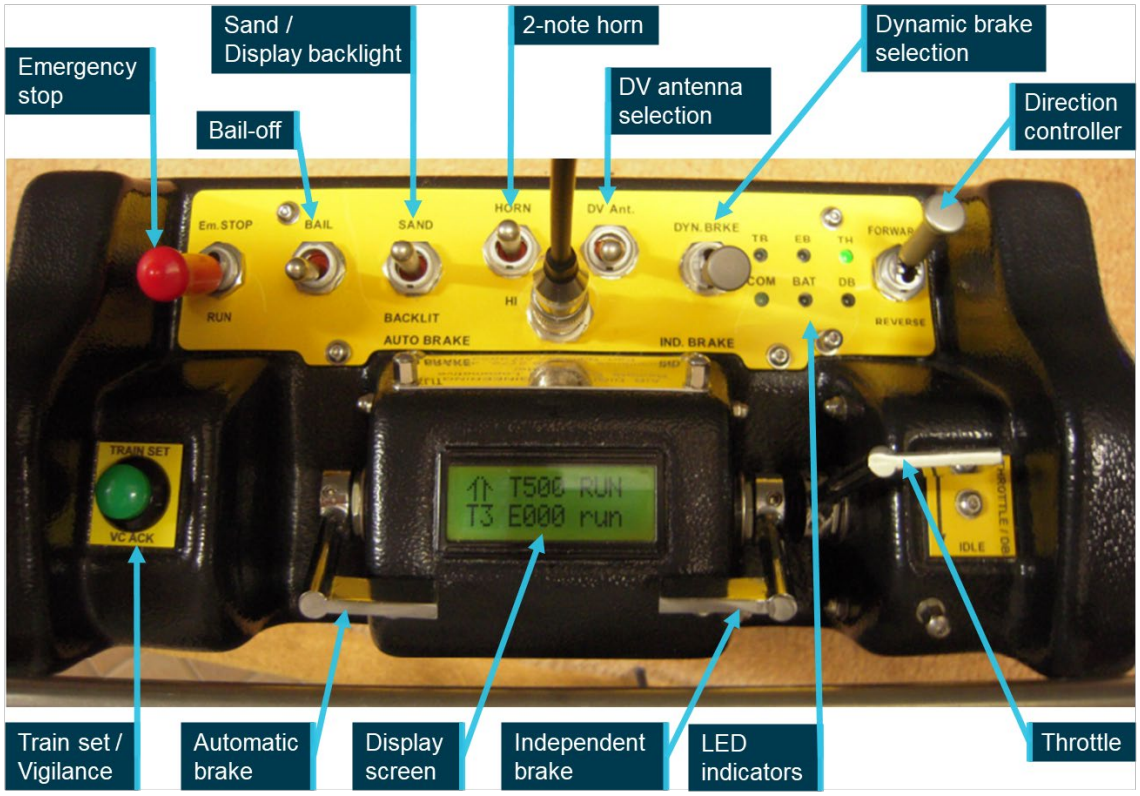


Image shows the RCE transmitter as initially supplied to TasRail for generation 3 RCE. Differences to generation 2 RCE's transmitter included reversal of the emergency stop position, and the addition of the dynamic brake switch. The transmitter's key switch was located on the left side of the transmitter (not shown).
Source: Air Digital Engineering, annotated by the ATSB

The direction controller had 3 positions:

- forward (up)
- neutral (middle)
- reverse (down).

The neutral position was gated; that is, the driver had to lift the selector switch up to go past the neutral position. Although not recommended by ADE in its RCE operation manual, it was possible to immediately change direction from forward to reverse and vice versa on the transmitter without pausing in the gated neutral position, if the selector switch was lifted clear of the gate. In contrast, on a locomotive the change of direction was delayed through the length of travel of the direction controller between the forward and reverse positions and a detent for the neutral position.

The RCE transmitter's throttle and brake controls had a significantly shorter travel and lighter feel than those of the locomotive's throttle / dynamic brake handle, automatic brake handle and independent brake handle. Detents for these controls were provided on the transmitter to enable the driver to feel the lever position more precisely.

In summary, although most commands available to a driver when operating from the TR class locomotive cabin were replicated on the transmitter, the control interface was significantly different.

The RCE transmitter display screen was a liquid crystal display (LCD). The display screen provided information to the driver of:

- direction selected
- throttle / dynamic brake notch setting

- brake pipe and control pipe pressures
- the RCE's operating mode (for both the transmitter and receiver), including fault states.

The transmitter's key switch was located on the left side of the transmitter. Its positions included:

- on (used during normal train operation)
- off
- interlock (used during loading and unloading, see below).

The RCE transmitter was attached to a vest worn by the driver when operating from the locomotive or outside the train, and placed in a receptacle when the RCE was being operated from the driver's van.

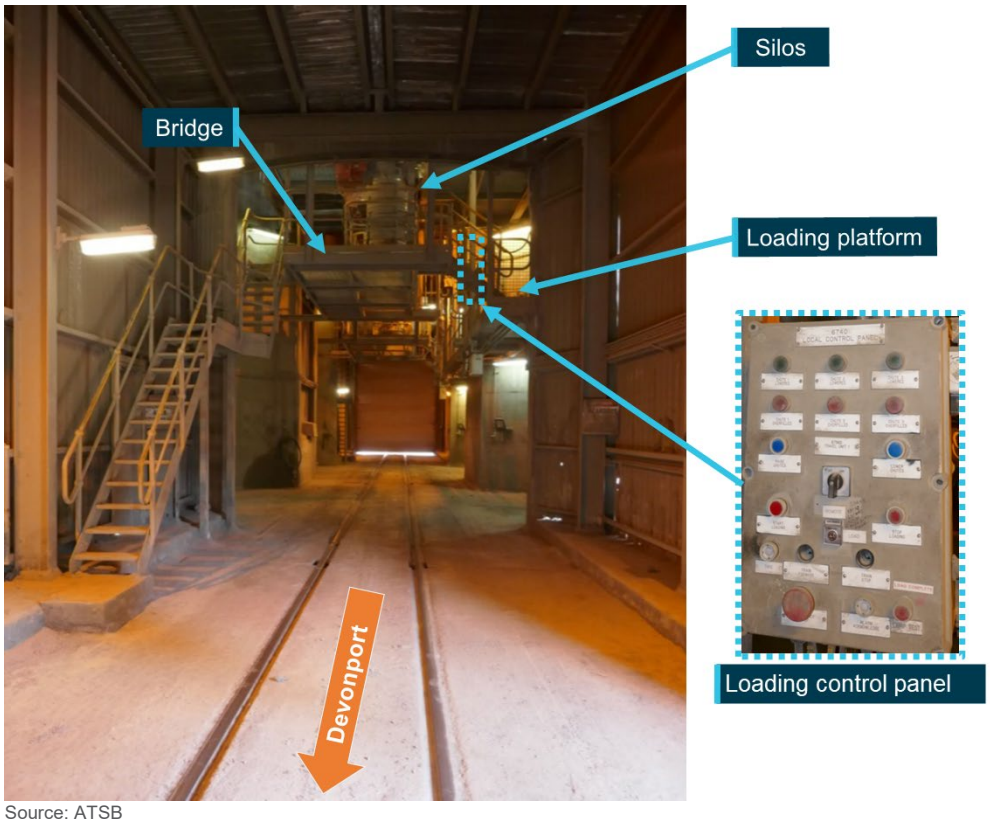
Train loading process

After the train entered the Railton loading facility, the driver would stop the train and alight from the driver's van at one end of the silos and, using the RCE transmitter, operate the train slowly past the driver, performing a general inspection and checking the bottom discharge doors were closed on the Western Line side of the train. The driver would stop the train once the inspection was complete, aligning wagons 1 and 2 under the silos in preparation for loading.

The driver would then enter the loading facility and proceed to the loading platform (Figure 14). Once there, they would:

- configure the RCE transmitter with direction in neutral, throttle idle, independent brake fully applied, and automatic brake in at least the 'initial' position
- switch the transmitter key to the 'interlock' position (activating the Railton loading interlock, which prevented train movement with the loading chutes in the lowered position)
- remove the key from the transmitter
- insert the key into the loading control panel, located on the platform, to allow loading operations.

Figure 14: Railton loading facility



Source: ATSB

Selecting ‘interlock’ allowed the transmitter key to be removed from the receiver, and also caused a minimum-service brake application (50 kPa brake pipe pressure reduction) to be applied and held on the train (see *Automatic brake*). Any manipulation of the transmitter’s controls while in ‘interlock’ mode (apart from increasing an automatic brake application) resulted in an emergency brake application.

In the event of an overshoot of the stopping mark, the train would be reversed and realigned. Due to the weight of a heavily-loaded train combined with the descending grade, if an overshoot occurred towards the end of the train loading process, it would sometimes be necessary to release the 50 kPa automatic brake application to allow re-positioning.

Once train loading was complete, the driver would walk from the loading facility to the TR class locomotive at the Devonport end of the Railton cement siding, board the locomotive and drive the train to Devonport using the RCE transmitter.

Safety design elements

Overview of safety features

The safety features in the generation 3 RCE’s design included, among others:

- emergency stop function
- vigilance function
- processor watchdog and self-reboot
- communication failed mode
- control fault mode
- failed train brake application function
- dual direction fault interlock.

In addition, the system was designed so that many faults involving the emergency stop or braking signal paths would result in venting the relevant pipe(s) to apply brakes. For example, relays and pneumatic control valves had to work correctly in order for the brake pipe not to be vented.

Emergency stop function

The RCE used electrically-controlled pneumatic valves within its air box to vary air pressure within the train’s braking system. When activated, the emergency stop mode applied emergency braking by the removal of an electrical signal to the emergency brake valve in the RCE air box. This released air at a rapid rate from the train’s brake pipe.

The emergency stop mode would normally be entered in normal operation (that is, after initialisation) when:

- the driver activated the RCE transmitter’s emergency stop switch (see Figure 13)
- the driver commanded traction with excessively low brake pipe pressure (less than 300 kPa)
- software commanded a brake pipe pressure below or equal to 450 kPa, and then sensed brake pipe pressure stayed above 480 kPa for more than 15 seconds (that is, when an attempted brake application failed); see *Failed train brake application function*.

In the emergency stop mode, the RCE receiver software would issue commands to:

- open the RCE emergency brake valve to reduce brake pipe pressure rapidly to 0 kPa (which would apply locomotive and wagon brakes)
- set control pipe pressure to 325 kPa (which would separately apply locomotive brakes)
- command the release of sand for rail-wheel friction
- command the locomotive to remove traction and set the direction to neutral.

The RCE required a functioning radio link to respond to a driver-commanded emergency stop application. ADE considered a driver’s responses to failures during the design process. It

emphasised that a driver would always have the availability of the emergency stop function, provided there was a radio link (see also *Safety integrity*).

The RCE receiver could not be triggered into the emergency stop mode with a rapid drop of brake pipe pressure (for example, as a result of brake pipe rupture during a derailment or train separation). If this occurred, the receiver would attempt to regain the last-commanded brake pipe pressure. The consequences of this are discussed further in *Reduced effectiveness of automatic emergency brake.*

Some hardware faults such as power failure would also result in a hardware-induced emergency brake application: the train's brake pipe would be rapidly vented in a similar manner to a manual activation of the emergency stop mode by the driver. The locomotive reacted to this in the same way as it did to a brake pipe rupture (as described in *Emergency brake*), sensing the resulting reduction in brake pipe pressure and acting to create its own brake pipe pressure exhaust. If the pressure in the brake pipe was low enough, the locomotive also would remove propulsion.

Vigilance function

The purpose of the RCE's vigilance function was to stop the train in the event of driver unresponsiveness (for example, due to incapacitation). On a non-remotely-controlled train, this function was controlled by the TR class locomotive. It required the driver to either acknowledge a periodic vigilance warning or make a control input to avoid entry into a penalty mode, which would result in removal of traction power and a penalty brake[40] application (called a vigilance penalty).

The RCE vigilance function required the driver to acknowledge a vigilance warning on the RCE transmitter at set time periods and it also had a penalty mode that resulted in a loss of traction power and a penalty brake application. However, the ATSB found that:

- the RCE vigilance function required a radio link to be maintained between the transmitter and receiver for it to operate
- the penalty mode, and the resulting penalty brake command and alarm to the network control centre, were inoperative when the RCE was in the communication failed mode
- the penalty mode could be reset after 30 seconds, unlike the 60-second timeout of the TR class locomotive's vigilance function (shorter reset times can result in increased in-train forces due to the time taken for braking signals to traverse the entire train).

During remotely-controlled train operations, the TR class locomotive vigilance control system was suppressed as a necessary consequence of the locomotive having to be in the 'trail cut-out' mode to accept commands from the RCE (as previously discussed under *Train information*).

Processor watchdog and self-reboot

The RCE receiver included a 'watchdog' function. The software regularly toggled one of the processor's outputs, which was monitored by an electronic circuit. In the event of a major processor hardware failure or fatal[41] software error, the unchanging signal would cause the watchdog circuit to remove power to (and thereby open) the emergency brake valve in the RCE air box, depleting air from the train's brake pipe and activating the emergency brake without entering the emergency stop mode. That is, the watchdog function was separate to the emergency stop function.

Unlike the emergency stop function, the watchdog function did not directly affect control pipe pressure, command the release of sand, or change the direction. Rather, the circuit would cause the processor to reboot and reinitialise the RCE receiver. The driver could then proceed by completing steps similar to the normal start-up sequence.

---

[40] Penalty brake: when induced, reduced the brake pipe to 0 kPa at a service rate, with an emergency alarm sent to the network control centre. The resulting locomotive brake cylinder pressure was about 350 kPa.

[41] Fatal error: a software condition or error that caused the software program to crash (stop running completely).

The receiver was not able to operate until the watchdog was activated, which happened early in the initialisation sequence. The watchdog was triggered using software timers separate from the main processing loop, so it was unable to detect 'endless loops.' Further, watchdogs are unable to detect other non-fatal software problems (that is, 'bugs' where the software continues running but does not operate as intended).

Communication failed mode

In instances where communications between the RCE transmitter and receiver were interrupted for more than 4 seconds, the receiver would enter the communication failed mode. When activated, this mode would:

- remove traction power
- reduce the brake pipe pressure to 400 kPa (an intermediate application of automatic and independent brakes)
- if the brake pipe pressure was already less than 375 kPa, set the control pipe pressure to 325 kPa; otherwise, retain the previous control pipe pressure setting
- set the direction to neutral after 10 seconds
- display 'COMF' on the transmitter display to indicate that the system was in this mode.

If communications resumed while in this mode, the receiver would not respond to any command messages from the driver (from the transmitter) other than the tilt function, emergency stop function activation and the reset command (see *Failure mode reset procedures*). These driver commands still relied on a radio message from the transmitter being received and processed by the receiver to function.

Control fault mode

In certain circumstances where the locomotive response did not replicate the driver's transmitter command, the receiver would enter the control fault mode. These conditions were:

- a throttle command mismatch
- the generator field remaining on when commanded to be off
- failure of the independent brake to apply.

In response, if the train was moving under traction power with brakes released, the receiver would, on initiation of the control fault mode, remove traction power. Then, after 10 seconds:

- set the direction to neutral
- reduce the brake pipe pressure to 350 kPa (equivalent to a full-service brake application)
- set the control pipe pressure to 325 kPa (maximum locomotive brake cylinder pressure)
- display 'CNF' on the transmitter display to indicate that the system was in this mode.

The RCE was designed to accept and respond to emergency stop commands from the driver while in the control fault mode.

Failed train brake application function

The RCE had a function that was described in the RCE operation manual as 'Failed Train Brake Application results with an Emergency Mode application of the system'. The system state required to activate this function was not described, nor was a procedure for diagnosing and correcting the condition.

ADE advised the ATSB that the fault mode resulted from the brake pipe pressure being at or more than 480 kPa for 15 seconds while an automatic brake command was in effect. That is, it resulted from a failure of either the RCE receiver or the air box to effect an automatic brake application requested from the transmitter. This was conceptually similar to the control fault mode but applied to the automatic brake. The RCE would then enter the emergency stop mode.

Dual direction fault interlock

As part of the generation 2 RCE upgrade, ADE introduced a dual direction fault interlock. The interlock created an emergency brake application by the RCE receiver (through hardware) if both the forward and reverse direction outputs were selected simultaneously, as this was believed to have occurred during a February 2010 accident (see *Operations with previous remote control equipment*).

The dual direction fault interlock was retained with the introduction of generation 3 RCE. Although present in both generation 2 and 3 RCE, the dual direction fault interlock was not described in the RCE operation manual for either system.

Independent stop mechanisms

When using the generation 1 RCE, TasRail fitted an independent remote stop mechanism external to the RCE to 4 DQ class locomotives. A button on a portable hand-held radio carried by the driver would send a radio signal to a receiver (separate to the RCE receiver) to activate the vigilance control valve on the locomotive to simulate a vigilance penalty, resulting in de-excitation of the main generator and an emergency brake application. The mechanism was not designed under recognised system safety principles (see Appendix B). It was removed by TasRail with the introduction of generation 2 RCE. TasRail advised that it relied on the RCE emergency stop function as having sufficient safety integrity (see *Safety integrity*).

In addition, ADE advised that all 3 generations of RCE were compatible with the fitment of a stop button on the locomotive, external to the RCE. If fitted and then activated, this device would cause the RCE to vent the brake pipe and remove traction power. The external stop button was not used.

Failure mode reset procedures

The RCE could be reset in 3 ways:

- resetting the transmitter and receiver from communication failed mode by configuring the transmitter (with direction in neutral, throttle idle, independent brake fully applied, and automatic brake set) and then pressing the train set button on the transmitter (Figure 13)
- resetting the receiver from control fault mode or failed train brake mode by cycling the transmitter power
- restarting the receiver completely by either cycling the receiver's isolation circuit breaker or removing and reinserting the TR class locomotive's multiple unit electrical cable into the RCE receiver.

ADE advised the ATSB that the RCE was designed to facilitate a fast communication failed mode recovery when the train was travelling at speed to avoid stopping the train.

Inspection and maintenance

The generation 3 RCE was serviced every 30 days by an external contractor at Devonport. To ensure continuity of service, TasRail had purchased 2 complete RCE units, which comprised of a receiver box, an air box and a transmitter. When the in-service unit was removed for servicing, it was replaced by the spare.

There were also requirements (from both TasRail and ADE) for the units to undergo regular in-service testing. Although some of ADE's requirements were not specified in the RCE operation manual, it had advised TasRail of these test requirements in correspondence 3 weeks after generation 3 RCE commenced operation (February 2018). The RCE in-service tests specified by ADE are compared with those that TasRail required in Table 2.

Table 2: Generation 3 RCE in-service test intervals

RCE tests	Test intervals	
	ADE advice	TasRail instruction
Vigilance function	Shift change[1]	First entering service and after locomotive shutdown[2]
Tilt function	Shift change[1]	Not specified
Emergency stop	30 days[1]	Not specified
Railton loading interlock	Not specified	30 days
General functionality: • independent brake • automatic brake • emergency stop • direction test, with power	After a cold start of the receiver (following power removal)[3]	Not specified

[1] ADE advised TasRail of these test requirements in correspondence 3 weeks after generation 3 RCE had commenced operation.
[2] A locomotive shutdown involved the engine being turned off and the battery switch opened (for example, during track closures).
[3] Specified in the RCE operation manual.

Neither the RCE operation manual or TasRail required post-failure troubleshooting or testing to occur after a communication failed mode, control fault mode or failed train brake reset. Therefore, there was no requirement to ensure correct functionality and safety of the RCE prior to continued use after a fault mode had occurred. TasRail drivers also advised that, after experiencing an RCE fault, functionality tests were not routinely conducted.

TasRail advised the ATSB that testing of the interlock at Railton was not routinely performed. Additionally, several drivers advised that the tilt function test was performed on initial RCE setup or after a locomotive shutdown rather than at shift change. The driver of train no. 604 advised that they performed the general functionality test every 7 days or after a locomotive shutdown. There were no records provided to the ATSB documenting when tests were conducted, and it is believed their performance were not routinely recorded.

Remote control equipment safety considerations

Overview

As previously discussed and detailed in Appendix A, analysis of available evidence identified that, during the accident sequence, the RCE became unresponsive to driver commands at the point of a fast direction change from forward to reverse. The RCE tried to oppose a locomotive-induced brake application after the RCE fault state cleared, and then triggered 2 emergency brake applications and releases, which did not replicate any documented fault condition behaviour.

Hardware tests after the accident indicated that there were no permanent hardware faults associated with the RCE.

Accordingly, the ATSB analysed the design, behaviour and integration of the RCE in detail using test results, design documentation, software code, interviews with ADE, and other information. During these activities, design and integration issues between the RCE and cement train consist were identified. Most of these related to the way ADE had designed the generation 3 RCE to interact with and control the operation of the braking systems outlined in *Train braking systems*.

This section discusses a range of RCE design and integration problems that ATSB testing and analysis identified.

Reduced effectiveness of some safety features

The RCE replicated several safety features that were available to a driver operating a non-remotely-controlled train. However, some of the safety features were absent or had reduced effectiveness when a driver was using RCE to control the train, and some were absent when the driver was not in the locomotive cab (that is, using the RCE from outside the train or within the driver's van). A list of safety features that were available to the driver of a non-remotely-controlled train (when operated from the TR class locomotive cab) is provided in Table 3. A comparison of whether these functions were also available under RCE control, when the driver was operating the train from specific locations, is also provided.

In addition, the efficacy of several of the safety features that were replicated during RCE operations were altered. TasRail could not provide evidence that risk assessments were performed for the absence, suppression, alteration or limited access to the safety features listed in Table 3, as a result of RCE operations (see also *Risk assessments for remotely-controlled train operations*).

Table 3: Summarised driver controls and selected safety features

	Non-remotely-controlled train	RCE operations (driver location)		
Control input / safety feature	**TR locomotive**	**TR locomotive**	**Driver's van**	**Remote from train**
Main reservoir air pressure	✓	✓	✗[6]	✗[6]
Brake pipe charging flow indicator	✓	✗[5]	✗	✗
Brake cylinder air pressure	✓	✓	✗[7]	✗[7]
Horn (high / low)	✓	✓	✓	✓[8]
Vigilance function[1]	✓	✓	✓	✓
Overspeed protection[2]	✓	✗[5]	✗	✗
Isolation switch (engine control)[3]	✓	✓	✗	✗
Emergency radio Selcall activation	✓	✓	✗	✗
Emergency engine stop button	✓	✓	✗	✗
Brake pipe emergency dump valve[4]	✓	✓	✓	✗

[1] Vigilance function marked orange: although vigilance function was available under RCE control, the vigilance system used on a non-remotely-controlled train was inactive due to the locomotive being set to 'trail cut-out' mode for RCE operation. The RCE transmitter had a vigilance function but the functionality differed.
[2] Overspeed protection was a feature of the TR class locomotives only and was not a requirement on the TasRail network or part of accreditation.
[3] The isolation switch isolated the engine from responding to electrical driver control inputs.
[4] A brake pipe emergency dump valve allowed the driver to vent brake pipe air separate from the airbrake controls.
[5] Inactive due to the locomotive set to 'trail cut-out' mode for RCE operation.
[6] The transmitter display screen would show a warning when main reservoir pressure was <700 kPa.
[7] Control pipe pressure was displayed on the transmitter display screen however, this did not accurately indicate independent brake applied brake cylinder pressure (as a result of the J-multiplier function), or brake cylinder pressure resulting from an automatic brake application.
[8] Operated the horn on the locomotive only, which was at the rear of the train when operating from Devonport to Railton.

Reduced effectiveness of automatic emergency brake

As explained in *Emergency vent valves*, the TR class locomotive's VX vent valves and emergency magnet valve (EMV) were designed to locally exhaust the brake pipe on sensing a rapid rate (emergency) brake pipe pressure reduction.[42] In addition, the locomotive's braking system would cease recharging the brake pipe. These actions assisted propagation of both driver-commanded

42 See *Automatic brake* for an explanation of the function of these valves.

and uncommanded emergency brake applications. Further, once the brake pipe pressure was less than about 297 kPa, the locomotive would activate the power control switch (PCS), removing all traction power.

The ATSB found that the RCE receiver would not recognise brake applications (including emergency applications) it did not command. Instead, it would oppose uncommanded reductions in brake pipe pressure (for example, as the result of a derailment or train separation) and attempt to restore the brake pipe pressure to 500 kPa. As a result, following an emergency brake application at the driver's van, the locomotive's emergency brake response would not activate. Tests conducted by the ATSB by making an emergency brake application from the driver's van without the RCE fitted also showed that, even without the RCE opposing the brake pipe pressure drop, there was insufficient pressure drop at the locomotive to activate the locomotive's emergency brake response.[43] Tests of emergency brake application at the driver's van with the RCE active resulted in the following effects:

- the driver's van almost immediately enacted an emergency brake activation as a maximum service brake application at the front of the train
- it took about 40 seconds for a minimum-service application to take effect at the locomotive
- the brake pipe pressure at the locomotive remained above 425 kPa after 60 seconds
- the locomotive's VX vent valves and EMV did not activate
- the locomotive did not invoke the locomotive's power control switch (PCS).

Had there been an event where the driver activated the driver's van emergency brake (for example, during a fail-to-unsafe event of the RCE) with the locomotive propelling under traction power, it would have been largely ineffective. As such, the 108-t locomotive would have remained under traction power pushing into 18-t empty wagons with high braking force at the driver's van and reduced wagon braking force closer to the locomotive. As explained in *Propelling operations*, the resultant buff forces originating from the rear of the train consist would have caused increased lateral force against the rail head and a reduction in wheel load, increasing the risk of a mid-train jack-knife derailment.

Unintended emergency brake application and release

ATSB tests showed that either of the following 2 actions resulted in uncommanded emergency brake applications that would clear without driver intervention:

- rapid RCE automatic brake commands past the minimum service position (when the train was configured as a light engine)[44]
- rapid movement of the RCE direction controller to the opposite direction.

The rapid decrease in brake pipe pressure resulted in an emergency brake application due to activation of the locomotive's VX vent valves and, in turn, EMV. In addition to assisting the brake pipe pressure drop, the locomotive's airbrake system would activate the locomotive's power control switch (PCS), removing the locomotive's traction power.

In this scenario, the RCE would not recognise the brake pipe venting and continue to attempt to recharge the brake pipe, as explained in *Reduced effectiveness of automatic emergency brake*. This would then lead to the brakes being released after the initial application.

A rapid brake command past the minimum service position was only observed to result in an emergency brake application when the train was configured as a light engine. This was very likely due to the greater volume of brake pipe air from a train consist leading to a slower reduction of brake pipe pressure during venting, preventing a trigger of the locomotive's VX vent valves.

---

[43] For a non-remotely controlled train, a driver could detect a brake pipe rupture at the rear of the train using a brake pipe charging flow indicator in the locomotive.

[44] Light engine: one or more locomotives coupled without wagons attached.

However, a fast direction change could result in an emergency brake application in any configuration (that is, with the locomotive leading the consist, trailing the consist, or configured as a light engine). The fast direction change resulted in a momentary trigger of the dual direction fault interlock, which rapidly exhausted brake pipe pressure.

When the test was conducted with the RCE integrated into the TR class locomotive, the momentary exhaust created a pressure reduction rate in the brake pipe sufficient to trigger the locomotive's VX vent valves. This subsequently activated the EMV on the locomotive and both continued to vent the brake pipe after the initial RCE fault had cleared.

When the ATSB tested the RCE in isolation on a passive test bench, the momentary exhaust of brake pipe air through the RCE emergency brake valve caused little pressure loss and the desired brake pipe pressure was quickly restored (that is, the response on the test bench was different to that on a train). Similarly, ADE reported that the condition could not be replicated during later bench testing.

ADE mistakenly believed VX valve activation was caused through an electrical command by software (in fact it was through rapid automatic brake pipe pressure reduction). ADE reported that it did not have any information in relation to the VX vent valves.

The issue of uncommanded emergency brake applications on light engines was highlighted to TasRail in correspondence by ADE in April 2018, and this integration concern was communicated in an email to RCE drivers in the following month.

Wheel locking in communication failed mode and later reduction of braking effectiveness

When using generation 2 RCE, if the radio link was lost when the train was moving under traction power with brakes released, the RCE receiver would (among other things) apply 325 kPa control pipe pressure and reduce the brake pipe pressure to 350 kPa (full service). Although this worked well with the DQ class locomotives, the communication failed mode was causing skidding and flat wheels on the then-new TR class locomotives. The TR locomotives had been introduced at the same time as new wagons (from HE class to THFY class), and it was suspected that the skidding problem was associated with the resulting changes in the braking system from the previous locomotive and wagon types.

ADE diagnosed the cause of the skidding problem to be the rapid exhaust of brake pipe pressure by the air box, which was activating the TR class locomotive's EMV, resulting in an emergency brake application.

In response, ADE changed the communication failed mode response in generation 3 RCE. Under the new response, the RCE would now reduce the brake pipe pressure to 400 kPa (less than a full-service application) and only set control pipe pressure to 325 kPa if it was already less than 375 kPa when the communication failure occurred (otherwise it would maintain the current control pipe pressure). There were no reports of locomotive flat wheel events related to communication failed mode events after the changes were implemented.

The TR class locomotive, unlike the DQ class locomotive, had an electronic brake control system. A feature of the system was the ability to apply increased locomotive brake cylinder pressure in response to control pipe pressure, known as the 'J-multiplier' effect. When the control pipe was charged to the maximum of 350 kPa, the locomotive brake cylinders would be charged to about 550 kPa.

Under the generation 2 RCE penalty mode, when the receiver entered the communication failed mode and commanded a maximum of 325 kPa in the control pipe, the TR class locomotive electronic brake control system responded by applying 520 kPa to the locomotive's brake cylinders. This brake cylinder pressure (520 kPa) was about 50% higher than what would be achieved during an automatic brake full-service application (that is, 350 kPa). The full-service

brake cylinder pressure was designed to be the highest level achievable on the TR class without risk of wheel lock in normal conditions.

Therefore, the ATSB found that the likely reason for the reported locked wheels was that the generation 2 RCE communication failed mode applied a significantly higher pressure in the locomotive brake cylinders than the maximum brake cylinder pressure that could otherwise be made (520 kPa vs 350 kPa).[45]

Further, testing conducted by the ATSB showed that an unintended emergency brake application could occur on a light engine, but not when the locomotive was attached to a train as was being reported. This explains why ADE's change to control pipe behaviour during the communication failed mode response prevented the generation of unintentionally high locomotive brake cylinder pressures and corrected the issue of flat wheels.

Uncommanded release of light engine automatic brake applications

As discussed previously, when configured as a light engine, rapid RCE transmitter automatic brake commands past the minimum service position resulted in unintended activation of the locomotive's VX vent valves and (in turn) EMV. This resulted in an uncommanded emergency brake application. The RCE's attempts to attain the selected brake pipe pressure would result in a partial release of brakes on a light engine. A full release was avoided due to the RCE seeking a pressure of 65 kPa in the control pipe during an automatic brake application.

The ATSB observed further issues during testing of the communication failed mode. In circumstances of a released independent brake at the initiation of a communication failed mode event, as may occur during light engine shunting operations, no control pipe pressure was commanded by the RCE. As a result, the restoration of the brake pipe pressure to 400 kPa after the uncommanded emergency brake application, which happened automatically, resulted in the release of the locomotive's brakes as the brake pipe pressure rise was a valid automatic brake release command. That is, although the transmitter displayed a brake pipe pressure of 400 kPa to the driver (indicating a brake application was in effect), the locomotive's brakes would be fully released.

Uncommanded release of wagon brakes

Following a locomotive engine restart after an automatic engine shutdown,[46] there would be a momentary loss of electrical power that would result in a cold start of the RCE (in the same way as cycling the power). The RCE receiver would power down, resulting in the brake pipe being vented and the brakes being applied across the train. When electrical power was restored, the RCE would restore the brake pipe from 0 kPa to that commanded by the driver on initialisation (for example, 350 kPa or full service). The brake pipe pressure rise was similar to a valid automatic brake release command and therefore resulted in a full brake release on all wagons.

In this situation, the RCE transmitter display screen would show restoration of brake pipe pressure to the driver's originally commanded automatic brake application (that is, less than 500 kPa), indicating to the driver that the wagon brakes were still applied.

As the independent brake was fully applied during a cold start / engine restart after automatic engine shutdown, a train runaway was normally prevented.

Uncommanded release of locomotive independent brake

Dynamic brake control was an addition to the generation 3 RCE that had not been present in previous generations. Shortly after introduction, drivers found that engaging dynamic brake on the

---

[45] The J-multiplier had no effect on a non-remotely-controlled train, because the control pipe would not be pressurised. Therefore, locked wheels would not occur in this situation.

[46] The TR class locomotive would perform an automatic engine shutdown (enter sleep mode) after a 15-minute period of control input inactivity provided certain conditions were met (for example, the train was stationary).

transmitter would result in an uncommanded release of the locomotive's independent brake. This was a design feature of the TR class locomotive that, ADE advised TasRail at the time, was replicated by the RCE.

The feature to which ADE was referring was the 'dynamic brake interlock' function. On application of dynamic brake, this function would release service rate brake cylinder pressure on the locomotive that was applied by the automatic brake (in order to prevent wheel lock). The locomotive dynamic brake interlock would not release brake cylinder pressure applied by the independent brake, while the RCE did release with independent brake application.

The effect of this integration issue was the potential for a train, being held stationary by the independent brake on a gradient, commencing to roll away uncommanded when dynamic brake mode was selected (for example, after completion of loading at Railton).

RCE dynamic brake was suspended from use by TasRail at the time of the 21 September 2018 runaway due to an unrelated issue (see *Issues after commissioning*).

Remote control equipment emergency brake reset

As previously discussed, the air box was relocated to the rear of the locomotive with the introduction of the TR class during generation 2 RCE (see Figure 12). This resulted in a greatly increased recharge rate of the brake pipe at the locomotive (smaller pipe air volume forward of the air box) compared to the rest of the train's brake pipe (larger pipe air volume behind the air box).

Testing conducted by the ATSB found that, on a non-remotely-controlled train of 220-m length, the locomotive registered a brake pipe rise from 0 kPa to 495 kPa in 49 seconds. On the 220-m long cement train with the RCE supplying air from the back of the locomotive, the same pressure rise for the locomotive took only 16 seconds. Although the recharge rate at the locomotive increased, the recharge of the brake pipe on the trailing portion of the train was not proportionally increased.

In effect, this meant that traction power, which was deactivated once the brake pipe pressure had risen sufficiently, could be regained much sooner on a remotely-controlled train than on a non-remotely-controlled train. Once this had occurred, the driver could reapply traction power.

In addition, the TR class locomotive's braking system prevented a reset of both driver-commanded and uncommanded emergency brake applications for 60 seconds. This ensured the train came to a complete stop before a brake release was attempted, which prevented excessive draft forces and possible train separation, as explained in TasRail's train handling manual. Conversely, the RCE allowed a reset of the transmitter's commanded emergency brake application in less than 30 seconds by cycling transmitter power.

In combination, the faster reset of the traction power inhibition once the brake pipe began recharging, and the faster pressure rise at the locomotive, resulted in a significantly shorter time between when the emergency brake application occurred and when power could be reapplied. The reduction was from about 1 minute 49 seconds on a non-remotely-controlled train to 46 seconds on the cement train fitted with generation 3 RCE.

Allowing the reapplication of traction power in a shorter time reduced the protection against excessive draft forces. The reduced time was likely to have been faster than the time required to release the fully-applied automatic brake along the remaining length of the train, raising the possibility of having the locomotive pull against applied wagon brakes, further increasing draft forces.

Software design

There was no documentation associated with the RCE's software, apart from limited comments in the software code (which sometimes contradicted the code).

An ATSB review of the code indicated that a state could exist during initialisation where the receiver would not do anything other than maintain previous commands. Specifically, there were several initialisation tests which, depending on certain conditions or in the event of a single

hardware or memory fault, had the potential to enter an endless loop (that is, the receiver could 'hang') without entering a fault state. Among the conditions that would result in this behaviour during initialisation were when the RCE receiver detected a non-neutral direction, measured train brake pipe pressure above 470 kPa,[47] or measured independent brake control pipe pressure below 300 kPa.

In this state, the receiver would not issue new commands in response to driver inputs, and would not enter fault states such as the communication failed mode. Recovery from this state was only possible through external correction of the conditions that caused it (such as the train brake pipe pressure dropping below 470 kPa via an external means). Even if power was cycled, the RCE would re-enter this state if the external condition remained unchanged.

ATSB review of the software indicated that the functions to set the train and RCE in a desired initialisation state (such as a set brake pipe pressure or direction selection) were not called before this loop, although this could not be tested.

Other issues identified during ATSB testing

In addition to several integration and design problems identified between the RCE and a train consist, the ATSB also noted the following instances of uncommanded (that is, not the result of driver input) locomotive behaviour during testing (see Appendix A) and subsequent review of the recorded data:

- The locomotive registered multiple instances of uncommanded dynamic brake activation, or light traction motor current, sometimes in conjunction with an electrical control fault mode occurrence.
- During one instance of an electrical control fault mode occurrence after conclusion of an uncommanded dynamic brake activation, the engine speed increased and the generator field activated in conjunction with light traction motor power. However, the direction controller had remained in the neutral position during this time. That is, these commands were not the result of driver inputs.

The ATSB could not determine the origin of these uncommanded dynamic brake and light traction motor currents. However, the ATSB noted:

- the uncommanded dynamic brake activations were not observed during periods when the RCE was not active
- the uncommanded light traction motor currents were still observed shortly after the RCE was made inactive.

Caroline Creek event

The ATSB also reviewed driver reports of faults (see *Fault reporting process*) and related information to identify any potentially similar events involving the generation 3 RCE to that which occurred at Railton on 21 September 2018. There were several events which indicated anomalous RCE behaviour. The most significant of these occurred at Caroline Creek in May 2018.

At 2214 on 8 May 2018, a network control officer (NCO) received an emergency alarm from cement train no. 311 while en route from Devonport to Railton. The driver advised the NCO that they had received an RCE emergency penalty and were attempting to reset it.

When several attempts to reset the transmitter had failed to restore control, the driver determined that the receiver would need a cold start to reset the fault. However, the cement train was straddling the Caroline Creek bridge, which had no walkway fitted. This meant that the driver, who

---

[47] The RCE operation manual provided conflicting advice, stating that the brake pipe pressure must be below 370 kPa during initialisation on page 10, or below 475 kPa on page 27. The ATSB reviewed this section of software code and observed that the actual pressure coded into the software was 470 kPa.

was positioned in the driver's van at the front of the train, required someone to attend the locomotive at the rear of the train to perform a cold start of the RCE receiver.

At 2237, the driver advised the NCO:

> …no good here I'm afraid, I can't get this thing to build up brake [pipe pressure] or anything. It builds up about 300 kPa of brake pipe pressure then it'll drop out, then I try and reset it and it goes to control faults [control fault mode], then it'll come back up again [brake pipe pressure] then it goes to control failures [control fault mode].

At about 2242, while assistance for the driver was being arranged, one attempt at a reset of the fault was successful, for reasons that were unclear. The cement train continued the journey to Railton shortly afterward.

As the event resulted in significant delay to the cement service, TasRail contacted ADE for assistance in identifying the fault condition. ADE replied that for a suspected control fault mode to reset, the following was required:

- clearance of the fault condition causing the control fault mode
- brake pipe pressure at or below 350 kPa (full service or greater)
- control pipe pressure over 300 kPa.[48]

TasRail subsequently provided ADE with a screenshot of the locomotive's recorded data from the event and a copy of the verbal conversation between the driver and NCO to assist in diagnosis of the cause that had resulted in the suspected control fault mode event. TasRail advised the ATSB that ADE later gave a sufficient verbal explanation for the event, which led to continued use of the RCE. No records were provided to detail what this explanation was and ADE later advised the ATSB that the cause of the vent could not be determined with certainty.

Analysis of the event at Caroline Creek event was conducted by the ATSB. The analysis utilised data recorded on the locomotive during the event and the information recorded during the driver's interaction with train control on the day. The ATSB identified that during the event:

- The train experienced an uncommanded emergency brake application followed by rapid and repeated brake pipe and brake cylinder pressure fluctuations. These observations were not consistent with any fault condition behaviour documented for the RCE.
- The generation 3 RCE likely released the independent brake and attempted to recharge the brake pipe on multiple occasions.
- The brakes remained applied on the locomotive due to systems external to the RCE; specifically, the locomotive's electronic airbrake system held locomotive brake cylinder pressure until brake pipe pressure rose above 350 kPa.
- Had the RCE successfully continued to increase the brake pipe pressure above 350 kPa in the absence of control pipe pressure, the locomotive brakes would have released without command, leaving the train in an un-braked state.
- The unknown fault condition was cleared by an uncommanded automatic locomotive engine restart, which likely cold-started the RCE receiver. Upon resumption from the cold start, the receiver did not resume the unknown fault condition and subsequently began accepting control messages from the transmitter.

Both the behaviour of the generation 3 RCE while a fault state was present (attempting to remove independent brake applications and recharge the brake pipe), and that external systems were required both to maintain locomotive brakes and cold start the RCE receiver, are indications that the RCE had entered a potentially unsafe state.

---

[48] The generation 3 RCE operation manual advised that to reset a control fault mode 'Reset Transmitter key switch OFF & ON'. There was no mention of required brake pipe and control pipe pressure conditions to be met. See *Driver training*.

Other selected fault events

In addition to the event that occurred at Caroline Creek on 8 May, the ATSB conducted analysis of recorded data from other selected generation 3 RCE fault reports from drivers. Reports were selected on the basis of driver descriptions of RCE behaviour that could not be readily attributed to a defined failure mode or response. These are summarised below:

- 16 February 2018: The driver reported mismatches between RCE transmitter display and locomotive display (likely transmitter screen freezes), commanded brake releases not effected by the RCE, slow response by the RCE to commands, and multiple communication failed mode events during their shift.

  ATSB analysis: Recorded data indicated that at least one of the reported communication failed mode events was likely a control fault mode event, based on the observed brake pipe pressure response. There was insufficient information available to identify the reports of mismatch between RCE and locomotive displays and between driver command and system response (brake releases not effected and slow response).
- 21 February 2018: The driver initially reported a non-descript RCE fault, and later advised that continued use of RCE was 'unsafe' after inability to reverse the consist.

  ATSB analysis: Recorded data showed direction returning to 'centre' (loss of direction selection while train was in motion with throttle applied). After the train had stopped, multiple instances of high throttle notch without direction selection occurred, corresponding to the time of the initial report. As the direction was in neutral, no traction power was applied. Further instances of throttle applied without direction selection occurred prior to the second report. No reason for the initial loss of direction, or subsequent non-applied direction, could be observed from the recorded data as the direction commanded by the driver on the RCE transmitter was unknown.
- 13 April 2018: The driver reported that the train had come to an uncommanded stop requiring a full locomotive and RCE restart to recover, and subsequently slow RCE response to driver commands while loading.

  ATSB analysis: Recorded data showed that the uncommanded stop was likely due to a RCE communication failed mode event (based on brake pipe and brake cylinder pressure behaviour). The slow response to RCE commands could not be directly observed as commands were not recorded. However, multiple instances of maximum throttle settings and high traction motor amperage, with no associated train movement, were observed during loading and therefore likely corresponded. There appeared to be attempts by the driver to reset dragging wagon brakes through the application and release of full-service automatic brakes. It is unclear whether this was related to or resolved the issue the driver reported.
- 19 May 2018: The driver reported an uncommanded emergency brake application with simultaneous uncommanded horn operation.

  ATSB analysis: Multiple instances of emergency brake pipe pressure decreases were observed. The reason for these system behaviours could not be determined from the available data.
- 3 June 2018: Multiple reports. An emergency Selcall received by the network control officer, and the driver reported the train had stopped while en route with a fault (initially reported as a control fault mode event then as multiple communication failed mode events).

  ATSB analysis: Although the RCE was capable of requesting the locomotive to send emergency Selcalls, the activation parameter was not recorded. There were no brake pipe reductions recorded consistent with an emergency or vigilance penalty corresponding to the time the Selcall was received. Multiple events, consistent with the RCE communication failed mode (based on brake pipe and brake cylinder pressure behaviour) occurred while the train was en route over a half-hour period, corresponding to the time of the driver's report.

In addition, a review of the RCE driver fault reports found 25 references to uncommanded emergency brake applications or alarms being reported. In at least 8 of these, the train incurred an

RCE-induced emergency penalty without driver command. The reasons for these were not determined, and were not found to be the result of any emergency penalty condition described in the RCE operation manual or the failed train brake application fault mode.

The data recorded for these events was limited (see *Effect of non-recording of remote control equipment data*), so confirmation of reported faults was generally not possible.

Summary

In summary, the ATSB testing and analysis identified several design and integration problems associated with the generation 3 RCE, including problems that could result in unintended brake application and unintended brake release.[49]

Apart from the uncommanded independent brake release during the use of dynamic brake and reduced communication failed mode braking, neither TasRail or ADE had identified any of the other RCE integration and design problems. Further, for these 2 problems that had been identified, Tasrail could not provide any evidence that a risk assessment was performed to assess the impact and immediate effect they may have had on the safety of its RCE operations (see also *Risk assessments for remotely-controlled train operations*).

Remote control equipment development

Overview

Given the problems identified with the RCE's design and integration, the ATSB investigation examined aspects of the RCE's design and development process.

The Rail Safety National Law (RSNL) (see *Relevant legislation)* stated that rail safety was a shared responsibility between various parties, including designers / manufacturers and rolling stock operators (as well as other parties such as rail safety workers and the regulator).[50] The RCE manufacturer was Air Digital Engineering (ADE). TasRail was the rolling stock operator that commissioned and then used the RCE.

Rail safety duties applicable to designers, manufacturers and suppliers of rolling stock were contained in section 53 of the RSNL. It stated in part that, so far as was reasonably practicable, rolling stock:

- was safe for its intended use
- was tested and examined to ensure safety for its intended use
- had information available for its correct use, including any conditions
- had results of testing and examination available.

Rail safety duties applicable to rolling stock operators were contained in section 52(4) of the RSNL. It stated that a rolling stock operator must ensure, so far as is reasonably practicable, a number of things including:

> (a) the provision or maintenance of rolling stock that is safe; and
>
> (b) that any design, construction, commissioning, use, modification, maintenance, repair or decommissioning of the operator's rolling stock is done or carried out in a way that ensures safety …

---

[49] In addition, other problems were identified during operations; see *Issues after commissioning* and *Remote control equipment fault reporting.*

[50] The RSNL also stated that the level and nature of responsibility that a party had for rail safety was dependent on the nature of the risk to rail safety that the party created from the carrying out of an activity (or the making of a decision) and the capacity that party had to control, eliminate or mitigate those risks.

This section of the ATSB report provides a background on ADE. It also details aspects of the design process for the RCE and the relevant ADE and TasRail interactions and activities throughout the development of the generation 3 RCE.

Information about the service history of the generation 3 RCE is provided in *Issues after commissioning* and *Remote control equipment fault reporting*. Information about TasRail's management and oversight of the generation 3 development project is provided in *TasRail change management and related processes*. Further information about regulatory background and oversight is provided in *Regulatory oversight*.

Manufacturer information

ADE is a small Australian-based company specialising in the design and manufacture of RCE used to control railway locomotives. Throughout development of the 3 generations of RCE, the company primarily consisted of one person, who owned the company, and conducted most of the hardware design, manufacture, and customer liaison work. Other individuals were utilised on an as-needs basis, such as a programmer who developed software code for the generation 3 RCE, and an electronics company in Devonport that was subcontracted to provide local maintenance support for TasRail on behalf of ADE.

External guidance

In 2005–06, the United States Federal Railroad Administration (FRA) published a series of reports addressing the risk of remotely-controlled locomotive operations in general (FRA 2005, 2006a, 2006b, 2006c). At the time there were 'limited' remotely-controlled main-line train operations (FRA 2005), so the reports primarily addressed yard operations. Collectively, these reports highlighted a range of different risks, notably situation awareness, operator training and procedures, equipment reliability, and radio security.

There was a broadly similar accident rate in yard operations between remotely-controlled trains and conventional (non-remotely-controlled) trains in the United States (FRA 2005). Injury rates tended to be lower in remote operations, which was proposed to be the result of a reduction in crew size.

FRA (2005) discussed system response to a loss of radio communications, stating concern about the amount of control afforded to the driver in such situations:

> For example, there have been incidents in yards where the [remote controlled train] suddenly stopped because of communication failure and caused a section of the cars being handled to break away. In one instance these cars rolled into the side of a train, causing a derailment. To have such occurrences on high-speed main tracks could prove catastrophic. FRA recognizes that penalty brake applications can and do occur to engineers [drivers] during conventional main track operations. However, the engineers have the ability to immediately respond to these situations with considerably more controls than those afforded to [remote controlled train operators].

Likely in part due to the limitations of the available equipment at the time in the United States, the FRA recommended limits on locomotive power, train length, speed, and grades for remotely-controlled trains, effectively recommending their use be limited to yards and short distances.

There were no design standards or guidance documents specifically developed for the design of RCE for trains. However, there are standards and guidance documents to aid in the system safety approach for rail systems (see Appendix B).

Safety integrity

Software integrity level and Australian Standard 61508

Functional safety is a concept relating to the need for a system to function correctly to maintain safety. Australian Standard (AS) 61508 (*Functional safety of electrical/electronic/programmable electronic safety-related systems*) is a functional safety standard. It provided suppliers of

components and subsystems with complete life-cycle processes to optimise system safety through risk-based and performance-based measures (see Appendix B).

Safety integrity was defined by AS 61508 as 'the probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.' The concept of 'safety integrity level' (SIL) was used by a number of standards, including AS 61508 and EN 50126.[51] Generally, SIL was a number specifying the safety integrity requirements of safety functions of a system. AS 61508 defined SIL ranges from 1 (the lowest defined level of safety confidence) to 4 (the highest).[52]

In correspondence with TasRail in February 2018, ADE stated:

> The [RCE] is designed with failsafe features following AS61508.

ADE reported that the RCE had always been designed with the objective of being fail-safe; that is, so that any hardware or software failures would always result in a safe state. TasRail advised the ATSB that, in relation to this aspect and the design of the RCE more broadly, it (as a consumer) necessarily placed significant reliance on the supplier's skill, expertise and representations.

The pre-delivery and commissioning testing report for the generation 3 RCE, dated 8 January 2018, defined 'safe state' as:

> Disabled propelling [traction] and brakes applied.

ADE later advised the ATSB:

> The emergency stop function on the Transmitter has always been the critical safety function that must work when required provided it is used at the correct time. In support of this claim, attached is the SIL testing documentation (Estopsil) undertaken in 1999 when the systems were designed and tested in accordance to AS61508. The philosophy of the design then has not changed relating to the use of Emergency Stop function.

The document referenced by ADE was *Estopsil* (an abbreviation of *Emergency Stop SIL*), authored by ADE and dated April 1999. The document described the assessment of safety of the emergency stop function of an RCE system developed in 1997, which was presumably the generation 1 RCE provided to TasRail in 1999. It was the only formal document produced that was relevant to the claim of design and test in accordance with AS 61508. The 31-page document contained information relating to a 'safety integrity level' (SIL) of the emergency stop safety function.

ADE also referred to a SIL in the generation 3 RCE operation manual:

> The safety functions that exist and operate within the equipment are provided for the maximum safety integrity level of the remote control equipment.

Although it is almost certain that the generation 3 RCE software was tested to some extent, there were no records of what was tested and to what extent. Records that were provided by ADE related to the generation 1 RCE.

Safety integrity scope

ADE's application of AS 61508 was primarily applied to the emergency stop function (described in *Emergency stop function*), with limited information about the RCE's other functions and processes.

The February 2018 correspondence from ADE to TasRail stated:

---

[51] EN: European Standard. Further information about EN 50126 *Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)* is provided in Appendix B.

[52] Under AS 61508, the 'risk reduction factor' (allowable probability of dangerous failure per hour) for equipment used continuously was equivalent to an allowable average of 0.1–1 million hours operation without a dangerous failure for SIL 1 and increasing by a factor of 10 for each subsequent SIL, up to 100–1,000 million hours for SIL 4.

> The primary safety mechanism relating to the AS61508 Safety Integrity Level is the Emergency Stop function.
>
> The Emergency Stop operation meets SIL 2 and SIL 3 provided it is tested periodically not more than 30 days for a high usage demand mode which the equipment would come under.

The *Estopsil* document contained:

- assessments of the dependability of the emergency stop function
- a flowchart of the software development process (which did not include any risk or safety analyses)
- a radio communications state diagram
- a table providing 'alternative pathway[s] that would be used' in the event of failure (for radio failure, the alternative was 'emergency stop or redundant radio').

The assessment did not consider external factors that could prevent the emergency stop function from working (such as radio communication, software, or hardware failures).

Assumption of acceptable dangerous failure probability

The *Estopsil* document stated an assumed acceptable dangerous failure probability of 1% per year of operation. There were no records indicating whether TasRail provided this as a specification to ADE, was informed of ADE's assumption, or later accepted this nominal safety acceptance criterion and assimilated it into its broader safety management system.

Software assessment

In relation to software modules associated with the generation 1 RCE, the *Estopsil* document stated:

> To test every [software] module individually for the preparation of this particular document is an impractical task for the following reasons:
>
> - Necessity to provide documentation at some point in time (preferably sooner) of testing the safety functions required to operate on demand in dangerous conditions rather than safety functions that continuously operate in high visible form.
> - To provide accurate calculation and the validation of the probability of a dangerous failure per operational hour.
> - In this case, it is believed more advantageous to collectively test a system with mainstream module structure and commonality of hardware.
> - The selection of the Emergency Stop to be tested was based on the fact that this single function is designed and displayed to the equipment user as the most effective means to generate a safe state from a potential dangerous state. This safety function is not uniformly cyclic as is others within the equipment and in judgment of these criteria this function becomes the subject of a targeted failure measure in both high & low demand mode of equipment operation.

Overall safety integrity assessment

The *Estopsil* document applied some concepts and methods from AS 61508 to the generation 1 RCE. The document stated:

> There is validity to the question that although any equipment has been tested in correct operational state, how reliable would any safety function be given that under fault conditions of predetermined foreseeable failures of system components, the safety mechanisms designed into the E/E/PE[53] equipment fail to protect as intended or render the E/E/PE in a dangerous state.

[53] E/E/PE: electrical/electronic/programmable electronic safety-related systems.

> In realistic term, to address these matters, reference has been drawn from the Australian Standard 61508 and various parts that allow a determining factor to be assessed of what is now accepted and termed a Safety integrity Level (SIL)…
>
> The documentation provided herewithin contains only relative information to performance of the safety function being tested and does not include explicit detail such as part numbers, circuitry structure, detailed software code or similar. Most of these items are a variable format on a system by system basis, however the pathways of execution remain somewhat consistent.

The document indicated that tests had been performed in support of reaching the SIL determination, recorded to have taken place on 1 December 1997 and 1–11 March 1999. The tests included the following:

- analysis of the effects of various faults in hardware logic related to the emergency stop function
- a test involving 'catastrophic' (complete) failure of the radio module, including power loss, which would result in an emergency stop activation. This was later contradicted by a communications flow chart that did not include this functionality.
- a test that concluded that 'a failure of the software component results in [activation of the hardware-induced emergency stop function] due to the watchdog not being acknowledged'
- an assessment of hardware reliability, which provided incomplete data related to failure rates, failure modes, and diagnostic coverage.

The document used some elements of the standard to perform basic analysis of the emergency stop function. It contained no information or evidence about the application of AS 61508 throughout the system's life cycle. For example, there was no assessment of the potential consequence of equipment failure or an evaluation of development practices against the recommended and highly recommended practices for each SIL defined in the standard.

The *Estopsil* document included notes about prospective design changes, such as the following:

> Initial test'g showed need to split double h/w opts to spread dependency from single h/w IC to two.[54] This can be done @ syst. design phase.

There was no explanation for why this change was necessary (for example, whether it exceeded some nominal failure rate maximum). There was also no information regarding whether the change was implemented, or whether doing so addressed the underlying problem.

Other than the 1999 *Estopsil* document there were no other records that would necessarily result from a design process complying with AS 61508, such as requirements specifications, hazard and risk analyses, and a safety case. This was the case for the generation 2 and generation 3 RCE as well as the generation 1 RCE.

In summary, ADE used elements of a system safety standard, AS 61508, to estimate the reliability of the emergency stop function for the generation 1 RCE in 1999 but this was not equivalent to having developed the equipment to that standard. The generation 3 RCE incorporated new functions, software, and radio and microprocessor hardware (see *Differences from previous generation*). Although such changes would necessitate re-analysis, there was no documented evidence that this was conducted.

Operations with previous remote control equipment

As previously noted, ATN Tasrail trialled ADE's generation 1 RCE in 1999. ATN Tasrail's planning manager (who was a qualified train driver) operated and tested the generation 1 RCE on the cement train for 4 months. Following these trials, ATN Tasrail commenced using the RCE. All Devonport cement train drivers were trained in its use, with a designated pool of drivers later formed under the supervision of the planning manager. TasRail personnel advised the ATSB that RCE operations initially operated in conjunction with a 2-person crew configuration to allow

[54] This probably means changing a signal path so that it passes through 2 integrated circuits (chips) instead of one.

familiarity, before changing to a driver only operation configuration. The planning manager retained supervision of the RCE driver team until a restructure in about 2009.

Generation 1 RCE operated without serious incident from its commencement in late 1999 until February 2010, when the RCE failed to an unsafe state. At the conclusion of a light engine movement, the driver brought the engine to a stop by applying full independent brake, removing traction power, and placing the direction controller in neutral. Shortly afterwards, the DQ class locomotive commenced an uncommanded powered movement while sounding the horn and dropping sand. It travelled in reverse for 150 m before colliding with a rake of stationary cement wagons at 15 km/h and continued to push into the stationary wagons after the collision. The driver took evasive action, including applying the emergency brake and switching off the transmitter but these actions had no effect. To stop the locomotive from continuing to power into the wagons, the driver removed the multiple unit plug from the receiver (on the locomotive) to cease the traction power command.

Subsequent investigation by ADE attributed the accident to an electrical short from a stray piece of metal within the receiver, causing all outputs through the multiple unit plug to be erroneously active. Issues with stray voltage to ground through the RCE antenna due to damaged cable insulation were also found. As a result, ADE introduced the dual direction fault interlock function into the generation 2 RCE.

As previously noted, TasRail replaced the generation 1 RCE with generation 2 RCE in about August 2010. After this period and until the generation 3 RCE project, TasRail did not have a nominated responsible person or team for the management of the RCE operation. TasRail advised that a shift from individual responsibility to departmental responsibility was consistent with modern practice.

Generation 3 remote control equipment project initiation

In early 2015, TasRail identified issues with decreasing reliability of generation 2 RCE. It initiated discussion with ADE regarding an increased maintenance regime to extend the RCE's operational life. However, ADE advised TasRail that generation 2 RCE could no longer be supported going forward due to discontinued manufacture of the transmitter and receiver microprocessors.

As a result, TasRail staff researched RCE replacement options. In consideration of these options, it was decided to approach ADE for a replacement, described by one involved TasRail employee as '…a like for like replacement of the existing [RCE]', including additional options.

In late May 2015, ADE provided TasRail a quote for one new RCE unit sourced externally (from a United States-based manufacturer), as ADE was reluctant to manufacture its own product due to the level of work involved. The externally-sourced RCE was substantially different to the ADE-manufactured generation 2 RCE.

In November 2015, funding became available for TasRail to purchase the new RCE, at which time a further quote was requested from ADE, with the addition of dynamic brake control via the RCE (see *Dynamic brake*) added to the required functionality. ADE provided the requested quote, again with RCE sourced externally, with a 12-week turnaround period. A GPS speed restriction option was also offered at additional cost.[55]

In late 2015, the Australian Communications and Media Authority (ACMA) advised TasRail of the need to vacate the generation 2 RCE radio spectrum allocation by April 2017, due to its reallocation to emergency services. ADE advised TasRail that the generation 2 RCE could not be reprogrammed with the newly-allocated radio spectrum. As a result, in December 2015, TasRail

[55] The GPS speed restriction option consisted of an audible alarm to the driver when the speed limit was exceeded by the train, followed by an emergency brake application and message to the network control centre if speed continued to increase.

advised ADE that generation 2 RCE was to be replaced, with a tender to be called after a business case was approved by the TasRail board.

In February 2017, a project manager for the RCE replacement project was appointed. TasRail also contacted ADE again to discuss the RCE replacement. At this time, on TasRail's request, ADE provided an updated quote, again for RCE units sourced externally. TasRail's project manager wrote to a colleague that, due to continuing delays in the project approval process, TasRail would need to start the process of writing to ACMA to ask for an extension for the radio spectrum allocation.

The RCE replacement proposal was approved at executive level in April 2017. In mid-May 2017, a meeting was held between the TasRail RCE project team and ADE to discuss TasRail's technical requirements for generation 3 RCE, including:

- retaining compatibility with both DQ and TR class locomotives
- compatibility with the new radio spectrum using a digital radio (previously analogue)
- inclusion of the Railton loading interlock (also on generation 2 RCE)
- addition of dynamic brake
- exclusion of the GPS speed restriction option.

ADE advised TasRail at this meeting that the externally-sourced RCE was no longer an option as it could not accommodate TasRail's unique requirements of the Railton loading interlock, dynamic brake and radio frequency change. The externally-sourced RCE was also primarily designed for marshalling yard work, not main-line operations.

Instead, ADE advised that it would manufacture and supply TasRail with the generation 3 RCE. This process ultimately resulted in an almost entire redesign, in part due to the requested additional functions and the need to source replacements for the microprocessors.

In late May 2017, TasRail ordered two generation 3 RCE units from ADE, with the addition of dynamic brake capability. Correspondence between TasRail and ADE during the remainder of the month included:

- driver feedback on transmitter layout
- addition of high and low horn functionality
- addition of an aerial on the driver's van, including an accompanying external port and selection switch on the transmitter
- radiofrequency spectrum allocation for the RCE.

Although delivery of generation 3 RCE was scheduled for October 2017, several issues delayed delivery. These issues related to last-minute radio frequency changes, discontinuation of antenna manufacture by the supplier, and the RCE intermittently failing-to-safe during bench testing.

These delays required driver training and RCE commissioning testing (which coincided with limited cement train shutdown opportunities) to be rescheduled. Frequent extension requests for the existing radiofrequency spectrum allocation by TasRail to emergency services were also required to allow continued use of the generation 2 RCE.

TasRail's initial project manager left in November 2017 and was replaced in mid-December by another project manager. This (final) project manager told ADE in December 2017 that continued delays were 'getting out of control' and that further slips were unacceptable.

The generation 3 RCE was ultimately delivered for commissioning testing on 18 January 2018.

Differences from previous generation

Neither TasRail or ADE provided the ATSB with a comprehensive list of changes between generation 2 and generation 3 RCE. However, a review of evidence by the ATSB indicated that

the TasRail generation 3 RCE project team were aware of several changes between the RCE generations. These included:

- new processors and motherboards (which also required the software to be rewritten in a new language in both the transmitter and receiver)
- conversion from analogue to digital radio on a new frequency
- addition of dynamic brake
- addition of high / low horn functionality
- addition of an aerial on the driver's van, including accompanying external port and selection switch on the transmitter.

Comparison between the generation 2 and generation 3 RCE operation manuals and schematics, review of correspondence, and interview evidence established that there were about 40 changes between the two generations of RCE. Records indicated that there were many undocumented changes, including:

- control fault mode receiver response
- communication failed mode receiver response (automatic and independent brake change)
- functionality of 'bail-off' control
- removal of data logger from the receiver
- new modes of operation and initialisation sequence
- alteration to transmitter audible alerts
- alterations to both transmitter and receiver displays
- locomotive vigilance system suppression and RCE receiver penalty response
- removal or change of several states that invoked an 'emergency' mode receiver response
- reversal of switch orientation to command an emergency stop
- alteration of receiver response when direction was set to neutral
- brake pipe pressure reduction levels in relation to automatic brake lever positions
- alteration of reverser violation penalty (changing direction while traction power applied) from an emergency brake application to power-down of applied traction power only.

Development process and documentation

TasRail had formed, but not formalised, a conceptual view of how the RCE would operate in practice. That is, that a system would be installed on the TR class locomotive that enabled a single driver to drive the train from within the locomotive, from the driver's van, or while loading from outside the train. There was also an identified need for certain high-level functions, such as the Railton loading interlock.

This information was communicated to ADE prior to the completion of the generation 2 RCE, while the need for additional high-level functions were advised to ADE during meetings in 2017 regarding the generation 3 RCE. After May 2017, according to several TasRail managers, TasRail had virtually no direct involvement in the generation 3 RCE design process until the commissioning testing in January 2018. ADE reported that there were no regular meetings for the duration of the generation 3 design project.

TasRail did not provide ADE with a documented set of requirements for the generation 3 RCE, including safety requirements, and it did not provide operational context and risk profile information that could be used to generate safety requirements. There was no explicit set of requirements or information about hazards and risks being documented by either TasRail or ADE.

Although some engineering design documents relating to the locomotive and braking systems had been sent to ADE by TasRail, ADE reported that it did not receive sufficient documented system

information for development, and needed to make some assumptions about systems and operations and were reluctant to ask for design documents due to intellectual property concerns.

ADE obtained an electronic brake control system manual (similar to that used for the TR class locomotive) from the internet. It did not consult directly with the train manufacturer or the electronic braking system manufacturer. Although the content of this manual described a similar system to that implemented on the TR class locomotive, some nuances of programmable functions were not described (for example, brake cylinder pressure, as affected by the J-multiplier). Further, although functionality of the EMV was described, there was no reference to the VX vent valves' existence or operation.

All ADE's physical and electrical design work and management of the project were performed by one person. Checks (reviews) were recorded for some design drawings, but these were by the same person.

According to ADE, the software was redesigned for the generation 3 RCE by a software engineer engaged specifically for this purpose. ADE did not retain permanent in-house capability to maintain the software and engaged the software engineer as needed.

The design documents produced by ADE for the generation 3 RCE are listed in Table 4.

Table 4: List of generation 3 RCE design documents

Document(s)	Date(s)	Delivered to TasRail
Operation manual	December 2017, revised July 2018	Yes
Physical specification (shape and dimensions)	July 2017	Yes
Electrical schematics	August 2017 – January 2018	No
Pneumatic schematics	January 2018	Yes
Pre-delivery and commissioning testing report	January 2018	Yes

ADE did not provide evidence to TasRail or the ATSB to show that the generation 3 RCE met any systems or safety engineering standards, or that the extensive process, analysis, technical and documentation requirements of a formal system safety process (such as outlined in AS 61508) were followed.

Driver training

With the introduction of generation 3 RCE, ADE provided additional training to drivers and supplied each driver with a copy of the RCE operation manual. The training consisted of a 20-minute session and was provided on a test bench at the RCE maintenance contractor's premises in Devonport, with the assessment consisting of a checklist. The driver of train no. 604 undertook this training along with 3 other drivers on 16 January 2018, 3 weeks before the introduction of generation 3 RCE.

Of the 40 changes identified by the ATSB between the two RCE generations, many were not recorded as having been assessed, including:

- functionality of 'bail-off' (see *Automatic brake*)
- transmitter audible alerts
- operation of dynamic brake
- vigilance suppression and RCE receiver penalty response
- brake pipe pressure reductions in relation to lever positions
- reversal of switch orientation to command an emergency stop
- significant changes to communication failed mode and control fault mode RCE receiver response (see also *Changes to braking effort during communication failed mode*).

One change that was assessed was related to the direction controller. The assessed item was in relation to the 'reverser violation' function. However, this was different and unrelated to the dual direction fault interlock, which was not assessed during training.

Commissioning

Pre-delivery testing (sometimes termed factory acceptance testing within industry) of both generation 3 RCE units was conducted at ADE's workshop using a test bench on 7 January 2018. The testing report listed 13 test elements conducted on both of the RCE units that ADE delivered to TasRail (Figure 15). There was no recorded test procedure or other records to describe the purpose, method, criteria, or outcomes of each test. All tests were marked with a symbol that denoted 'a validation for the test'; however, no relevant validation records were available.

Figure 15: Generation 3 RCE pre-delivery test record

Tests:

Safe State means: Disabled propelling and brakes applied.

Pre-delivery Test: Full operating system bench test of equipment

Site Test: System & locomotive/train test.

Software version: Txa / Rxa Jan 2018 (Software is the same for both systems)

System: AD9000 Tasrail System A

(V) – Denotes a validation for the test

Condition	Pre – Delivery Tested		Site	Comment
1. Transmitter Emergency Stop Activated	7th January 2018	(V)		
2. Transmitter Man Down	7th January 2018	(V)		Note 1
3. Vigilance short cycle (45secs)	7th January 2018	(V)		Note 1
4. Vigilance long cycle (6mins)	7th January 2018	(V)		Note 1
5. Railton interlock Violation	7th January 2018	(V)		Note 4
6. Direction Selection Violation	7th January 2018	(V)		
7. Radio Communication Loss	7th January 2018	(V)		
8. Independent Brake Failure	7th January 2018	(V)	NA	
9. Autobrake Failure	7th January 2018	(V)	NA	Note 4
10. Excitation control (off) failure	7th January 2018	(V)	NA	
11. Throttle mismatch	7th January 2018	(V)	NA	
12. CPU Failure	7th January 2018	(V)	NA	Note 2
13. Electronic Output Lockup (Reverser & GFC)	7th January 2018	(V)	NA	Note 3

Note 1 Site test to include notification to Train Control.
Note 2 Software loop failure watchdog, failsafe output and safe state.
Note 3 Brake Pipe vented to atmosphere.
Note 4 Emergency stop application
NA Test requires embedded circuitry modification to verify correct response for the failure.

The undersigned verifies the above controls were confirmed to operative when tested.

Source: Air Digital Engineering

On 18 January 2018, with ADE in attendance, generation 3 RCE was installed on the cement train for the first time to undergo commissioning testing. A single return trip from Devonport to Railton with one of the RCE units was conducted, which included the use of dynamic brake and loading and unloading movements. During this testing, ADE found '…a requirement for an adjustment in this remote unit' necessitating the return of the 2 RCE receivers to ADE's workshop in Sydney. There was no record made of how the tests were conducted, the exact intent of the tests, or the outcomes.

ATSB assessment of this activity indicated that the tests conducted by ADE showed only that the RCE was capable of performing certain functions in a general sense. In the absence of test procedures or other documentation, there was no way to show whether any non-trivial safety objectives were met. For example, there were no records to show that functions would operate under all operational conditions, including different train configurations.

In addition, there was no record made of what the subsequent remedial repairs were, or if the pre-delivery testing was again performed on ADE's test bench. ADE advised TasRail that, on return of

the RCE to Tasmania, it would '…need to be properly tested again, preferably on a TR locomotive before putting it back on the Cement train'.

On 6 February 2018, commissioning tests of the two generation 3 RCE units were again undertaken. A test plan for this was developed by the TasRail project manager and reviewed by ADE, the rolling stock assets manager and driver supervisor. The plan was developed from technical advice supplied by ADE and the RCE operation manual.

The tests were conducted in the presence of ADE and the RCE maintenance contractor, with supervision on behalf of TasRail by a graduate engineer (who had started with TasRail the previous month) and some operational staff. The graduate engineer advised the ATSB that their first interaction with the RCE was on the day of the tests; they had very limited knowledge of the TR class locomotive systems, and their role was limited to observing the testing conducted by ADE. Engineering approval authority rested with the supervising engineer (the rolling stock assets manager), who was not present.

The testing was performed in Devonport Yard with limited train movement available. The test plan (a checklist, Figure 16) included items such as operational functionality, transmitter LED indicators and safety features.

Figure 16: Generation 3 RCE commissioning checklist

CEMENT TRAIN REMOTE CONTROL- TESTING & COMMISSIONING PLAN

Date: 6/02/2018

7.0 SITE TESTING AND COMMISSIONING (System-A)

The functions below are to be tested as well as moving the locomotive under its own power with all systems operating.

	System –D9000-NG –A	Checked	Comments	
1	Key Switch Off/ On/ILK	6/2/18		
2	Railton Lock	6/2/18		
3	Auto Train Brake	6/2/18		
4	Train Brake (TB)Indicator	6/2/18		
5	Independent (Engine) Brake	6/2/18		
6	Independent Brake Indicator	6/2/18		
7	BCP(locomotive) Indicator(EB Indicator)	6/2/18		
8	Throttle	6/2/18		
9	Throttle Indicator	6/2/18		
10	Emergency Stop	6/2/18		
11	Vigilance/ Arming- TS/VC Control	6/2/18		
12	Sand	6/2/18		
13	Independent Bail (Automatic)	6/2/18		
14	Backlight	6/2/18		
15	Dynamic Brake	6/2/18		
16	Dynamic Brake warning	6/2/18		
17	Dynamic Brake Indicator	6/2/18		
18	Reverser	6/2/18		
19	Forward & Reverse Indicator	6/2/18		
20	Horn / Horn High Note	6/2/18		
21	Tilt Switch	6/2/18		
22	Transmitter's Display	6/2/18		
23	Drivers Van (DV- Antenna Switch)	6/2/18		
24	Transmitter's Audible Alerts	6/2/18		
25	Systematic Resets	6/2/18		
26	Hose pipes		Required after testing completed	
27	Weather protection covers		Not fitted at Test Date	

CEMENT TRAIN REMOTE CONTROL- TESTING & COMMISSIONING PLAN

7.0 Cont SITE TESTING AND COMMISSIONING (System-A)

System –D9000-NG –A

Testing tasks below verifies controls operate when tested on locomotive & train

	Condition / Task	Validated	Date	Comments
1	Transmitter Emergency stop Activated		6/2/2018	
2	Transmission Man Down (TC)		6/2/2018	
3	Vigilance short Cycle (45 Sec)		6/2/2018	
4	Vigilance Long Cycle (6 mins)		6/2/2018	
5	Railton Interlock Violation		6/2/2018	
6	Direction selection Violation		6/2/2018	
7	Radio Communication Loss		6/2/2018	
8	Independent brake failure		7/1/2018	Pre delivery tested
9	Auto brake Failure		7/1/2018	Pre delivery tested
10	Excitation Control (off) Failure		7/1/2018	Pre delivery tested
11	Throttle mismatch		7/1/2018	Pre delivery tested
12	CPU failure		7/1/2018	Pre delivery tested
13	Electronic Outputs lockup (Reverser & GFC)		7/1/2018	Pre delivery tested

Notes

The checklist was initialled by the graduate engineer to indicate that the test was conducted (initials obscured).
Source: TasRail, modified by the ATSB.

The commissioning checklist did not denote defined steps, expected observations or pass / fail criteria. Further, it did not include several failure modes, which aligned with tests 8 through 13 on the pre-delivery testing document. These tests were labelled on the pre-delivery test document as: 'Test requires embedded circuitry modification to verify correct response for the failure'. This indicated that these tests were only able to be conducted on the ADE test bench.

Over the following 3 days, additional tests related to this list were conducted on the cement train service between Devonport and Railton, with ADE in attendance. The TasRail graduate engineer initialled next to tests 1–14 and 17–25 in the first table (Figure 16), and in the header block above

the second table. These indicated which tests had been performed. There were no further records of how the tests were performed, or the results.

Both generation 3 RCE units were formally accepted by TasRail as being '…commissioned successfully, without error and only minor omissions…' on 9 February 2018. There was no record of what the 'minor omissions' were.

Previously, in early 2014, TasRail undertook a substantial change to locomotive brake systems[56] that required locomotive and RCE testing. Like the generation 3 RCE test records, there was a list of tested functions (Figure 17) but no test procedure. By contrast, an independent consulting firm engaged by TasRail to verify the proposed locomotive functionality had a 16-page test procedure with defined steps, expected observations and detailed pass/fail criteria. An example procedure (Figure 18) shows how the consulting firm detailed how it tested the same functionality listed as item (k) in the ADE record.

Figure 17: Extract of RCE test documentation used by ADE in 2014

The functions below were then tested as well as moving the locomotive under its own power with all systems operating correctly.

(a) Key Switch – Railton interlock
(b) AUTO Brake (6 step operation 0 to 5)
(c) Train Brake Indicator
(d) INDEPENDENT Brake (6 step operation 0 to 5)
(e) BCP (Locomotive) Indicator (EB Indicator)
(f) Throttle (8 step operation 1 to 8)
(g) Throttle Indicator
(h) EMERGENCY Stop
(i) Vigilance / Arming
(j) Sand
(k) Ind. Bail
(l) Backlight
(m) Dynamic Brake (NA)
(n) Dynamic. Brake Indicator (NA)
(o) Reverser
(p) Reverser Indicator
(q) Horn
(r) Tilt Switch

Source: TasRail; unrelated highlighting removed by ATSB

Figure 18: Extract of locomotive test procedure used by independent consulting firm in 2014

Tested By :-	**Date:-**
Instruction **Locomotive Number:-**	**Result –** **✓ or Fail**
Full Service Brake Application - Trailing Locomotive Position	
1 Using the leading sponsor locomotive, make a full service automatic brake application, reducing the brake pipe pressure to approximately **350 kPa. Record BP pressure**	**_____kPa**
2 Brake cylinder pressure on the test locomotive must rise to between **350 ± 14 kPa.**	
3 Record BC pressure.	**_____kPa**
4 Move the independent brake handle downwards, activating bail-off, to pressurize the **IR (No.4)** pipe to **MR** pressure.	
5 Brake cylinder pressure on the test locomotive must fall to **zero kPa** and the brakes must release.	
6 Using the leading sponsor locomotive, release the automatic brake application by increasing the brake pipe pressure to **500kPa.**	**_____kPa**

Source: TasRail

[56] This was conversion of the DQ and 2050 class locomotives and generation 2 RCE from a 3-pipe to 4-pipe braking configuration. This added a fourth pneumatic connection between locomotives to allow the release of locomotive brake cylinder pressures induced through a brake pipe pressure reduction.

The generation 3 RCEs were used on the cement train service immediately following the 9 February 2018 commissioning tests. Once the generation 3 RCE entered service, ADE personnel rode with drivers for a short period of time to monitor RCE operation and performance.

Issues after commissioning

Screen freezes and radio signal strength

On 11 February 2018, problems with the RCE transmitter display screen were encountered. The transmitter was found to be frequently locking up (with the screen 'freezing') with no updates of air pressures or operating status available to the driver. ADE advised TasRail that this was a '…nuisance occurrence but…drivers are knowledgeable and using the Led's'; that is, ADE believed operations could continue based on the transmitter's LED indications alone.[57] Driver reports indicated that these screen freezes were frequently in conjunction with slow or non-responsiveness of the RCE to driver commands and communication failed mode occurrences.

In response, ADE communicated with the cement train drivers by telephone over a 2-day period (from 17 to 18 February 2018) to diagnose the fault. ADE initially believed the problem was caused by excessive radio signal strength between the transmitter and receiver causing transmitter-screen interference. The radio signal was altered to a lower strength on several occasions, however this did not resolve the transmitter lock-up faults.

At the end of June 2018, with work continuing on addressing reported problems, ADE found that the transmitter lock-ups were being caused by an '…incorrect reference to a microprocessor setting in the manufacturers information', not radio signal strength. Adjustments were made and the original radio signal strength was restored. These changes greatly improved the RCE's reliability and performance from late-June 2018 onward, including a reduction in communication failed mode events.

Traction motor flashover event

On 13 February 2018, a traction motor flashover event[58] occurred, damaging a traction motor on a TR class locomotive. After investigation by TasRail, the locomotive manufacturer and ADE, it was found that, while travelling in the forward direction, the driver had accidentally moved the direction controller from forward to reverse instead of de-selecting dynamic brake on the transmitter. Later, after de-selecting dynamic brake correctly, the driver applied traction power while still travelling forward, resulting in a wheel lock and flashover.

TasRail identified that the dynamic brake selection switch and direction controller looked and operated the same and were adjacent to each other on the transmitter (see Figure 13). In response, the use of dynamic brake on the cement train was suspended until changes were made to the RCE by ADE to prevent recurrence (see *Changes to remote control equipment prior to project completion*). Although the changes were made by June 2018, the drivers were not advised. As such, at the time of the 21 September 2018 runaway accident, dynamic brake was still not in use.

Changes to braking effort during communication failed mode

As discussed in *Differences from previous generation*, among the changes between the generation 2 and generation 3 RCE were changes to the communication failed mode response. The generation 3 RCE now applied a lessened automatic brake pipe pressure reduction (400 kPa instead of the previous full-service application of 350 kPa) in communication failed mode, and also maintained any previous independent brake application.

---

[57] LED indicators on the RCE transmitter (Figure 13) were automatic brake (TB) and / or independent brake (EB) application in effect, traction power (TH) applied, communication (COM) as a flashing light, low battery (BAT) and dynamic brake (DB) mode active.

[58] Flashover: an electrical arc in an electric motor, sometimes resulting in damage.

Although it is possible that the matter was discussed without being recorded, and the RCE operation manual had reflected the new response, the available evidence indicates that TasRail did not initially consider the potential effect of these changes on train stopping distance in communication failed mode. In April 2018, 2 months after the introduction of generation 3 RCE into service, the network access manager became aware of the changes and enquired about whether the change had been risk assessed.

TasRail then asked ADE if this change had been in the original scope of work. ADE advised that the change had been brought to the attention of the TasRail generation 3 RCE project team. This appeared to have occurred in an October 2017 email to TasRail (at the end of a list of unrelated questions) where ADE mentioned a change to the independent brake response for the generation 3 RCE during a communication failed mode response:

> …if there is a communication loss, I would like to be sure that by applying the safety factors for slower train speeds will also be suitable when the train is moving fast.
>
> With the new systems, as well as the Brake Pipe application the independent brake will maintain whatever the output command was before the comms loss [communication failure].

In any case, neither ADE or TasRail assessed the safety implications of the reduction in automatic braking level at this time. It is therefore likely that TasRail, at the time, did not appreciate that the train's braking performance in communication failed mode would be decreased with the generation 3 RCE compared to the generation 2 RCE.

Stopping distance tests were ultimately performed by TasRail in mid-June 2018, at typical yard speeds (up to 25 km/h). There were difficulties with recording fidelity, and later ATSB analysis concluded that the available results were inconsistent. Furthermore, although TasRail concluded that the new response 'sufficiently brings the train to a stop', there was no risk assessment or other analysis to determine the safety impact of the change. TasRail later advised the ATSB that the testing was intended to address the potential for loss of radio communications during yard operations, where the driver would be external to the train, and considered that driver access to the emergency dump valve in the locomotive would enable more rapid stopping in an emergency (while driving at speed) than the application of the communication failed mode braking response.

An action item that was generated as a result of this testing indicated that further driver training or instruction was to be provided on the continued availability of the emergency brake during a loss of RCE radio connection through operation of either the locomotive automatic brake handle or driver's van emergency brake (see *Emergency brake*). Although this training was noted as completed on 1 June 2018, available evidence indicates that it did not occur.

Other problems

Throughout the period from February to June 2018, drivers were reporting a significant number of fault events associated with the generation 3 RCE, primarily communication failed mode events as well as transmitter lock-up events (see *Reported faults*).

Further problems identified after commissioning of generation 3 RCE included:

- There were 2 different types of multiple unit cable pins within the receptacles across the TR class locomotive fleet. Identified in late February 2018, this resulted in ill-fitment with the receiver's multiple unit plug, causing issues with the selection of forward and reverse directions.[59]
- There was an uncommanded brake release and risk of runaway at Railton when resetting a communication failed mode occurrence. First identified in early May 2018 after a software change, it was found necessary to apply a full-service automatic brake application on the transmitter during each wagon placement at Railton to prevent an uncommanded brake

[59] TR11 (the accident locomotive) was confirmed to be fitted with the multiple unit pin type which provided the best contact with the receiver's multiple unit plug.

release in the event of a communication failed mode reset. ADE advised TasRail in late May 2018 that the issue had been fixed through a further software change, ensuring the brake pipe would not recharge when the RCE transmitter was switched back to 'interlock' from the 'off' position. As a result, drivers were instructed that a full-service automatic brake application after wagon placement was no longer required. However, less than 4 hours later, after a further undisclosed RCE fault was encountered,[60] the full-service instruction was reimposed. It appeared this issue was resolved at the end of May 2018.

- On 25 May 2018, a failure of the RCE transmitter's throttle occurred while tractive power was applied. The driver reported that they had used the TR class locomotive emergency dump valve to stop their train after being unable to remove tractive effort on the transmitter. TasRail advised ADE that the driver did not use the transmitter's emergency stop switch as 'The driver did not trust the remote [transmitter]'. TasRail further advised ADE that 'The remote [RCE] incidents have become a safety issue and require immediate rectification'. Another failure of the transmitter's throttle had also occurred 6 days earlier, with repairs made by the RCE maintenance contractor.
- Issues were reportedly encountered after fault mode resets. These related to an inability to release the independent and / or automatic brake, or an inability to reapply the automatic brake after fault resets.

TasRail response

In mid-May 2018, TasRail expressed to ADE concerns of a 'significant risk to the business' due to the ongoing generation 3 RCE faults, and it requested ADE to supervise the next onsite RCE changeover[61] to ensure ADE's latest modifications were successful. ADE did so and was presented by TasRail with a list of faults to address. Two follow-up meetings were held between TasRail and ADE in June 2018 to address these matters. TasRail later advised the ATSB that, at this time, it was concerned with the communication and braking issues.

TasRail expressed to ADE twice (17 May 2018 and 6 June 2018) that it intended to reinstate generation 2 RCE until such time as ADE had rectified the ongoing faults with generation 3 RCE. However, this did not occur. Safety was not explicitly stated among TasRail's concerns. As a TasRail representative described to the ATSB, TasRail's concerns were from operational and business perspectives due to time delay impacts. The decision was made to continue using generation 3 RCE as:

- A large number of communication failed mode events had already been occurring with the end-of-life generation 2 RCE.[62]
- There was a need to test fault rectification modifications to the RCE by ADE.
- Although RCE drivers had raised safety concerns regarding generation 3 RCE, ADE gave TasRail assurances that the RCE would fail safe.[63]
- By late June 2018, the RCE's reliability had considerably improved. Reporting of communication failed mode events (most reports) had reduced to an 'acceptable level'.[64]

By the time of the June 2018 meeting, most RCE problems were occurring during loading and unloading activities.

---

60 The ATSB determined this was likely related to the throttle failure incident.

61 This entailed a change of transmitter, receiver and air box to the spare set, usually in conjunction with a locomotive change.

62 In its final 3 weeks of operation (up to 9 February 2018), generation 2 RCE had 73 reported events, 63 of which were communication failed mode events.

63 In March 2018, after ADE advised TasRail the RCE was 'designed with [several] failsafe features following AS 61508', TasRail issued a notice of this advice to its drivers, including that the RCE '…will only fail safe'.

64 After the cause of the transmitter screen freezes had been addressed, reported events reduced to an average of about 10 per month, 72% of which were communication failed mode events.

Changes to remote control equipment prior to project completion

After the traction motor flashover event in February 2018, ADE altered the dynamic brake selection switch from a forwards / backwards to a left / right orientation, to differentiate the switch physically from the direction controller. In addition, ADE took the opportunity to add time delays before the RCE receiver would apply traction power after de-selection of dynamic brake, and before the application of dynamic braking effort after selecting dynamic brake mode. Both these changes were made by late June 2018.

Other changes to generation 3 RCE after commissioning, but prior to acceptance, included:

- multiple software changes
- communication failed mode behaviour while in Railton loading interlock mode
- alteration of 'bail-off' capabilities
- a reduction in radio signal strength, which was subsequently reverted
- radio component changes
- change in level of brake pipe pressure reduction for a minimum-service application.

Most of the changes above were made without any record of subsequent testing. On 2 occasions, TasRail recorded that testing had occurred; however, there was no description of the tests conducted or the outcome of testing. Both occurred in June 2018. The first test was in response to several modifications that had been made to improve reliability of the RCE. There was no record made of what the changes were. The second test was of the impact to cement train stopping distances due to changes to the communication failed mode, as discussed previously in *Changes to braking effort during communication failed mode*. Although this change existed in the commissioned version of generation 3 RCE, it was not tested at that time.

No risk assessments were performed for any of the changes to generation 3 RCE after commissioning (see also *Risk assessments for remotely-controlled train operations*).

Acceptance and project completion

The post-commissioning modifications to the generation 3 RCE from late June 2018 resulted in greatly improved reliability. Fault reports had reduced from up to 20 per day earlier in the month to 1 or 2 per shift. As this was deemed to be an acceptable level of faults by both ADE and TasRail, generation 3 RCE was accepted for practical completion on 26 June 2018.

Asset handover from the RCE project team followed on 2 August 2018, noting that dual inspection by both the asset manager and end user was yet to occur. The project was closed with the following comments:

> The new remote controls units have had over the past six months undergone Extensive testing, modifications both on and off the cement train [and] has provided a Safe and efficient remote control mechanism that is both compliant with ACMA, TasRail and ONRSR [Office of the National Rail Safety Regulator] requirements.
>
> The periodic loss of communications with Communication failures (CMF) [communication failed mode] has been adjusted and is currently held to a manageable minimum and will continue to be monitored to identify any trend or location issues with the remote areas.

Remote control equipment fault reporting

Fault reporting process

There was no dedicated form or procedure for reporting generation 3 RCE faults, although drivers could report faults through other means. For example, driver reports received by the duty network control officer (NCO) would be noted in the NCO incident log. Accordingly, reports of substantial time delays attributable to the RCE were recorded in the log.

In addition, drivers completed a cement train shift form each day during their shift. This form included multiple options for recording time delays, with one termed 'remote issues'. This form included both reports that were also made to the NCO, and further faults and events which did not result in significant time delays.

Driver reports received by the duty NCO would be referred to the relevant section for action. For generation 3 RCE faults, these were to the driver supervisor, rolling stock assets manager or superintendent technology and communications. However, the decision of who was best placed to address these was at the NCO's discretion. In addition, the customer service delivery manager would tabulate RCE specific cement train shift report delays and forward these to the TasRail project manager, who would then forward a selection of these to ADE for diagnosis and rectification.

Reported faults

From 9 February 2018 (the date that generation 3 RCE was commissioned) to 21 September 2018, there were 68 entries for a total of 125 faults identified in the NCO incident log and 116 entries totalling 281 faults identified in the collated cement train shift reports.

It is likely that many of the entries in these 2 types of forms were duplicates (the same occurrence being recorded by both reporting channels). However, there was insufficient information to confidently identify all duplicate entries, and some entries that were likely to be duplicates recorded different fault conditions for potentially the same fault. Therefore, no attempt has been made to remove duplication from the analysis presented below. There was also insufficient data available to determine the validity of the reported fault type with confidence.

Acknowledging these limitations, the ATSB analysis indicated that TasRail recorded:

- 214 communication failed mode events
- 90 events where the fault mode was either not specified or not a penalty mode (for example, throttle failure, Railton loading interlock failure and brakes not releasing)
- 79 transmitter lock-up events (including screen freezes)
- 17 driver-initiated receiver shutdown and restarts (cold starts) to reset fault conditions
- 25 uncommanded emergency brake applications or alarms
- 4 control fault mode events
- 1 driver reporting the RCE as 'unsafe' for use
- 1 driver ceasing use of the RCE after it became unresponsive.[65]

Some of the reported events, such as the cold starts, almost always happened because of other faults (as they were recovery actions), and others were reported simultaneously (such as simultaneous communication failed mode and transmitter freeze).

Although on most days there was only a single fault recorded, this varied. Occasionally reports included over 10 faults in a single day, with the most recorded being 20 in one day in June 2018. As previously noted, the number of faults significantly decreased after June 2018, down to 1 or 2 per shift.

Extent and accuracy of fault reporting

A TasRail representative expressed concerns in interview to the ATSB that drivers had become overly confident with RCE failure resets with the generation 3 equipment, and were under-reporting faults. The representative stated drivers thought if 'I do a reset and it keeps running, I'll use it…until it stops'. These thoughts were shared by the incoming driver (on the day of the accident), who advised the ATSB that, provided an RCE fault reset was successful, operations

[65] After direction selection failure (21 February 2018), and throttle failure (25 May 2018) incidents respectively.

would continue. TasRail drivers also advised that they would only log and report generation 3 RCE faults with their supervisor or the NCO if the faults were persistent.

In May 2018, it was recognised that not all RCE faults were being reported by drivers, including some being reported informally to the RCE maintenance contractor. This resulted in the driver supervisor sending an email to all RCE drivers, requesting urgent advice of all encountered faults '…no matter how trivial', to coincide with an onsite attendance by ADE for rectification.

Concerns regarding the informal nature of fault reporting by drivers was again raised at a meeting between the generation 3 RCE project team and ADE in June 2018. However, the issue was not formally recorded on the meeting minutes, nor noted who raised the concern. No evidence was provided by TasRail to indicate how, or if, this problem was addressed.

The seriousness of control fault mode events was recognised by the network access manager, who had previously implemented generation 1 RCE in their former role as the planning manager. In interview, the network access manager described instances of control fault mode as an unsafe condition that required an emergency brake application by the RCE because it was quite serious. They also noted that, if the locomotive was moving, the emergency brake application would create an alarm at network control.[66]

The network access manager reported that they had reviewed driver reports and noted that several network control centre emergency alarms with generation 3 RCE were being logged as communication failed mode events. They stated that this was incorrect as these did not send a Selcall alarm. They also noted that communication failed mode events were, in their experience, viewed as a productivity issue not a safety issue.

Furthermore, it was common in their experience for communication failed mode and control fault mode events to be misdiagnosed by drivers as they looked similar on the RCE transmitter display screen (that is, they had similar letters, with communication failed indicated by 'COMF' and control fault indicated by 'CNF', Figure 19). This view was shared by the NCO on shift at the time of the 21 September 2018 runaway accident, who advised that it was normal for a communication failed mode to trigger an emergency alarm. The NCO would then follow up and the driver would also indicate that it was a communication failed mode event.

[66] The network access manager described that a control fault would create an emergency brake application and alarm. While this was the intended response in generation 2 RCE it was not correct for generation 3 RCE as the control fault mode response had significantly changed.

Figure 19: RCE transmitter and display screen

Image shows the RCE transmitter with detail images of communication failed mode (left) and control fault mode (right) presentations on the transmitter screen.
Source: ATSB

To ensure appropriate scrutiny and tracking of control fault mode occurrences within the driver reports, the network access manager advised the NCOs to challenge drivers who reported communication failed mode occurrences when there was an accompanying emergency alarm in the control centre.

Both the network access manager and NCO reported having an expectation that communication failed mode or control fault mode events would create Selcall alarms. They also received reports of these events after receiving Selcall alarms. However, this was not the designed behaviour of the generation 3 RCE, which were not intended to create an alarm. The control fault mode response had been changed from the generation 2 RCE (which previously would create an alarm when moving) and the communication failed mode response also was not intended to create an alarm.[67]

As discussed in *Other selected fault events*, there were at least 8 instances of uncommanded emergency brake applications reported by drivers. Although it is likely these were considered to be instances of control fault mode events, the ATSB found that none of these events were related to either a known fault mode or any other emergency penalty condition.

In addition, during review of the NCO incident log records, the ATSB identified at least 2 occasions where a driver had reported a full-service penalty, as occurs in control fault mode, as a communication failed mode event.

In summary, there was evidence of incorrect expectations, misreadings and mode confusion in reports made by the generation 3 RCE drivers and received by network control. This resulted in periodic misdiagnoses of control fault mode (CNF) events with communications failure mode

[67] For a description of the designed behaviour refer to the following sections of the report:
- the generation 3 RCE control fault mode, see *Control fault mode*
- the generation 3 RCE communication failed mode, see *Communication failed mode*
- conditions which resulted in alarms to the network control centre, see *Network control.*

(COMF) events. In addition, uncommanded emergency brake applications, which were not attributable to any known fault or penalty condition, were at times misdiagnosed and reported by drivers as either communication failed or control fault mode events.

TasRail response to reported faults

In instances where driver reports received by the NCO were deemed to be a risk to safety (including 'Category A and B' notifiable occurrences), the NCO was to create an entry in TasRail's 'risk wizard' system. This incident recording database allowed for the identification, tracking and recording of actions against identified safety incidents. From the introduction of generation 3 RCE to the day of the accident, only one entry in relation to the RCE was made in risk wizard. This related to the event at Caroline Creek in May 2018 (see *Caroline Creek event*), and was recorded on the basis of work health and safety considerations due to lack of trackside access to the locomotive. This single risk wizard entry for generation 3 RCE did not include any follow-up actions (see also *Occurrence notification*).

As noted above, RCE driver fault reports received by the network control centre were referred by the NCOs for follow-up. Communication failed mode occurrences were occasionally sent for follow-up, although this appeared to be dependent on which NCO was on duty at the time of the occurrence. The rolling stock assets manager was also frequently advised of faults.

The rolling stock assets manager advised the ATSB that, after the commissioning of generation 3 RCE, they worked with ADE (through the project team) to rectify rolling stock–RCE integration faults, including the issues with dynamic brake, multiple unit pins and communication failed mode events (see *Remote control equipment* and *Issues after commissioning*). The rolling stock assets manager would forward RCE specific faults to the RCE maintenance contractor for rectification. Once final acceptance of generation 3 RCE was complete, the rolling stock assets manager worked directly with ADE.

Several TasRail staff advised the ATSB that they had been concerned regarding the overall monitoring, coordination and follow-up of generation 3 RCE faults. There was a heavy reliance on ADE and the RCE maintenance contractor for a technology that was largely an 'unknown' within TasRail.

The ATSB was advised these concerns were raised at the daily TasRail operations meetings; however, there were no records available to confirm this had occurred.

TasRail change management and related processes

General information

TasRail was required to have procedures within its safety management system (SMS) for ensuring that changes that could affect the safety of its railway operations were identified and managed.[68] This included ensuring that changes were fully identified and described, and the risks associated with the change were identified and managed.

The TasRail change management procedure (BIC-PRO-300) detailed that, other than 'routine change',[69] changes were to include a:

- consultation process
- change management plan
- risk assessment
- documented record of the changes

---

[68] *Rail Safety National Law National Regulations 2012*, Schedule 1 (clause 12 – Management of change).

[69] Routine change was defined in the procedure as those currently '…controlled by existing standards, codes, rules, procedures and the SHE management system [SMS]'.

- check of compliance against legislation
- safety validation where the change impacted ‘safety activities’ (with safety activities including ‘driving and operation of trains’ and ‘control the movement of trains’).

Change management processes

According to the change management procedure, all changes were to be classified by an initial impact assessment (IIA) to determine the project management level required. The IIA was split into 2 parts:

- Part A included 9 questions, answers to which determined if the change was to be considered ‘small’ (checklist only) or ‘significant’ on the basis of factors such as:
  - impacts on people, processes, or systems
  - inter-departmental cooperation
  - safety (‘Are there any negative safety implications associated with the initiative?’)
  - strategic influence
  - cost
  - requirement to notify ONRSR in accordance with notification of change guidance.
- Part B applied to changes that had been assessed as significant. This part asked 6 questions on business and safety risks, some of which were broken down into more detail. Each question could provide up to 5 points, and the points were totalled to give the project a ranking of P0, P1, P2 or P3 in increasing order. Less than 14 points resulted in a classification of P0 or P1 depending on cost, while 14-21 points resulted in a classification of P2. P0, P1 and P2 projects were further ranked with a ‘+’ if the project had added ‘significant’ strategic or ‘high’ safety impacts.

At the end of the IIA form, there was a ‘project management assurance requirements and approvals record’, listing several ‘gates’ (or checkpoints) for P1 and P2 projects, as follows (in addition to provision for other gates as required):

- approval of the project classification
- acceptance in principle (P2 only)
- approval to proceed
- approval of the project business case
- acceptance of design
- acceptance for testing (P2 only)
- acceptance for operations/implementation (P2 only).

All these gates required authority from the executive to proceed. There was also a project closure checklist required to be authorised by the project sponsor.

All ‘significant’ projects required a range of activities, such as risk assessment, risk action planning, life cycle safety validation, and reviews, each producing documentary records. Projects with higher classifications required additional approvals and documents.

Two of the defined processes for significant changes were BIC-PRO-302 (*Change management processes for P0/P0+/P1/P1+ projects*) and BIC-PRO-301 (*Change management processes for P2/P2+/P3 projects*). Until late July 2017 (during the generation 3 RCE project), both were in draft form and not available on TasRail’s intranet. However, TasRail advised the draft processes were ‘…possibly used in-house’ during this period. Documents produced for the project indicated that this was the case.

Both these processes contained a series of ‘gates’, which served as checkpoints that required documentation and / or approvals before the project could progress. The project management

processes contained the regulatory requirements for change management (see *Notification of change*).

The change management procedure and processes (the latter of which were more related to project management) mentioned the requirements for conducting technical investigations, creating preliminary designs, and performing safety validation for the whole of the system life cycle for the assessed change. However, there was no direction to the relevant sections of TasRail's SMS or external guidance materials that would apply in this regard (for example, relevant engineering standards, procedures and processes, see *Design assurance processes* for further information). Such guidance was particularly relevant for accurately assessing the safety impacts the change may have on current operations and conducting appropriate activities to address these impacts during the change process.

Generation 3 remote control equipment project

Business case

In early 2015, the generation 3 RCE project informally commenced (see *Generation 3 remote control equipment project initiation*). A formal project business case was completed in December 2015. It noted a requirement to replace the ageing generation 2 RCE due to:

- reduced reliability
- end of ADE support
- lack of dynamic brake capability
- inability to transition the current RCE to a new digital radio.

Four options were presented in the business case, including a '…simple like for like replacement' of the generation 2 RCE units, with:

- the addition of dynamic brake capability
- compatibility with the newly-allocated radiofrequency spectrum allocation.

Initial impact assessment

An initial impact assessment (IIA) for generation 3 RCE was completed in November 2016. The completed IIA referred to the addition of dynamic brake but did not include consideration of other changes to generation 3 RCE that were known or requested by TasRail. It did not specifically identify the dynamic brake as a change from the previous generation of RCE, just that it was included.

Part A of the IIA was completed as follows:

- The summary of the main change implications of the initiative was 'continued use of remote control systems in a safe manner and in compliance with regulations'.
- There were 'Yes' answers to the questions about impacts on people, processes or systems, inter-departmental cooperation, and cost.
- There was a 'No' answer in relation to whether there were 'any negative safety implications associated with the initiative'.
- There was a 'No' answer in relation to whether notification of change to ONRSR was required, with a note that read: '…assuming that as a replacement part units can function under any authority currently granted……need to confirm'.
- The question to record whether the change was significant was not completed, but Part B was completed, indicating that the 'Yes' answer in Part A led the assessor to determine that the change was significant.

Items of note in Part B included:

- The assessment of risk (to business, people or processes) was 'low'. The guidance description for the low-risk category was that 'initiative is an administrative change or a change of like for

like' and the associated justification was that the proposed RCE was the 'same units which are more modern but perform the same tasks more safely'.

- 'Professional human factors services' were not required.
- In determining the 'failure consequence', which asked 'Impact due to worst case scenario arising from system failure or human error?', the assessor recorded the middle score (3 points), associated with 'limited…safety, operational or organisational impact' (the other options were 'minimal' with 1 point or 'significant' with 5 points).
- In response to an 'assessment of complexity,' the assessor recorded that there was 'minimal systems integration' and 'straightforward' incorporation of safety requirements. The overall assessment of complexity, based on a combination of other assessments, was the middle of 3 available scores.
- In response to an 'assessment of novelty,' generation 3 RCE was stated as 'in widespread use' outside of TasRail, and that the implementation did not require new standards or procedures. The overall assessment of novelty, based on a combination of other assessments, was the lowest of 3 available scores.
- The assessment of strategic value was 'None'. The guidance description for this category was 'initiative is a change of like for like and has no impact on TasRail's business value.'
- The assessment of impact on safety was 'Medium'. The guidance description for this category was 'initiative is an adaptation of an existing system, function or asset'.

The overall score of 12 resulted in the change being classified as a significant change of level P1 (minor business impact, project value outside general manager's financial delegation) requiring the 'significant change management process' to occur.

The initial project manager reported that the IIA was checked by the project stakeholders identified within the IIA and by the general manager of asset services. However, the project management assurance requirements and approvals record was blank and TasRail had no evidence that the necessary approvals had been obtained.

Revised business case

In January 2017, the business case for generation 3 RCE was resubmitted. As with the business case about a year earlier, it recommended the purchase of two RCE units with dynamic brake capability, noting it was a 'simple like for like replacement', although training would be required. Known business and operational risks of not proceeding with the purchase were detailed, with the risk register flagged as requiring updating.

In the 'change management plan' section of the business case, the project level was increased to P2 (important business impact) from the previous IIA-assessed P1 level. The relevant procedure stated that where an increase in scope or cost of the project occurred, as can be inferred from the increase to P2 level, another IIA was to be completed and submitted for executive approval. However, TasRail could not provide a reworked IIA or other details explaining why the project level had been increased to P2.

Although termed a 'like for like' replacement, the person who developed the business case told the ATSB that the inclusion of the options represented a 'significant change' that affected the assessment, and that, in hindsight, these changes meant that it was not like-for-like.

The business case recommended single-source supply procurement from ADE, rather than a tendering process, as ADE was:

- familiar with TasRail's operational requirements (having previously supplied generation 1 and generation 2 RCE)
- able to assist TasRail with developing the required technical specifications
- available for local support

- able to meet the 'tight timeframe' for delivery of generation 3 RCE by May 2017, with commissioning complete by the end of August 2017 (due to ACMA requirements).

The business case on multiple occasions referred to adhering to the project management process as a means of fulfilling the business case requirements.

As noted in *Generation 3 remote control equipment project initiation*, TasRail appointed a project manager for the project in February 2017. TasRail also contacted ADE to obtain an updated quote for the RCE and proposal was supported at executive level in April 2017.

TasRail's risk and compliance manager advised the ATSB that, during this period, they were aware that an upgrade of the RCE was occurring; however, they were not involved in the project as it had been deemed 'like for like'. Neither the freight services or assets management safety specialists (who reported to separate general managers) were involved during the generation 3 RCE procurement and commissioning process.

Change management activities

TasRail's change management processes listed gates (3 for a P1 project and 6 for a P2 project) intended to prevent a project from progressing unless certain requirements were met. In addition, the processes listed 20 documents required to be produced for P1 projects, and 33 documents for P2 projects.

TasRail produced 11 of the listed project documents. Of these, 5 were incomplete, including 3 not containing the required approvals. There were no records to show that the 6 required gates for a P2 project were formally passed with the appropriate executive-level approvals.

Relevant documents required for a P2 project but not produced included:

- risk assessments
- notification of change process
- change management plan
- stakeholder engagement and communications
- technical investigations / preliminary designs
- regular monthly reports to the TasRail Board
- acceptance for testing form
- acceptance for operations form
- post project review report.

TasRail's internal investigation report into the 21 September 2018 runaway accident found that:

> Based on the long safety record of previous generations [of RCE] and in the belief by the TasRail project staff that the third generation remote-control was an enhanced "like-for-like" and fail-safe replacement, TasRail's procurement processes were truncated...No specification was issued and the procurement was treated as a product purchase. As a result, TasRail's normal project management and engineering controls were circumvented and full reliance placed on the supplier to deliver and commission the units.

As noted above, the concept of the generation 3 RCE being a like-for-like replacement was used in the December 2015 business case and the initial impact assessment (IIA). The initial project manager also advised the ATSB that it was a like-for-like replacement that replaced one remote with another, and that related safety procedures were still valid for the new RCE, excepting those relating to the new dynamic brake feature. They therefore felt that the safety impact of the replacement was low. In addition, TasRail advised the ATSB that the limited amount of driver training required indicated that the operational changes were not substantial, reinforcing the perception that the generation 3 RCE was comparable to the previous generation.

Even though there was a view within the project team that generation 3 RCE was a like-for-like replacement product, there was no allowance for the steps, gates or required documents of the project management process to be bypassed on this basis.

The final project manager, who took over the generation 3 RCE project in mid-December 2017 (shortly before commissioning of the generation 3 RCE), advised the ATSB that the initial project manager had advised them that the generation 3 RCE was the same as generation 2, with the addition of dynamic brake functionality, so the final project manager did not realise the extent of differences.

The final project manager further reported that:

- very little documentation was passed on during project handover, with no documented RCE specifications, functions, or expectations
- no-one within TasRail challenged the lack of documentation.

Project review and audits

Document BIC-PRO-100 (*Project review and auditing*) detailed the procedures to ensure compliance to TasRail's change, risk, and project management processes. At the start of each financial year, the project management office's senior project manager, chief operating officer, general manager asset management and general manager freight services would select 12 significant change projects for audit and review. The generation 3 RCE project was not selected as part of these reviews.

TasRail had additional audit requirements for projects funded under the state-federal partnership's infrastructure improvement program. However, as an above-rail asset, the generation 3 RCE did not qualify as a project under the program, so these audits were not required. There was no audit of the generation 3 RCE project performed by TasRail's project management office.

Risk management activities

Risk management requirements

An integral part of change management is identifying the hazards and assessing, controlling, monitoring and reviewing the risks associated with the change. TasRail's method of risk management was contained in documents CGR-BCP-001 (*Corporate governance and risk management*) and CGR-PRO-100A (*Risk management*).

TasRail's chief executive officer (CEO) delegated responsibilities for risk management. The general managers of freight services and asset management were responsible for ensuring the application of risk management principles to railway operations. The risk and compliance manager was responsible for the application of the risk management process, and assurance of compliance with the process (including risk control monitoring). Risk acceptance and ownership by TasRail management was based on a tiered risk ranking from T1 (low – project managers and supervisors) to T36 (extreme – CEO).

Assessment of risk from identified hazards was to be performed by 'appropriately qualified staff', using a qualitative TasRail risk assessment matrix. All identified risks, including environmental and health and safety risks, were to be contained within a risk register. The risk owner (the delegated accountable manager) was required to ensure the timely implementation of risk controls and arranging periodic reviews for critical and high risks (annually), and moderate and low risks (every 3 years). In addition, CGR-BCP-001 required a reassessment of risk and update to the risk register during a significant change, as triggered by the change management process (BIC-PRO-301).

Risk assessments for remotely-controlled train operations

Examination of TasRail records identified 3 safety risk assessments for the generation 2 RCE operations. These were for:

- RCE commissioning, maintenance, and operations, conducted in December 2009 (prior to generation 2 RCE implementation) and revised in December 2011 (after implementation)
- main-line driving between Devonport and Railton, conducted in January 2014
- unloading and loading operations, conducted in June 2014.

The December 2011 revised risk assessment identified 39 safety hazards, including the following relevant hazards and associated risk controls:

- maintenance or transit damage causing RCE 'to fail safe or operate abnormally', mitigated by safety checks, authorised maintainers and repairers, and proper shipping methods
- failure of vigilance or tilt functions, mitigated by daily tests
- loss of communications, with the relevant control stated as 'loss of communication causes system to revert to a safe mode'
- brake or throttle control failure on the transmitter, mitigated by:
  - primary and secondary[70] emergency stop controls
  - ADE's 'safety analysis of [the] system'
  - emergency alarms to train control
  - safety checks before use
  - fault reporting processes.

This risk assessment did not explicitly define the meaning of 'operate abnormally' as it might relate to the potential for the RCE to fail to an unsafe state. Neither of the other 2 risk assessments identified the potential for a fail-to-unsafe[71] RCE event as a potential hazard.

The January 2014 risk assessment (RCE main-line operations) identified hazards related to driver unfamiliarity with RCE, level crossing collision and track warrant authority exceedance. For the authority exceedance hazard, the risk controls were driver qualification and a 'proven remote control [RCE] fail safe system'. The method with which this fail-safe design was developed and how this had been proven was not explained further. Risks associated with the operational configuration of TasRail's remotely-controlled trains (such as operating from the driver's van while propelling at maximum track speed) were not assessed.

Among the hazards assessed in June 2014 were undesired train movement during loading and unloading, resulting in cement spill. The controls for the unloading hazard comprised driver competency and driver communication. For the loading hazard, the Railton loading interlock was the only nominated control.

There were no additional risk assessments conducted prior to the introduction of generation 3 RCE. During March–April 2018 (post-implementation of generation 3 RCE), TasRail completed a further risk assessment in relation to the risk of a collision resulting from failure of RCE on the cement train. There was no explanation about the type of failure assessed, or how the identified risk controls would mitigate the risk. Identified controls included (paraphrased):

- driver competency
- January 2014 (generation 2 RCE) risk assessment for main-line driving
- new generation 3 RCE

---

70 This refers to the independent remote stop mechanism discussed in *Independent stop mechanisms*.

71 Fail-to-unsafe: a failure of a system whereby it fails to a dangerous state (for example, the train's brakes do not apply in the event of a system failure).

- driver's van emergency brake valve.

Several additionally-identified risk controls relied on a radio link between the RCE transmitter and RCE receiver or continued functioning of the receiver. These were:

- tilt function
- vigilance function
- communication failed mode
- transmitter flat battery warning.

Only one of the risk controls, the driver's van emergency brake, enabled operation independently of the RCE. However, it required the driver to be in the driver's van to operate it, which was not addressed in the risk assessment.

The residual risk from the 2018 risk assessment was rated at the lowest end of medium, requiring monitoring. CGR-PRO-100A classed this rating as follows:

> - Most controls are designed correctly and are in place and are reasonably effective.
> - Some additional action(s) are required to improve the effectiveness and reliability of controls to provide reasonable assurance that objectives will be achieved.

Design assurance processes

TasRail had 2 documents for the design and verification of rolling stock: RS-PRO-017 (*Design procedure – rolling stock*) and RS-PRO-016 (*Design verification, validation, and acceptance procedure – rolling stock*). Jointly, they provided process requirements such as:

- responsibility involvement of relevant stakeholders
- technical specification, which can include a design process, accreditation and engineering standards
- a plan for how requirements and standards would be met
- staged process reviews, including that 'calculations and decisions for defined critical systems have been independently checked and verified'
- risk assessment, including safety risks, and risk assessment workshops
- review of identified failure modes (for reliability), including the suggested use of specialised techniques such as failure modes and effects analysis (FMEA)[72]
- design and development planning
- documentation requirements
- configuration management
- verification and validation
- design endorsement, approval, and acceptance.

RS-PRO-016 stated:

> Any change that results in a departure from the approved design shall be documented and may require further verification and validation prior to such acceptance being granted.

The process also stated:

> Design acceptance can only be granted by a Certified [chartered] Engineer. This is required particularly for all designs and modifications that are classified as Safety Critical.

RS-PRO-017 and RS-PRO-016 were not referenced by, or otherwise linked to, other TasRail processes, such as those for change management and risk management.

[72] FMEA: a systematic approach to document the potential effects of component failures in a system.

These engineering processes stated the intent to meet the 'design elements set out in AS [Australian Standard] 4292.1 and AS 4292.3' (see *Design assurance standards*).

Regulatory oversight

Relevant legislation

In Tasmania, the *Rail Safety National Law (Tasmania) Act 2012* adopted the *Rail Safety National Law (South Australia) Act 2012* (RSNL) and the subordinate Rail Safety National Law National Regulations 2012. That is, the South Australian Act and the national regulations applied in Tasmania. Prior to the application of this legislation, rail safety in Tasmania was regulated by a state-based regulator (the Tasmanian Rail Safety Regulator).

General regulatory approach

The 2018 publication *The ONRSR way*[73] stated that ONRSR's primary objectives were to encourage safe rail operations, ensure compliance with the RNSL and to promote and improve national rail safety, using a risk-based regulatory approach. This was done through a co-regulatory framework. Co-regulation, while not unique, was not common in the transport industry. *The ONRSR way* explained:

> …The nature of the RSNL means that we are not a technical regulator.
>
> The regulatory framework is co-regulatory in that the Australian governments do not directly prescribe the standards or rules by which railways need to operate. Rather, they set a performance requirement on railways to operate safely and provide operational flexibility to establish and implement standards, rules and methods of operation necessary to meet the safety performance requirement of their operations. The co-regulatory framework of the RSNL enables us to tailor our approach to each operator and their circumstances, while at the same time aiming to present a consistent regulatory approach to the rail industry so as not to surprise…
>
> The co-regulatory framework is strongly founded on the distribution of responsibility for the management of risks to safety, which is expressed in the RSNL through the:
>
> - principle of shared responsibility for rail safety risks;
> - establishment of specific safety duties for rail transport operators, designers, manufacturers and suppliers to the rail industry, loaders and unloaders of freight and rail safety workers; and
> - establishment of the role and function of the Regulator [ONRSR]…
>
> Co-regulation is not a partnership between ONRSR and the rail industry when it comes to the obligation to ensure, so far as is reasonably practicable, the safety of railway operations.
>
> This responsibility clearly rests with those parties that are directly in a position of control and management of railway operations, which is principally the accredited or registered rail transport operators and their various suppliers and contractors.
>
> The overall success of this regulatory framework to address and mitigate risks to safety is predicated on individual operators and the broader industry fulfilling their respective roles in engaging the appropriate expertise and competence towards collaboratively identifying and assessing risks and developing, applying and maintaining standards and processes to manage safe railway operations…

In terms of how this approach was intended to be applied, *The ONRSR way* stated:

> We [ONRSR] have the dual, but complementary, roles of administrator of the RSNL accreditation regime and the regulator of a duty-based safety management regime (an educator, monitor, and enforcer). The nature of the RSNL means we are not an approver of equipment, services or processes.

[73] ONRSR 2018, *The ONRSR Way*, pp. 8-9. Version 2 of *The ONRSR Way* was published in 2020 and the information referenced in this report was effectively the same in both versions.

> In conducting these roles, we seek to engage with operators in a way that directly influences those with the ultimate responsibility for delivery of safe railway operations and environments. We take a predominantly facilitative approach to regulating safety, with our rail safety officers collectively acting as a safety conscience and compliance coach to our regulated parties, targeting education where necessary and giving opportunity for operators to address identified safety issues. However, where this is not effective with individual operators or more immediate, publicly accountable action is required, we will employ the range of enforcement options available to us to secure safe outcomes and compliance with the law.

The ONRSR Way stated that ONRSR's role was to administer accreditation, monitor safety management performance, and ensure operators and duty holders comply with the requirements and safety management standard set by the law (the RSNL).

Rail transport operators (RTOs) were responsible for the establishment and implementation of the standards, rules and procedures for safe operation. They were also, along with contractors, suppliers, and manufacturers, accountable for ensuring (so far as is reasonably practicable) safe operations and activities. Rail industry standards groups (such as the Rail Industry Safety and Standards Board or RISSB) supported this through the development of 'good practice' guidance or standards.

ONRSR's monitoring, investigation and enforcement activities were undertaken through an array of regulatory activities, which were:

- reviewing notifications of change, which may have impacted an RTO's accreditation (see *Notification of change*)
- enquiries, meetings, site visits, inspections, audits and investigations
- advice, education, and non-conformance reports
- review of operators' safety performance reports or annual activity statements
- notifiable occurrence response
- issuance of statutory notices, such as improvement, prohibition and infringement notices
- acceptance of enforceable voluntary undertakings
- prosecutions
- additions of conditions / restrictions, or suspension, or cancellation of RTO accreditation / registrations.

Notification of change requirements and guidance

General information

As outlined in regulation 9(1)(a) of the national regulations, accredited[74] RTOs were required to notify ONRSR of proposed decisions, proposed events or changes to their operations.

The regulation prescribed 12 items of railway operations to which this requirement applied (reproduced in Appendix C). No item numbers under regulation 9(1)(a) explicitly mentioned notification of changes to ONRSR relating to RCE. In response to questions by the ATSB, ONRSR advised that TasRail could have submitted a notification of change in relation to the generation 3 RCE based on one of the following notifiable items:

> …Table Item 3 – change to a safety critical element of existing rolling stock, if the operator believed that the change to the remote control equipment (RCE) changed a safety critical function that it performed; or

[74] An accredited RTO had satisfied ONRSR that it had '…the competence and capacity to manage the risks, implement the controls and manage changes associated with the railway operations for which it is accredited'. Source: ONRSR 2014, *Regulatory response to the management of change policy*, p. 9.

> Table Item 5 – change to safety standard for the design of rail infrastructure or rolling stock, if the operator believed the change represented a change to the expected or required safety performance (standards) of the equipment.

Timeframes for notifying ONRSR of a change were also nominated in the regulation, which were typically 28 days before implementation.

The ONRSR *Notification of change to railway operations* form required RTOs to:

- provide a description of the change
- advise change management procedures that were or would be followed
- advise whether risk assessment of the change had been conducted
- advise risk controls for the change that were, or would be, in place
- advise whether consultation with affected parties was or would be conducted.

Regulator actions in response to a notification of change

The *ONRSR Internal Framework – Risk based Regulation* document described the regulator's role of encouraging and promoting improvements to rail safety through '...an approach to regulation in which regulatory effort is commensurate with risk and scope for improvement'. The framework ranked ONRSR's decisions in 3 tiers that determined their impacts to rail safety. Decisions related to notification of change and follow-ups were ranked as tier one decisions; that is, those that had the 'greatest potential impact on rail safety…made to directly fulfil primary functions of ONRSR'.

The ONRSR internal notification of change process was detailed in the *Notification of change procedure*. The process required that the assigned branch accreditation manager would perform an initial review to determine if:

- the change was within the RTO's scope of accreditation, including conditions and restrictions (if not, change was not permitted and a variation of accreditation was required)
- there was an immediate risk to safety posed by the change (if so, immediate regulatory compliance and enforcement action was invoked)
- further information was required:
  - to assess the extent and impact of the change
  - to confirm that change management and risk management processes were being followed
  - in instances where there was significant change to the RTO's SMS or risk profile.

Where further information was required, a rail safety officer (RSO) was then allocated the notification of change for follow-up and review. The assistance of ONRSR technical specialists could be sought to assist rail safety officers during this review process.

ONRSR did not approve or reject notifications of change. Rather, based on any further information received, previous RTO compliance history, the type of rail operation and SMS maturity, ONRSR could undertake further regulatory activities either prior or post the notified change taking effect. These included:

- meetings
- site visits
- inspections
- audits.

Guidance for the interpretation of the notification of change regulation

The ONRSR Way stated that, to provide a consistent regulatory approach, ONRSR aimed to (among other things):

> ...provide a single, common interpretation to the RSNL and our expectations on operators arising from this interpretation (made public through our published guidance material)…
>
> …We have an important role of interpreting the RSNL, explaining this to regulated parties, and acting consistently with this interpretation…ONRSR develops comprehensive guidelines which clearly articulate our expectations in relation to complying with the RSNL. These guidelines provide key information and clarification to both the rail industry and public on legislative, regulatory and technical matters.

For the notification of change process, ONRSR provided guidance to RTOs and ONRSR staff within several documents:

- *ONRSR Notification of change policy*, which provided direction on the requirements for a notification of change
- *ONRSR Regulatory response to the management of change policy*, which defined ONRSR's regulatory requirements for accredited RTOs planning change to their railway operations
- *ONRSR Notification of change guideline*, which provided advice regarding requirements for the submission of a notification of change
- *ONRSR Notification of change fact sheet*, which provided an overview of the process
- *The ONRSR Way*, which provided an explanation of 'how ONRSR intends to work … operationally and strategically', including ONRSR's functions and powers, and the application of the co-regulatory framework
- *ONRSR Notification of change procedure,* which was for internal use only, and included:
  - guidance to ONRSR rail safety officers on key areas to be addressed in processing the notification of change that were not detailed in the rail safety legislation
  - responsibilities and accountabilities for tasks within the process
  - communication of information to the relevant parties (internal and external)
  - management of internal systems, including the records required to be captured throughout the process.

The ONRSR *Notification of change policy* stated that 'routine operational and administrative changes that occur within railway operations' should be managed by the operator's management of change procedures and were not required to be notified to ONRSR. The available guidance for interpretation of the 12 items nominated in regulation 9 is discussed in the following subsections.

With the exception of *The ONRSR Way* and *ONRSR Notification of change procedure*, all of the above ONRSR documents contained a recommendation that an RTO '…contacts the ONRSR to discuss the change/s…' prior to submission of the *Notification of change to railway operations* form if the RTO was unsure whether the change was within the scope of its accreditation or whether regulation 9(1)(a) reporting requirements applied.

ONRSR advised the ATSB that RTOs could contact either the head office (in Adelaide) or their local rail safety officer for notification of change clarifications. An ONRSR representative advised the ATSB that rail safety officers were expected to either: seek internal assistance (for example, the director of operations, legal counsel or the technical team) if unsure how to answer a clarification enquiry; or, alternatively, advise the RTO to submit the notification of change. ONRSR advised the ATSB that there was no specific internal guidance to assist rail safety officers when answering notification of change clarification requests.

Terms pertaining to the notification of change

With regard to item 3 in regulation 9, definitions for 'safety critical element of rolling stock' or 'safety critical' were not provided in the *Rail Safety National Law* (South Australia) or the *Rail Safety National Law National Regulations 2012* (NSW).

The *Notification of change guideline*[75] included interpretations and examples for 3 of the 12 notifiable items in regulation 9(1)(a). These related to changes to rail infrastructure (item 4, one descriptive paragraph), network rules (item 8, one descriptive paragraph) and work scheduling practices related to fatigue risk management (item 10, 2 descriptive paragraphs). There were no interpretations and examples included for items 3 or 5.

The *Notification of change procedure* stated that its purpose was, in part, to provide rail safety officers with '…key areas to be addressed in processing the Notification of Change which are not detailed in the rail safety legislation'.[76] However, this document did not provide a definition or examples of what constituted a 'safety critical element of existing rolling stock', the interpretations of the terms 'safety critical' or 'change'.

Interpretation of 'element of ... rolling stock'

The RSNL and Regulations defined 'rolling stock' as:

> …a vehicle that operates on or uses a railway, and includes a locomotive, carriage, rail car, rail motor, light rail vehicle, train, tram, light inspection vehicle, self propelled infrastructure maintenance vehicle, trolley, wagon or monorail vehicle…

RCE was not explicitly defined in the legislation or the related guidance (as an element of rolling stock or otherwise). ONRSR advised the ATSB that, in relation to generation 3 RCE, it had '…the primary purpose of enabling the driver to control the movement and operation of the locomotive, [therefore it] is considered an element of the rolling stock (locomotive)'.

Interpretation of 'safety critical'

The *Notification of change fact sheet* included the following definition:[77]

> Safety critical elements: are identified in the [RTO's] safety management system and include any component part of equipment, plant or system whose failure could substantially contribute to a major accident.

Additionally, ONRSR advised the ATSB that:

> Safety critical, is not defined in the RSNL and scope is given for an operator [RTO] to interpret this in the context of their own railway operations. It is typically taken to mean elements of rolling stock that are critical to the safe operation or movement of rolling stock, particularly in regard to preventing unsafe/uncontrolled operation or are critical in being able to respond to mitigate or prevent risks to safety of persons, includes but not exclusively, braking systems, coupling, communications, safety recording devices, automated train protection systems etc.

In addition, prior to commencement of the RNSL and national regulations, each state and territory had its own rail safety legislation, including definitions. The *Rail Safety Regulations 2010 (Tasmania)*, which required a notification of change to the then-regulator for Tasmania for 'a change to a safety-critical element of existing rolling stock', did not define 'safety critical'. In

---

[75] ONRSR transitioned to the use of an online portal for some functions in late 2018, after (and unrelated to) the Devonport runaway accident. Among other things, the online portal replaced the previous forms, processes, and guidance related to the notification of change discussed in this report. With respect to the items listed in regulation 9(1)(a), the portal only had guidance for rail infrastructure (item 4).

[77] The term 'safety critical element' was not used in any of the other 11 listed items requiring a notification of change. When ONRSR transitioned to the use of an online portal for some functions in late 2018, this definition was no longer included.

contrast, Schedule 5 of Queensland's repealed *Transport (Rail Safety) Regulation 2010* included the following definition:

> safety critical element, of rolling stock, means any part of the rolling stock that could cause, or affect the impact of, an accident or incident if the part failed to operate properly.

Interpretation of 'change'

ONRSR advised the ATSB that, although guidance on interpretation of the extent of change notifiable for regulation 9(1)(a) was not provided to RTOs, internally it would consider a change notifiable under item 3 if:

> …the change involved a change to how a safety critical element of rolling stock is likely to perform or is operated. A like-for-like (replacement/repair) would not be considered a change but a minor/major redesign for the element to behave differently or require 're-training' for use would.

Other definitions of 'safety critical'

Appendix E of AS 4292.3-2006 (*Railway safety management, part 3: rolling stock*), effectively superseded in 2017, provided a recommended list of 25 items that should be considered 'safety critical items' on rolling stock.[78] Although RCE was not mentioned on this list, 'braking systems' and 'event recording equipment' were included. The information provided in the standard was not reproduced among the RISSB products that superseded AS 4292.

Australian standard AS 7501:2013 (*Rolling stock compliance certification)* did not define 'safety critical.' A related standard, AS 7702:2014 (*Rail equipment type approval*), defined it as 'directly influencing safety (when applied to equipment or systems).' Notably, this standard specifically excluded rolling stock in its scope, but allowed for application of its principles to rolling stock, except where there was conflict with AS 7501.[79]

AS 7702 also required the supplier to provide documentary evidence of safety and specified that products typically require type approval if (in part):

- the product is used in a safety critical function where its failure can directly affect the safety integrity of the railway
- the product is used in a function where its failure will affect the railway.

TasRail notifications of change

Generation 3 remote control equipment notification of change

ADE advised the ATSB that, although it had interactions with the Tasmanian Rail Safety Regulator during development of generation 1 RCE, it did not interact with ONRSR for generation 3 RCE.

TasRail defined 'safety critical' in its documents RS-PRO-016 (*Design verification, validation and acceptance procedure – rolling stock*) and RS-PRO-017 (*Design procedure – rolling stock*) as 'any element whose failure or malfunction may result in death or serious injury to people, or loss or severe damage to equipment or environmental harm.'

On 19 December 2017, in response to a request by the final project manager, TasRail's risk and compliance manager sought clarification from ONRSR to confirm whether a formal notification of change was required. The manager advised the ATSB that they had a phone conversation with an ONRSR rail safety officer, during which several items were discussed, including the generation 3 RCE project. The TasRail risk and compliance manager recalled that they advised the rail safety officer the RCE was like-for-like with the addition of a dynamic brake.

---

[78] AS 4292 *Railway Safety Management* provided a set of railway safety requirements for incorporation into the management systems of railway organisations. It was published progressively from 1995.

[79] There was no requirement for TasRail to comply with the requirements of AS 7501 or AS 7702.

The ONRSR rail safety officer made a note of this conversation in their official notebook for recording their activities and interactions with RTOs:

> Replacement / upgrade of Remote Control System on Cement Train.
>
> The locomotive remote control unit will be replaced shortly. [The TasRail risk and compliance manager] advised this is a like for like replacement of the existing unit which has been in operation for some time and due for routine replacement. I confirmed to [the TasRail risk and compliance manager] that this is not a notifiable change.

There was no mention in this note that the manager had advised the rail safety officer of the addition of dynamic brake to generation 3 RCE.

Consistent with this conversation, TasRail did not submit a formal notification of change in relation to the generation 3 RCE project.

Previous TasRail activities regarding the notification of change

A review of the notification of change submissions received by ONRSR determined that 15 were submitted by TasRail between May 2015 (commencement of the generation 3 RCE project) and the day of the accident. Of these, 6 were related to introduction, re-introduction or changes to rolling stock. Seven required requests for further information by ONRSR, including 3 that had been submitted incomplete.

ONRSR advised the ATSB that it did not receive a notification of change from TasRail relating to the conversion of the DQ and 2050 class locomotives and generation 2 RCE from a 3-pipe to 4-pipe braking configuration in 2014.

Occurrence notification

TasRail was required to report 'Category A' notifiable occurrences immediately to the ATSB,[80] with a follow-up written report within 72 hours to ONRSR. For 'Category B' notifiable occurrences, TasRail was required to provide ONRSR with a written report within 72 hours of the occurrence.[81]

Depending on the type of failure, failure events of generation 3 RCE could have been considered notifiable occurrences under the following legislative subparagraph:

- 57(1)(b)(xvii) the detection of an irregularity in any rolling stock that could affect the safety of railway operations [Category B].

TasRail's risk and compliance manager was responsible for advising the ATSB and / or ONRSR of Category A and B notifiable occurrences. These were based on risk wizard entries, which, in the case of RCE failures, were created by the NCO receiving the RCE driver's report (see *Fault reporting process*).

A review of both the ATSB and ONRSR notification and occurrence databases found no reports of notifiable occurrences received from TasRail in relation to generation 3 RCE, apart from the accident on 21 September 2018. The risk and compliance manager advised that instances of RCE failing-to-safe were likely not recognised by NCOs as being of a safety concern and therefore not placed in risk wizard.

---

[80] The requirement for reporting Category A notifications changed after the runaway. From 1 July 2019, significant (Category A) rail safety occurrences were required to be reported to ONRSR.

[81] *Rail Safety National Law* (South Australia), section 121, *Rail Safety National Law National Regulations 2012* (as published on NSW legislation website), regulation 57.

Requirements and guidance related to system safety

Safety management systems

The RSNL regulations required operators to have safety management systems (SMS) with 30 elements that included:

- a safety policy
- safety culture
- governance, compliance and internal control arrangements
- individual accountabilities
- safety performance measures and audit arrangements
- change management and risk management procedures
- engineering standards and procedures, and operational systems, safety standards and procedures, including for engineering design of rolling stock.

ONRSR also provided guidance on SMS implementation.

Major projects guidance and expectations

In 2014, ONRSR issued *ONRSR Guideline – Major Projects* to 'provide guidance to the industry as to how projects can safely manage major change.' The guideline stated:

> In the context of this guideline, a major project is considered to be an entity, or entities, that are managing the delivery of a significant change to railway infrastructure or rolling stock.

There was no definition for what constituted a 'significant change' in this context, although the guideline separately stated that major projects involve multi-disciplinary activity, complex contractual structures, and intricate organisation structures.

The guideline was not intended to apply to complex, safety-critical projects that did not include these types of activities and structures, such as the development of the generation 3 RCE. However, it referred to methods, standards and other guidance on systems engineering and safety assurance principles that could be beneficial for complex, safety-critical projects other than major projects. These included:

- safety assurance planning
- independent safety assessment
- documented safety limits (that is, the limits of acceptable risk)
- human factors integration, including human-system interface assessment and risk-based training needs assessment
- 'good practice system engineering principles' such as safety requirements management, 'V-model' principles (see Appendix B), use of relevant safety standards such as IEC 61508 and EN 50126/8/9, and management of project-specific risks.

Design assurance standards

There was no regulatory framework for national or state-wide type approvals for rolling stock. Rather, there could be a form of type approval process within the SMS (as TasRail had). Similarly, there were no prescribed regulatory requirements for RTOs to follow systems engineering or system safety design processes for rolling stock or infrastructure other than those nominated by the RTO itself.

There were voluntary Australian Standards (AS) relevant to rail safety, including:

- AS 4292 *Railway safety management* (withdrawn—see below)
- AS 7501 *Rolling stock compliance certification*
- AS 7702 *Rail equipment type approval.*

AS 4292 (*Railway safety management*) was 'prepared primarily with a view to achieving uniformity in the management of railway safety both as a general principle and with specific reference to the accreditation of railway industry participants.' It comprised 6 parts (AS 4292.1 through AS 4292.5, and AS 4292.7).[82]

AS 4292.1 contained information about safety management systems, risk management, and related processes, including engineering design control processes. It included the requirement to 'implement and maintain a documented set of engineering and operational systems safety standards' to cover all relevant aspects of rolling stock and other systems and infrastructure. With respect to engineering design, it required:

> (a) Identification of the responsibility for each design or development activity.
>
> (b) Safety risk review at both the design input and design output stages taking into account reliability and maintainability.
>
> (c) Assignment of design verification and validation functions.
>
> (d) Control of design changes in accordance with Items (a) and (b).

AS 4292.3 provided information about establishing processes for the design of rolling stock. It included:

- a recommendation to identify hazards that might affect the 'integrity' of rolling stock and trains
- a requirement to establish standards and procedures for the selection and design of rolling stock, including braking systems, electrical equipment, and 'operation of rolling stock, safety elements'
- a requirement to establish standards and procedures for the verification and validation of all stages of the design of rolling stock, including conformance to safety requirements and standards, with an 'appropriate level of independence from the design process' depending on the risk of process error and the overall level of safety risk
- a recommendation to have an inspection and test plan, including 'verification that the system conforms to the design and operating requirements of the client and the operating parameters of the railway' and 'validation that the installed system conforms to the required safety standards and client requirements'
- a recommendation to include 'commissioning tests' for 'operation of rolling stock safety elements', which included driver's controls and warning devices
- a recommendation for monitoring to identify 'safety critical faults'
- a recommendation for consideration of the effects of modifications to rolling stock on the railway system as a whole, and the need to follow design processes for the modification
- recommended lists of items to be considered when developing performance standards during the design stage, which included 'safety critical items' such as braking systems.

In 2017, Standards Australia announced that the 6 parts of AS 4292 were to be withdrawn. RISSB advised in a technical note to industry that most components from AS 4292 had been absorbed into other standards, codes of practice and guidelines.[83] AS 4292 was withdrawn in 2021.

AS 7501 (*Rolling stock compliance certification*), first issued in 2013, included process requirements for the design or modification of rolling stock. These requirements included independent verification by a person with (among other attributes) demonstrated experience and knowledge of the requirements of AS 4292 and experience in assessing rolling stock against standards. There was no requirement or recommendation to produce a safety case or conduct specialised hazard analysis techniques such as FMEA.

---

[82] AS 4292.6 was absorbed into AS 4292.1 as part of a revision in 2006. From 2017, Standards Australia no longer maintained the AS 4292 suite of documents.

[83] RISSB n.d., *AS 4292 Railway safety management technical note*.

The comparable voluntary standard primarily intended for use with rail infrastructure (AS 7702 *Rail equipment type approval*), first issued in 2014, had the following requirements:

> The supplier shall provide documentary evidence of satisfying the RTO's safety requirements.
>
> In relation to the above clause the supplier should provide details and reports for any safety analysis such as Safety Integrity Level demonstration (including documentation on which any report is based) either carried out by the Supplier, or independent reports…
>
> The Supplier should provide details of:
>
> (a) failure modes, degraded modes (effect on operation of partial failure), emergency operation;
>
> (b) the effect on railway operations of degraded modes of failure;
>
> (c) emergency operations;
>
> (d) fire performance: flammability and smoke;
>
> (e) vandal resistance.

AS 7702 additionally stated:

> Safety may, for example, be demonstrated by Independent Safety Assessor Report, Safety Case document or FMECA[84] analysis with risk assessments being undertaken in accordance with AS/NZS ISO 31000 [*Risk Management*].

In other words, this voluntary standard for rail infrastructure identified the use of a safety case or analysis to support the evaluation of system safety, but this guidance was not present in the equivalent standard for rolling stock.

Event recorders

Event recording used on TasRail cement trains

Three devices with recording capability were fitted to the TR class locomotive:

- a forward-facing, closed-circuit television
- a dedicated event recorder
- the system for automated locomotive computer control (SAL).

Parameters recorded by the event recorder and the SAL differed to some extent, and both recorded parameters that were not replicated on the other. Although not its primary function, the SAL recorded parameters relating to locomotive control.

A data recording device was also fitted to the driver's van, which was only capable of recording driver's van headlight and horn operation. With no link to the locomotive or RCE, the usefulness of any data recovered would have been minimal.

A data logger was not included in the generation 3 RCE. TasRail enquired about the addition of data recording to the generation 3 RCE on 2 further occasions in May and June 2018, both times coinciding with RCE operational events. This request progressed as far as ADE providing a quote for the inclusion of a recording capability in June 2018 at an additional cost of about 4% of the total cost of the 2 RCE sets; TasRail had not progressed this further by the time of the 21 September 2018 runaway.

Requirement to use an event recorder

There was no explicit requirement in the RSNL or the national regulations for a train or locomotive to be fitted with an event recorder. ONRSR personnel advised that modern locomotives were generally fitted with an event recorder.

---

[84] FMECA: failure modes, effects and criticality analysis. This is similar to a FMEA but with the addition of quantified probability-severity analysis.

TasRail's accreditation, as RTO, which was initially issued by the Tasmanian Rail Safety Regulator, was transitioned across to ONRSR in January 2013.[85] The transitioned notice of accreditation included conditions and restrictions. One condition related to event recorders, which stated:[86]

> All leading locomotives or other vehicles used as the leading vehicle of a train shall be fitted with an operating event recorder.

The condition was not restricted to any type of train, and therefore applied to TasRail's remotely-controlled train operations as well as its other train operations.

As previously stated, when operating the cement service, the locomotive was the leading (front) vehicle when travelling to Devonport and the driver's van was the leading (front) vehicle when travelling to Railton. However, the RCE receiver was providing the driver's interface and command outputs to the locomotive at all times. Therefore, although TasRail did not explicitly define a 'leading vehicle' in the cement train consist, it was reasonable to consider that the RCE was fulfilling this function because it assumed the controlling role of a lead locomotive over airbrake, throttle, direction, and other safety-related controls such as the vigilance function.

ONRSR described in *The ONRSR Way* that one of the purposes for accreditation conditions and restrictions was:

> …to secure a specific method of operation or use of technology that the operator [RTO] has committed to in order to achieve accreditation (meaning that the operator [RTO] will need to apply for a variation to accreditation to change this).

ONRSR advised the ATSB that the 'condition on requirement for event recorder' was a legacy condition transitioned from the previous state regulator upon changeover to the Rail Safety National Law. However, *The ONRSR Way* indicated that ONRSR did have the discretion to remove conditions unilaterally:

> …we will monitor the effectiveness and relevance of what [conditions] we have imposed. We will act to remove these, without initiation by the operator, should we decide that the condition or restriction is no longer needed for our purposes.

An ONRSR representative stated that it was not common for a condition related to event recorders to appear on an RTO's accreditation notice. Although they were not aware why this legacy condition was on TasRail's notice of accreditation, they believed it would have been for a safety reason.

The Tasmanian Department of State Growth indicated that it did not retain a copy of the previous notification of accreditation permitting the use of remote control locomotives or records indicating why the requirement for event recorders was originally applied.

In relation to the event recorder condition on TasRail's notice of accreditation, ONRSR advised the ATSB:

> Whilst the condition calls specifically for the event recorder being fitted to the leading vehicle, ONRSR considers an event recorder fitted anywhere in the consist, that is recording the key parameters, as meeting the intent of the condition.
>
> There is no requirement to log control inputs of remote control equipment.

ONRSR did not provide further definition or explanation of what were considered 'key parameters'.

TasRail were requested to provide safety management system (SMS) documents relating to requirements for event recorders on its trains. In response, it provided a procedure that applied to 'the collection and retention of Data Logger data'. The procedure did not include any requirements or references stating what parameters had to be recorded. Therefore, there was no evidence

---

[85] *Rail Safety National Law (Tasmania) Act 2012*, section 13(2).

[86] Event recorder: a device installed on rolling stock capable of recording multiple input parameters, in digital or analogue format, related to the operation of the rolling stock. Also known as a 'data logger' or 'data recorder'.

provided to indicate what parameters TasRail required to be captured on its event recorders in order to meet its condition of accreditation.

External guidance on event recorders

Following an accident involving an inter-urban passenger train at Glenbrook, New South Wales, in December 1999, which resulted in 7 fatalities, a Special Commission of Inquiry noted that there was no data logger (event recorder) fitted to the train, and that this hampered the effectiveness of the investigation. In relation to this aspect, the inquiry final report made the following recommendation:

> All trains be fitted with data loggers to enable, among other things, train driver performance to be monitored.

Following an accident involving a suburban passenger train at Waterfall, New South Wales, in January 2003, which resulted in 7 fatalities, a Special Commission of Inquiry noted that there was a data logger fitted to the train but it was not operational at the time of the accident. The commission's report found that the absence of recorded data hindered the establishment of important facts. The commission final report stated (McInerney 2005):

> The data loggers, and the data they provide, are crucial to the monitoring and improvement of the reliability of rolling stock, because of the data obtained relating to the performance and maintenance of the rolling stock…They are an essential piece of equipment for the determining of the causes of incidents and accidents…
>
> Data loggers are such an important piece of equipment that, in my opinion, it should be mandatory for all trains to be fitted with them and rail organisations should not be accredited to operate on the New South Wales rail network unless each train is fitted with an operational data logger. This requirement should be a condition of accreditation for any organisation seeking to operate on the New South Wales rail network.

AS 4292.3:2006 (*Railway safety management, part 3: rolling stock)*, effectively superseded in 2017 as described in *Design assurance standards*, listed 'event recording equipment' among a list of 'safety critical' items 'to be considered when developing performance standards … for new or modified vehicles.'

AS 7527:2015 (*Rolling stock event recorders*) 'describes the requirements for event recorders installed in locomotive… rolling stock vehicles'. Although use of the standard was not mandatory, it gave RTOs guidance about which parameters an event recorder should monitor in order 'to ensure that event recorders fitted to rolling stock capture a minimum set of appropriate data for the use of rollingstock operators, rail infrastructure managers, investigators and maintainers for forensic investigation of rail incidents'.

The standard specified what information was required to be recorded in order to achieve compliance with the standard. It separated the information into either 'mandatory' or 'recommended' requirements.[87] The standard also indirectly contained requirements for some parameters to be displayed to the driver.

Appendix D provides a review of parameters that were identified as relevant to the 21 September 2018 runaway accident, the requirements detailed in AS 7527, and comment on their application to RCE operations. In summary, some mandatory and recommended data relevant to the RCE (such as driver inputs and the vigilance function) were not recorded when using the RCE. In some cases, the locomotive response to driver input was recorded but this did not meet the intent of the standard (for example, train direction was recorded at the locomotive, but direction as selected by the driver on the RCE transmitter was not recorded).

---

[87] A mandatory requirement was defined as a requirement that the standard provided as the only way of treating the hazard. A recommended requirement was defined as one where the standard recognised that there are limitations to the universal application of the requirement, and that there may be circumstances where the control cannot be applied or that other controls may be appropriate or satisfactory.

Other specific requirements in AS 7527 for a 'driverless vehicle or remote-operated vehicle' were not recorded on TasRail trains under RCE control, including:

- all changes to the operational status of the vehicle (mandatory)
- all control messages received and transmitted by the vehicle (mandatory)
- all status messages received and transmitted by the vehicle (recommended).

Effect of non-recording of remote control equipment data

Although the TasRail locomotives did have data recording capability, they did not record the functioning of the generation 3 RCE (that is, parameters relating to the RCE modes, states, inputs, and outputs). This hindered the TasRail and ADE investigations into the Caroline Creek event and other potential precursor events. One of the TasRail representatives who had worked with ADE to address identified faults with the generation 3 RCE told the ATSB that recording capability would have assisted in both fault finding and rectification.

TasRail representatives asked ADE in February 2018 if there was a data capture port fitted to generation 3 RCE after multiple faults were encountered, and in May 2018 further indicated that data logging capability would be beneficial and help determine and/or understand the root causes of any issues.

ADE did not directly address the addition (or the absence) of data recording on the RCE in correspondence, but indicated that it was experiencing difficulties replicating faults reported on the cement train. For example, ADE suggested to TasRail that, upon drivers encountering unrecoverable faults, drivers should record video of what the RCE was reporting and doing when trying to recover to assist in fault condition identification.

The absence of recorded RCE data significantly hindered investigations into the runaway accident. There were insufficient parameters recorded to identify or replicate the failure state that the RCE had encountered, or to determine the states, modes, inputs and outputs of the RCE with a high level of confidence.

TasRail's internal investigation report noted that the absence of recorded RCE data meant that investigators could not determine why communication was not restored. Similarly, ONRSR's enquiries into the accident noted that the absence of recorded data prevented a full examination of driver actions and RCE receiver responses and recommended that the recording of RCE data should be considered for any future remotely-controlled train operations.

Safety analysis

Introduction

On 21 September 2018, TasRail freight train no. 604 rolled away from a cement loading facility at Railton, Tasmania. There was no train crew on board the train at the time. Travelling predominantly on down gradients toward Devonport, the train's speed was uncontrolled and it exceeded the maximum track speed in place to ensure safe travel through curves, level crossings and points. The train travelled for about 20 km before being routed into a dead-end siding in Devonport, where it subsequently derailed, resulting in damage to the locomotive, 7 cement wagons and some surrounding infrastructure. Two pedestrians within the public area received minor injuries from fence debris.

Given the nature of the occurrence, the extent of injury and damage could have been much worse. A train runaway can cause injury or loss of life, substantial damage to rolling stock and infrastructure, and disrupt rail operations for an extended period. Accordingly, rolling stock operators and rail infrastructure managers need to implement sufficient preventative and mitigating controls to manage this hazard.

In this case, TasRail's cement train service was operated using remote control equipment (RCE). It commenced these RCE operations in August 1999, with RCE designed and built by Air Digital Engineering (ADE). Subsequently, this was upgraded in about August 2010 to ADE's generation 2 RCE, with TasRail commissioning ADE to manufacture the replacement generation 3 RCE in May 2017. Final delivery and commissioning of generation 3 RCE, the equipment used on the runaway train, occurred in February 2018.

It is almost certain that the cement train's TR class locomotive and the locomotive and wagon airbrake systems were operating normally under the control of the RCE on the day of the accident. In addition, the driver was trained and considered competent in RCE operation, and their actions did not contribute to the accident in any reasonably foreseeable way.

Accordingly, this analysis will focus on the performance of the RCE and the controls in place to assure its performance and recover from any failure. More specifically, the analysis examines:

- the performance of the generation 3 RCE during the runaway sequence
- the risk controls in place to prevent an unsecure train from entering the main line
- the processes for responding to emergencies such as a runaway train on the main line
- design and integration problems associated with the generation 3 RCE
- the system safety assurance process used by the RCE manufacturer
- the rolling stock operator's processes for acquiring RCE and managing its operations
- the notification of change to the regulator and guidance for making such notifications
- the rolling stock operator's change management process
- the rolling stock operator's process for fault tracking and analysis
- the recording of RCE functions and the associated requirements for recording
- the guidance available for applying system safety assurance processes in the Australian rail industry.

Remote control equipment in unsafe state

A few minutes prior to the runaway, the driver was nearing completion of loading operations at Railton. During positioning of the last 2 wagons for loading, using the RCE transmitter, the driver misjudged the stop, which required the train to be reversed back into position.

Recorded data from the locomotive showed that, as the train stopped, the direction controller state quickly changed from forward to reverse (without a recorded pause in neutral). Following this:

- there was an immediate venting of the brake pipe, equivalent to an emergency brake application, followed by a recharge of the brake pipe
- at about this time, the RCE ceased to respond to driver commands
- there were a further 2 subsequent emergency brake applications and releases.

Although there was no inherent safety concern with overshooting the stopping mark or reversing the direction, the ATSB later observed during multiple tests that a fast direction change (using the RCE transmitter) resulted in an unintended and momentary activation of the dual direction fault interlock and then emergency vent and recharge of the brake pipe.

The dual direction fault interlock function was designed to activate when forward and reverse direction outputs were detected as being simultaneously selected. However, an unintended consequence of this interlock function was an emergency brake application. The rapid decrease in brake pipe pressure it created resulted in activation of the locomotive's VX vent valves and, in turn, emergency magnet valve (EMV).

Recorded data from train no. 604 showed similar brake behaviour coincident with the change from forward to reverse, indicating that the driver rapidly changing the direction on the RCE transmitter's direction controller resulted in an unintended momentary emergency brake application due to activation of the dual direction fault interlock on the RCE receiver.

The dual direction fault interlock was not a feature that existed on the train's TR class locomotive. Further, the length of travel between forward and reverse positions on the locomotive's direction controller (during non-remotely-controlled train operations) limited the speed with which a change of direction could occur. However, on the RCE transmitter, the small size and ability of the direction controller switch to bypass the gated neutral position allowed almost simultaneous changes of direction.

The dual direction fault interlock function was not described in the RCE operation manual, and it was not assessed during driver training for the generation 3 RCE. A dual direction fault interlock event could also be cleared without intervention by a driver. Therefore, it is likely that the driver of train no. 604 was unaware that a quick change of direction could result in a momentary uncommanded emergency brake application, as occurred during the period prior to the runaway. Certainly, the driver could not have reasonably expected that a fast direction change would result in the RCE becoming unresponsive or lead to a runaway.

Although ATSB testing was able to reproduce the emergency vent and recharge of the brake pipe, testing of fast direction changes did not reproduce the unresponsive state or the following additional events that occurred immediately prior to the runaway:

- the RCE ceasing to respond to driver commands
- 2 subsequent emergency brake applications
- the final release of all train brakes.

Even though the nature of the persistent unsafe state could not be fully understood, the investigation could still determine factors that increased the likelihood of the state occurring, and decreased the ability of the RCE or other systems to prevent or manage the effects of the state. These factors, and others relating to TasRail's remotely-controlled train operations using the ADE RCE, are discussed throughout later sections of this report.

Given the timing of the fast direction change before the immediate uncommanded emergency brake application (and subsequent events), and the absence of any other apparent trigger mechanism, it is likely (but not certain) that the fast direction change was the initiating event of the runaway. By comparison, the Caroline Creek event in May 2018 similarly involved an emergency brake application, but it was probably not initiated by a fast direction change (as the train was en route at the time).

The driver advised the ATSB that, after changing direction from forward to reverse on the RCE transmitter, they applied traction power. On noticing that the train did not respond, the driver observed the message 'Connecting 9863 v1.4' displayed on the RCE transmitter display screen. This message indicated that the transmitter did not have a communication connection to the receiver.

Accordingly, the driver initially treated this as a communication failed mode event (that is, where the receiver had detected communications between the transmitter and receiver had been interrupted for more than 4 seconds). As such, the driver attempted to reset the fault, by configuring the transmitter with full independent brake, automatic brakes applied, throttle to idle, and direction in neutral.

After observing that this was unsuccessful, the driver reported maintaining the RCE transmitter in the reset configuration while they attempted the control fault mode reset (that is, turning the transmitter off and on via the transmitter's key switch). The driver advised that once the train commenced to roll away, they also applied a full-service automatic brake application, followed by tilting the transmitter (which should have activated the tilt function and applied the emergency brake) and removing the transmitter's battery (which should have invoked a communication failed mode brake application).

However, the data recorded on the locomotive did not show locomotive responses consistent with the throttle application, the configuration of the controller required to recover from a penalty mode, or the actions the driver took to attempt to stop the moving train (key switch reset, tilt function or communication failed mode). Instead, the 2 emergency brake applications and releases were observed, followed by all train brakes being released. The configuration of the locomotive during these emergency brake applications, with no independent brake application apparent and the direction remaining in reverse, was not consistent with the RCE's emergency mode or any other documented RCE fault condition.

The driver also thought they operated the transmitter's emergency stop switch, although exactly when in the sequence could not be determined. However, this switch relied on a radio link to function, and based on the driver's observations, the radio link was lost at the beginning of the non-responsive period. Therefore, it is highly unlikely that an emergency stop command would have had any effect. The other actions that the driver recalled performing (attempting to invoke a brake application by using a key switch reset and tilting the remote, and removing the battery) were appropriate and should have commanded the train to apply brakes and stop.

When the RCE software intentionally commanded an emergency brake application, the RCE receiver would enter its defined emergency stop mode. In addition to creating an emergency vent of the brake pipe, it was designed to command full independent brake and to set the direction to neutral. However, responses to these commands were not observed to occur during the runaway sequence. Therefore, the emergency brake applications that did occur during the sequence were very likely not a response to the software-commanded emergency stop mode.

In summary, the driver's fast direction change from forward to reverse almost certainly (and unintentionally) resulted in a spurious fault condition associated with the dual direction fault interlock, which applied emergency brake. Through an undetermined mechanism, this likely initiated further anomalous RCE behaviour: the RCE ceased to respond to the driver's commands, and 3 emergency brake applications and releases were recorded that were not consistent with previously identified fault state(s). A short time later, while still unresponsive to driver commands and with the train's brakes still released, the train started to roll away.

Absence of runaway protection at Railton

The siding at Railton used for cement train loading was located on a downhill grade towards the main line in the direction of Devonport. The gradient posed a risk of a rolling stock runaway in the event of loss of braking effort.

An added risk unique to the Railton siding was the loading process, enabled by the use of RCE, where the driver was away from the operating train for a substantial period. This meant that multiple conventional means for immediate intervention by a driver in the case of an uncommanded movement were not available. For example, if the driver was in the locomotive cabin or the driver's van, they could apply the locomotive brakes using the cab handle unit or the in-cabin emergency brake.

Additionally, TasRail's advanced network train control system (ANCS) was deactivated on trains that were within yard limits. This included the cement train when it was within the limits of the Railton cement siding. Consequently, the ANCS system would not detect a runaway train leaving a yard and entering the main line. Therefore, no authority exceedance alarm would occur, and the runaway train would not be visible to the NCO. This limitation of the train control system increased the reliance on other systems existing that could prevent unauthorised movements from exiting yards onto the main line, and alerting the NCO if a runaway occurred.

TasRail conducted a risk assessment for the hazard of runaway rolling stock during March–April 2018. An action arising from the risk assessment was for TasRail to assess its network for the addition of catch points or derailers, the purpose of which was to divert and derail uncontrolled rolling stock movements from a siding away from the main line. At the time of the accident, the cement-loading siding at Railton had not been assessed and there were no devices in place to prevent or protect against unauthorised movement (such as derailers or catch points), the absence of which allowed the cement train to exit the yard onto the main line.

Remote control equipment response outside radio communication range

Once the RCE transmitter and the RCE receiver were linked (necessary for train operation), the RCE was designed to enter the communication failed mode if communications between the 2 components were interrupted for over 4 seconds. These interruptions could have resulted from corrupted messages, loss of radio communications or otherwise unlinking (for example, switching off the transmitter or pulling out the battery). During this mode, the receiver was supposed to stop the train by removing traction power, reducing the brake pipe pressure to 400 kPa and, after 10 seconds, changing the direction to neutral.

As previously discussed, the driver described the transmitter and receiver as being unlinked at the time the RCE became unresponsive to their commands. In addition, the driver reported they subsequently turned off the transmitter key switch and removed the battery, both of which should have interrupted communication and invoked a communication failed mode response had they still been linked. Even if the driver had not performed these actions, once the receiver was out of radio range of the transmitter (after the train began to roll away), it should have experienced a loss of communication and entered the communication failed mode, which should have applied the brakes.

Instead, a review of the data recorded on the locomotive showed that, after the second emergency brake application, the brake pipe pressure was maintained at the released level and there was no brake cylinder pressure indicating that the brakes on the wagons and locomotive were released. The recorded data also indicated that there was no brake application during this period.

Further, at the point of the derailment and rupture of the brake pipe in Devonport (over 20 km from Railton), the recorded data indicated that it was more likely than not that the RCE was supplying air from main reservoir no. 1 in an attempt to recharge the brake pipe to the desired level, which continued until the locomotive was shut down by emergency services. That is, the recorded data showed no evidence of the RCE receiver commanding a communication failed mode and applying the train's automatic brake when out of radio range of the transmitter.

The overspeed protection on the TR class locomotive was set to apply brakes if the measured speed reached 88 km/h. In this case, the train's maximum recorded speed during the runaway was 87.5 km/h. However, even if the train had reached 88 km/h, the overspeed protection would not have applied because the function was suppressed when the locomotive was configured in 'trail cut-out' mode for use with the RCE (see *Suppressed or absent safety functions*).

In summary, after the train rolled away from Railton, the RCE receiver did not apply the train's brakes as designed when outside radio communication range. The train's brakes remained in a released state until the train reached the end of the line and derailed at Devonport.

Emergency response actions and procedures

Actions by key personnel

As previously noted, after the RCE became unresponsive to driver commands, the driver attempted to reset it using the transmitter. Shortly after, the train began to roll away. Although the driver made further attempts to stop the train using the transmitter, these were unsuccessful. At this point the driver called the network control officer (NCO) to report the runaway train.

Although the NCO discussed with the driver where the train would likely stop, background conversations of other TasRail staff in attendance determined that the best course of action was to route the runaway train away from the main line to derail in Devonport Yard, and arrangements were made to configure the points at the entrance to the yard to achieve this. On conclusion of the phone call with the driver, and in accordance with the TasRail emergency response procedure, the NCO called emergency services to report the runaway train.

Over the next 16 minutes the NCO (and later the network access manager) liaised with emergency services to assist in the response. They were assisted by the rolling stock asset manager who monitored the train in real time, allowing emergency services to be advised of train location and speed.

This critical information allowed a coordinated and effective response by Tasmania Police, who deployed to close level crossings in front of the train. Although emergency services were quickly advised, by the time the Tasmania Police response was initiated the train had passed many of the level crossings between Railton and Spreyton township. Police also alerted members of the public to the danger through activation of lights and sirens on all attending police vehicles. When achieved, these actions counteracted the increased risk of level crossing collisions from the reduced warning time at the active crossings (due to higher train speed) and lack of train headlight for visibility and horn for audible warnings at all crossings.

Although the train was seriously damaged during the derailment accident, injuries were limited to 2 pedestrians who received minor injuries. All persons involved in managing the runaway train on the day, including TasRail and emergency services, acted to effectively minimise the consequences of the runaway and derailment.

Processes for responding to emergencies

Although the emergency response was successful on this occasion, this was not assured. TasRail's emergency response procedures were generic in nature, requiring an NCO to immediately protect an area and notify emergency services. However, the procedures provided little other guidance or assistance to an NCO dealing with specific types of incidents that may require a time-critical tailored response, such as a runaway or track warrant authority exceedance. For example, the effective management of the Railton runaway involved sound decisions (routing the runaway train away from the main line and coordinating with emergency services to close level crossings in front of the train) that were not included in the emergency procedures but could have been considered in advance.

It is recognised that emergencies can take many forms and, as such, decisions and procedures require some level of flexibility. However, emergency responses involve high workload,

distractions, interruptions, time pressures and stress. This can result in an environment where omissions and errors can easily occur. The Rail Industry Safety and Standards Board (RISSB) guideline document *Rail emergency management planning* stated:

> Maintaining 'quick references' is recommended to support response and recovery. In the initial onset/identification of the emergency, Procedures or Action Cards and Checklists should detail immediate and important actions to help workers at all levels perform effectively.

The absence of a formal quick-reference procedure or checklist to deal with specific types of incidents meant there was a significant risk that NCOs, when dealing with events requiring time-critical decisions and response, would make errors and omissions.

Two types of checklists would be useful in this regard. The first is 'read-do', where the checklist item is read and the action performed, which is particularly useful when performing an infrequent task (Dismukes and Berman 2010). The second is 'flow-then-check', where several actions are performed from memory, then verified as completed through a checklist. However, as useful as these are, both types of checklist require firm underlying procedures to be most effective.

Another aspect worth noting is that the runaway occurred during normal business hours when extra staff were present who contributed to share the NCO's workload in dealing with the emergency. In particular:

- the network access manager coordinated with emergency services
- the rolling stock asset manager obtained information of the train's location and speed to pass onto emergency services
- the general manager freight services arranged diversion of the train into Devonport Yard
- a Devonport shunter switched point numbers 85 and 88 to divert the runaway train from the main line into Devonport Yard.

Had the runaway occurred outside business hours, the NCO would have been required to respond on their own, and would likely not have been able to achieve the same positive results alone. For example, a shunter would probably not have been available to divert the train into Devonport Yard.

In summary, TasRail's processes for ensuring immediate network control actions in response to emergencies (such as runaway and authority exceedance) fundamentally relied on the experience and knowledge of NCOs and did not include the provision of procedures, tools and checklists detailed enough to support the effective management of specific types of incidents that require a time-critical response.

Safety-related design and integration problems

Introduction

Given that the RCE entered an unsafe state, and the communication failed mode did not function to stop the train, the ATSB tested the functionality and performance of the generation 3 RCE to assist in determining the possible mode of failure during the runaway sequence. Although the specific mechanism involved in the RCE's persistent unsafe state was not identified, the testing identified, or confirmed, several problems with the safety-related design of the generation 3 RCE and its integration with related systems.

Unintended activation of locomotive emergency brake

As noted above, during ATSB testing, activation of the RCE dual direction fault interlock was observed to activate the TR class locomotive's VX vent valves and emergency magnet valve (EMV), triggering an emergency brake response of the locomotive, separate to the RCE. When RCE was in use on a light engine, an emergency brake response could also occur at the initiation of the communication failed mode and in response to rapid applications of the automatic brake.

These activations of emergency brake were unintentional and inconsistent with non-remotely-controlled train operations.

An emergency brake application was not recognised by the RCE if the RCE itself did not initiate it. As a result, the RCE attempted to oppose it. Unlike a situation where the emergency vent occurred due to a broken pipe or deliberate driver action, in these circumstances the activation of the locomotive VX vent valves and EMV were temporary. Once they deactivated, the vent stopped and the RCE was successful at recharging the brake pipe, releasing the brakes.

This was true even in situations where the RCE was commanding a service-level brake application at the same time. The RCE would only recharge the brake pipe to the desired level but the train brakes would respond to the pressure rise as an automatic brake release command. Therefore, the level of RCE-commanded brake application would not occur or could release.

The configuration of the RCE air box, which was connected to the brake pipe in close proximity to one of the VX vent valve's connection at the rear of the locomotive, was found to contribute to the sensitivity of inadvertent application of this VX vent valve. ADE's understanding that the operation of the VX vent valves were triggered by an electrical command (as opposed to a pneumatic pressure drop) was not correct.

As already discussed, an inadvertent activation of the dual direction fault interlock occurred when the direction controller was changed quickly from forward to reverse at the beginning of the runaway sequence, which resulted in an unintended activation of the locomotive's emergency brake response.

Reduced recovery timeouts

The timeout periods implemented in the RCE before permitting resets of the emergency brake and penalty conditions were inconsistent with those of the electronic airbrake on the TR class locomotive. The electronic airbrake manufacturer imposed the timeouts to ensure a safe state was reached (that is, the train was stopped) prior to reset. Otherwise, the combination of rapid application and release of brakes at the locomotive would result in uneven brake application due to the inherent delay in braking application and release towards the rear of the train, which could lead to excessive in-train forces and train separation.

The RCE allowed both the emergency stop switch and vigilance penalty resets to be effected after 30 seconds, unlike the 60-second period imposed during non-remotely-controlled train operations. Resets of other RCE states, such as the communication failed mode and control fault mode, did not have a direct equivalence to the electronic airbrake as they were unique to the RCE. Both these modes could be reset without any required timeout while a train was in motion (that is, a running reset).

The appropriateness and effectiveness of shortened or absent time delays was not assessed by ADE when they were implemented. Therefore, the risk of resets being effected before a train had stopped was not quantified and the possibility of it leading to a train separation was not controlled.

Potential persistent unsafe state during initialisation

Analysis of the generation 3 RCE software found that, during initialisation, it had the potential to enter an endless loop (that is, the receiver could 'hang') without entering a fault state. Among the conditions that would result in this behaviour were the train brake pipe pressure remaining above 470 kPa, which included fully-released brakes.

In this condition, the receiver would not respond to driver inputs, would not change the status of the locomotive's previous commands (such as braking and traction), would be unable to continue normal operations, and would not enter the communication failed mode during a loss of communication.

The RCE's watchdog timer ran through a separate timer loop, so it would not trigger for this type of problem. Dunn (2002) stated:

> …gross faults in software structure will usually result in a program halt or crash. In a second category of faults, the program will continue to run but generate incorrect data which can propagate to operator or effectors [control outputs], thereby setting up conditions for a mishap.

However, there was insufficient evidence available to fully evaluate whether this condition actually occurred during the runaway sequence, and the behaviour was not reproduced during testing, either by rebooting the RCE or through imitating the train configuration and control inputs made at the time (as the tests were not specifically designed to evaluate this aspect of RCE function). Furthermore, initialisation only occurs during an RCE reboot, and there was insufficient evidence to establish whether a reboot did occur during the runaway sequence or, if it did reboot, what caused it.

Opposition to emergency brake applications from an external source

ADE advised TasRail that the emergency stop function was the RCE's 'primary safety mechanism.' It was designed to exhaust pressure from the brake pipe on driver command and during some system fault conditions.

In a conventional (non-remotely-controlled) train, the brake systems on all vehicles were designed to respond to any rapid and complete exhaust of air from the brake pipe by applying the brakes, and the locomotive would also automatically remove traction power; both actions were to stop the train and prevent it from subsequent movement. This behaviour was consistent with Australian Standard AS 7510.6:2014 (*Braking systems part 6 – train*), which required that, in the event of a train separation, an emergency application of the stopping brake occurred on every vehicle of the train (though compliance with the standard was not required).

When the RCE's emergency stop function was activated, it replicated an emergency brake application on a non-remotely-controlled train. However, the RCE did not recognise emergency brake commands from an external source. The RCE would oppose instances of brake pipe rupture (as occur with a derailment or train separation), and driver operation of the in-cabin emergency brake, by attempting to raise brake pipe pressure.

The RCE's opposition to the loss of brake pipe pressure would mean that the brake application on some vehicles was less than a full application and the locomotive's system to remove traction power would not activate if:

- a brake pipe rupture occurred a sufficient distance from the locomotive, or
- the emergency brake was activated from the driver's van.

This meant that, in the event a driver did not command an emergency stop using the RCE transmitter prior to a collision or in response to an imminent collision or mid-train derailment, the locomotive could retain tractive effort, driving into the collision or derailment. Similarly, In the propelling configuration (locomotive at the rear), the locomotive could continue powering into heavily-braked wagons, increasing the risk of wheel lift and flange climb derailments.

Effect of communication loss on vigilance and driver-commanded emergency brake functions

Both the RCE's vigilance and emergency stop functions required an active radio link to operate. That is, in the event the RCE transmitter and receiver unlinked (for example, after turning off the transmitter to reset a fault mode), these functions were not available until communications were re-established.

The locomotive's vigilance system was suppressed during RCE operation and replaced by the RCE vigilance function. This required a link to the RCE receiver to effect a penalty brake. Because of this requirement, the RCE vigilance function would not activate if the driver became incapacitated while the transmitter and receiver were unlinked.

A driver could apply emergency braking from the locomotive or driver's van, or with the RCE transmitter. However, most of the cement train operation cycle required the driver to be outside the train (during loading, unloading or shunting). During these periods, the only available means to apply emergency brakes was via the RCE transmitter's emergency stop switch, and this was not available if the transmitter and receiver became unlinked.

Although the RCE receiver was supposed to stop the train by entering the communication failed mode when unlinking occurred, the resulting brake application was less than that of an emergency stop or vigilance penalty.

Summary

Overall, the generation 3 RCE had several safety-related design and integration problems, which included:

- unintended activation-and-release of emergency braking on the locomotive
- recovery from an emergency brake application and certain penalty states that was inconsistent with locomotive braking system timeout controls
- the potential to enter an unsafe state during initialisation, which was unrecoverable without external intervention
- the absence of a means to detect and respond to an emergency brake application from a source external to the RCE
- the vigilance and driver-commanded emergency stop functions were unavailable in the absence of an active radio communications link.

All of these problems were readily identifiable after the runaway accident, and should have been readily identifiable before the runaway through more thorough integration and testing. Of these problems, the unintended activation-and-release of emergency braking on the locomotive was likely involved in the occurrence sequence, based on the braking system's response to the reported driver inputs early in the runaway sequence of events.

In addition, the absence of a means to detect and respond to an external emergency brake application meant that the RCE most likely opposed the initial, unintended, emergency braking application, thereby releasing the brakes. Finally, the potential to enter an unsafe state during initialisation might also have been realised, although there was insufficient recorded data to determine whether this was the case. The other problems, left uncorrected, had the potential to lead to other types of occurrences.

System safety assurance limitations

Introduction

Elements of the RCE design showed that the developer and manufacturer, ADE, made safety an important consideration throughout development and operation of each generation of RCE, and the equipment had many safety functions and design attributes. However, the safety objectives, requirements, and claims were not clear or recorded, so there was no solid foundation for the design of safety elements. As discussed in the previous section, there were also several integration and design issues, which indicated limited design assurance. This section discusses these system safety assurance concepts further.

Use of incomplete locomotive system information

The developer of RCE for a train needs detailed information about the train such as its interfaces, functions, performance and operational hazards. However, limited approaches were made by ADE to TasRail for technical information, as ADE had concerns regarding infringing intellectual property rights of the manufacturers of the electronic airbrake and locomotive. ADE did not approach the manufacturers themselves for this information. Instead, ADE sought technical

information from unofficial sources, including from the internet. Furthermore, TasRail were minimally involved in technical aspects of the system's development.

The information ADE did use was, at least in part, erroneous and incomplete. Without access to vital engineering information about the systems with which the RCE interfaced, integration problems were more likely.

For example, as already noted, ADE's understanding that the operation of the VX vent valves were triggered by an electrical command (as opposed to a pneumatic pressure drop) was not correct. As another example, ADE incorrectly diagnosed the cause of wheel lock as being due to inadvertent emergency brake application, when in fact the cause later identified by the ATSB was found to be excessive control pipe pressure. ADE's decision to change the communication failed mode brake pipe pressure reduction to 400 kPa and not 350 kPa did not address the issue, and instead likely increased stopping distance.

Reliance on communication failed mode

For operational reasons, changes were made to the communication failed mode with the introduction of the generation 3 RCE function that decreased the brake application level, and there was no record of an evaluation of the potential effect on safety. Although TasRail tested the effect on stopping distances in April 2018, this testing was not representative of typical operational scenarios (that is, tests were done with an empty train travelling below 15 km/h). .

More importantly, the RCE radio link and the associated communication failed mode were relied upon almost completely for safe operation. All the commands originating from the transmitter passed through the radio link, which included all driver commands, the tilt function and the vigilance function. Without a radio link, a driver could no longer control the train or command an RCE emergency brake application. This made the RCE's radio link, and its behaviour when the radio link was lost, at least equally important to safety as the emergency stop function.

ADE relied on software intervention when there was a communication failure. The system needed to detect the loss of radio link and then act on it by sending commands from the RCE receiver to the air box and locomotive, which would then vent the brake pipe to provide a brake application and remove or prevent locomotive power.

However, unlike the hardware-induced emergency stop function on the locomotive, which had a 'default' or relaxed state of having brakes applied, the RCE's communication failed mode response relied on fully-functioning software to work. There was always an inherent potential for software flaws to interrupt this process. This resulted in an increased potential for the communication failed mode response to itself fail, as it did during the runaway sequence. It similarly reduced the availability and reliability of the RCE's driver-induced emergency stop function.

Limitations of pre-delivery testing

The United States National Research Council (2007) stated that 'it cannot be stressed too much that for testing to be a credible component of a dependability case, the relationship between testing and the properties claimed will need to be explicitly justified.' This means that tests are only credible if there is a clear relationship between the testing and requirements (part of what is termed 'traceability'), and there needs to be a record of the manner in which the tests show compliance with the requirements.

Although ADE undoubtedly performed informal ad hoc testing throughout the development and commissioning of the generation 3 RCE (and previous generations), these activities were almost entirely undocumented. There were no detailed step-by-step test procedures, and no pass/fail criteria, so the tests were not repeatable. Where tests were documented, there was no recorded relationship between desired (or required) behaviour and testing methodologies, so there was no way to make an evidence-based argument that the tests provided meaningful information about the safety of the system.

Pre-delivery testing by ADE was limited to bench tests, and ADE specifically noted that several of its bench tests could not be replicated during the on-train testing phase. The tests that were not conducted while fully integrated on the train included the control fault mode (the application of brakes during a control fault being critical for safe operations), and the dual direction fault interlock (which was observed immediately preceding the runaway). The ATSB found that it was possible to test both with the RCE integrated on the train.

The first on-train tests of generation 3 RCE were conducted during commissioning testing on 18 January 2018, but no records existed of these tests or the reason they did not pass. By the time of the second commissioning test conducted in February 2018, a test plan (consisting of a checklist only) had been developed by TasRail. As with the pre-delivery testing, exact objectives were unstated and documentation was minimal. There were no test procedures or descriptions of how the tests were to be performed.

The effectiveness of the onsite testing that was conducted in February 2018 was probably diminished further by a limited understanding of the safety characteristics of the overall system: ADE had limited visibility of the broader system before this, while TasRail did not have any subject matter experts present. As a result, many safety-related aspects of the RCE's integration were very likely not tested, including the equipment's response to an emergency brake application from the driver's van or via brake pipe rupture (both later found to be ineffective).

Limitations in the development process

Although software provides opportunities to enhance the functionality of a system, it can also be a vulnerability. It has been claimed that, in practice, it is impossible to have complete knowledge about a system that incorporates software (Hawkins 2009) or, by extension, any other complex system. This means the safety of such a system cannot be proven with certainty. However, processes and guidance have been developed to enable the safety of a system to be substantiated to a nominal degree of confidence.

Neumann (1994) contended that the development of a complex system with 'correctness' requirements (such as safety) requires an extremely principled approach to system development, well beyond what is traditionally experienced in general practice. In other words, the need for a high level of safety assurance demands not only the inclusion of relevant safety features but a structured, principled approach to the development process itself. Doing so helps reduce errors in the design process, adding to safety dependability.

Similarly, Hawkins (2013) stated that the need for traceability is widespread or universal across software safety standards, as are stepwise validation of the software requirements and methods of showing that requirements are satisfied.

These concepts are fundamental to system safety processes such as those outlined in Australian Standard AS 61508 and European Standard EN 50126 (see Appendix B). In general, they provide methods to develop safety objectives, requirements and claims, in order to make an evidence-based argument that the system meets (or does not meet) the objectives.

The generation 3 RCE was not developed using such comprehensive, top-down design principles, so its dependability, and therefore the safety of the broader system, was unproven.

ADE attempted to apply a limited subset of reliability analysis techniques based on AS 61508 to its generation 1 RCE in 1999, but this application was inherently flawed. The highly-structured and fully-documented development process required by the standard was absent, and the neacessary groundwork for this analysis, such as a requirements specification, or defined hazards and consequences, had not been established. Therefore, the analysis undertaken had limited value in terms of determining safety.

To a significant extent, ADE did not address critical considerations such as the RCE's reliance on radio communications, start-up state, software reliability, or the reliability and effectiveness of other safety functions. The assessment explicitly excluded detailed design elements such as 'part

numbers, circuitry structure, [and] detailed software code' – all necessary for a final assessment to be comprehensive and effective. The assessment also did not recognise that software could have flaws that would not result in the watchdog activating, and it did not include any software assessment even though such processes comprised a significant part of AS 61508.

Most critically, the generation 3 RCE was significantly different to the generation 1 RCE system that was assessed in 1999, rendering the assessment obsolete (even if it were originally applicable), and it was not redone.

Most systems safety methodologies explicitly or implicitly require the production of a significant amount of process and design documentation, which is naturally developed as part of the process; that is, information about the system cannot be fully understood until it is documented. The documentation also serves as evidence for independent verification of the development process and can be revisited when changes later take place.

The design documentation produced by ADE for the generation 3 RCE was not suitable for these purposes—most relevant information was held in informal records and the system's development and maintenance relied heavily on the developer's individual system knowledge. Similarly, the development process itself was mostly undocumented and unstructured, and involved just 2 people. According to Hobbs (2020), a lack of 'intellectual diversity' among a development team can be problematic.

In the absence of structured system safety assurance activities, ADE's claim that the RCE would always fail to a safe state could not be substantiated to any reliable degree. ADE did not produce sufficient process and product documentation to allow TasRail to independently verify the safety of the RCE in the context of the broader operational system.

Summary

Although ADE had safety as a design objective and safety elements were included in the RCE, the equipment was not developed using system safety assurance activities appropriate to its application. These limitations in the development process contributed to a range of design and integration problems, as already discussed.

Acquisition and use of remote control equipment

Introduction

TasRail began to consider a replacement for the generation 2 RCE in early 2015 with a formal business case developed in December 2015. It subsequently ordered the new generation 3 RCE from ADE in May 2017.

It is notable that, by the time generation 3 RCE was introduced, TasRail had operated the cement train service successfully using previous generations of the RCE for about 19 years without any accidents attributable to the RCE, and largely without serious incident. In addition, ADE had provided TasRail with assurances of the equipment's safety integrity. This likely contributed to a high level of confidence in the use of RCE and the overall operation.

Even so, the development and integration of new equipment is not solely the responsibility of the equipment manufacturer. Although ADE undertook the technical challenge of RCE development, TasRail, as the rail transport operator (RTO), ultimately held a duty to ensure that the cement train service (and the RCE as part of the broader system) was safe. However, TasRail had limited further involvement in the development of the system, and there was ultimately no formal definition of safety requirements or verification that the system met a specified level of safety, as outlined below.

Operator involvement in the development process

The generation 3 RCE was a new build specifically for TasRail. Although ADE initially proposed to use an existing product from a third party, this option could not provide some of the functions

TasRail had requested, such as dynamic brake, the Railton loading interlock, and conversion to a digital radio on a new frequency. Subsequently ADE proposed manufacturing a new product, which became the generation 3 RCE. TasRail had also been told by ADE in 2015 that the transmitter and receiver microprocessors would change; however, it was unclear whether the extent of the consequences of this change—specifically that it required a complete software rewrite—were fully discussed.

Although TasRail was aware of the above changes to some extent, there were numerous other important changes of which TasRail was unaware. TasRail did not directly ask ADE for information about changes that were being made to the RCE and did not conduct risk assessment activities for the changes that were known.

For example, the level of brake application in the communications failed mode had been reduced by October 2017, but ADE did not inform TasRail until April 2018. Tests of stopping distance were not conducted until June 2018, 4 months after the RCE was commissioned and in use.

Overall, TasRail seemed to not fully appreciate the extent of the change, with a widespread view that the transition to the generation 3 RCE would be ‘like-for-like’. This view was asserted multiple times in documentation:

- the original business case in December 2015
- the initial impact assessment (IIA) in November 2016
- the revised business case in January 2017
- discussion with the Office of the National Rail Safety Regulator (ONRSR) in December 2017 in relation to the need for a notification of change.

Conversely, there was evidence showing that the change was not actually like-for-like, including:

- requests for multiple changes made by TasRail (including the addition of dynamic brake functionality)
- discussions between TasRail and ADE about the need for other changes (including change to radio type and frequency)
- identification that driver retraining was needed and provided (this was brief, which may have reinforced TasRail’s perception that the changes were minor; however, major changes can occur while maintaining comparable driver interfaces), along with a new and revised operation manual.

Once the generation 3 RCE was in service, a TasRail staff member raised concern that the communication failed mode brake application had changed. Although this prompted a response within TasRail, it was not a direct challenge to the concept of like-for-like replacement and did not prompt consideration of whether other changes had occurred that had the potential to affect safety.

Even with information available that changes to the RCE were occurring, there was no evidence that the assertion of like-for-like was challenged within the change management process. Consequently, the concept of a like-for-like replacement promulgated through the organisation to become the accepted view, at least until after the generation 3 RCE was commissioned and in service in February 2018.

It is likely that this view, along with a 19-year history of using previous generations of RCE with very few serious problems, influenced TasRail’s approach to the development and post-operational assessment of the generation 3 RCE. Rather than approaching it as a new design, requiring more direct involvement and oversight, TasRail’s approach was more consistent with that of a slight modification to an existing design.

In addition to the accepted view of the change as like-for-like, there were also other limitations with TasRail’s corporate knowledge about the RCE. Within TasRail, a single person had maintained responsibility for management and operation of the RCE from 1999 through to about 2009. While

the RCE was still used from then on, there was no nominated person or team responsible for it until 2017. From 2009 on, there was one person nominated for responsibility of the RCE project at a time, with a maximum of about 1 year in this position.

TasRail advised that a shift from individual responsibility to departmental responsibility was consistent with modern practice. However, it is likely that a significant amount of RCE subject matter expertise had been developed over time and then effectively lost in 2009, and again with the change in project managers shortly before commissioning the generation 3 RCE. The limitations in corporate knowledge were likely worsened by the absence of documented RCE specifications, functions, and expectations, and minimal documented information about the project itself. This limited TasRail's ability to effectively oversee the generation 3's development and integration from a technical perspective, particularly the safety-critical aspects of its function.

TasRail also applied limited subject matter expertise to the development and oversight of the RCE commissioning tests. The commissioning test plan was reviewed by the TasRail rolling stock assets manager, driver supervisor, and ADE, but there was no detailed independent review of the procedures for completeness and validity by locomotive and train systems subject matter experts. Although TasRail representatives were present during the testing itself, TasRail's involvement appears to have been largely limited to passive observation. The testing was supervised by a graduate engineer who had started with TasRail the previous month and had little opportunity to become familiar with the locomotive and RCE systems.

Finally, the absence of a structured acquisition process also appeared to contribute to ad-hoc practices in notifying and addressing RCE faults, as well as post-implementation testing.

In summary, TasRail did not fully engage with the development process of the generation 3 RCE from initial design through to commissioning. Associated with this limited involvement it did not understand the extent of design changes that ADE were implementing (and the implications of changes that TasRail were requesting). This reduced TasRail's capability to prevent, identify and resolve design and integration problems.

Absence of safety requirements

The safety of a 'system' (which may be viewed as a broad undertaking, such as the cement train service using RCE, or a subsystem such as the RCE itself) is dependent on a high-level, organisational understanding of safety. When that understanding is limited, the level of attainable safety is similarly constrained.

In general, TasRail had a high-level approach to safety through the application of an organisational safety management system with embedded change management and risk management principles. TasRail also had a long-established conceptual view about how the cement train and RCE would operate.

However, the safety objectives for the cement train service were not explicitly stated. This is particularly important in this case because the operation—and therefore risks—were considerably different to other types of rail operation. This, in effect, made safety an invisible target.

The absence of documented system requirements, including safety requirements, and limited evaluation of safety-related design characteristics, meant that any results of testing would not have been sufficient to make an evidence-based argument about the safety of the system because there was no documented expectation of performance.

In particular, TasRail did not specify a maximum acceptable likelihood that RCE performance could contribute to certain hazardous events, such as a runaway, derailment, or collision with a road vehicle. Had this been done, ADE would have been obligated to prove that this requirement was met to a certain degree of confidence. The process of making this proof probably would have improved overall understanding of the cement train system and RCE subsystem and resulted in a safer design. The tangible evidence it provided would have enabled TasRail's decision-making process about the broader system to be better informed.

Without TasRail definitions, the safety elements of the RCE design stemmed from ADE's concept and perspective of what 'safe' meant. This was primarily the availability of the emergency stop function, backed by other safety functions and the intent of a fail-safe design. This approach may not provide an optimal level of safety when compared with a carefully considered and explicit definition. Without this information, and with minimal TasRail involvement, ADE had to make assumptions about how the RCE had to be designed, built, and operated for it to be safe, and these assumptions were not formalised or challenged.

The loss of RCE communications, for instance, was recognised as a safety concern: when the RCE detected a loss of radio link for 4 seconds, it would remove traction power and make a service brake application that should bring the train to a stop. However, the RCE response was not based on a formally-defined and evidence-based safety requirement, and was therefore not necessarily optimal. There was no consideration how much braking effort provided minimal risk across the entirety of operations, or whether those parameters should change depending on the train's load, consist, speed, location or direction. Braking performance tests were not representative of actual operations (there were no tests on a loaded train or at speeds above 25 km/h). There were also no requirements for functions to work under specific conditions, such as the communication failed mode being operable during initialisation, potentially leading to undesired RCE responses under unforeseen combinations of conditions (as happened during the runaway).

Finally, there was no assessment of how critical each RCE and locomotive function was to safety, how dependable these functions were, and whether secondary safety measures existed or were required in the event that an unsafe failure occurred. For example, had there been a requirement for the RCE to detect external emergency brake applications, ADE would have had to implement that function.

Verification of system safety

TasRail's safety assessment of the RCE and its integration with the overall system was limited. Risk assessments done in 2011 and 2014 largely did not effectively assess the potential for the RCE to fail to an unsafe state. Although the 2011 assessment acknowledged the potential for the RCE to 'operate abnormally', it did not contain sufficient detail to evaluate what this meant or verify the effectiveness of controls, and it did not consider causes other than incorrect maintenance or transit damage (such as problems with design and integration). The potential for transmitter brake or throttle control failure, a limited subset of potential causes of an unsafe state, listed a risk control that was later removed (the independent remote stop mechanism), and a safety analysis that was no longer valid after substantial design changes.

After the generation 3 RCE was in service, a risk assessment in relation to a collision resulting from failure of the RCE identified several risk controls, and concluded that the risk was adequately controlled. However, it did not appear to consider their efficacy or reliability, and the stated risk controls were actually not reliable. More specifically, in terms of the cited risk controls:

- Driver competency could not always address an RCE failure; for example, when the driver was not on board the train.
- Several RCE and train functions were cited without consideration of their effectiveness. Some would not work with a lost radio link or were being routinely reset without diagnosis of underlying cause.
- The driver's van emergency brake was largely ineffective when tested by the ATSB, and had the potential to increase the risk of derailment in some situations.
- The generation 3 RCE itself was seen as reducing risk without consideration of the potential for hazards generated or changed by the new equipment.

Several further changes were made to the generation 3 RCE after commissioning was complete. There were no formal risk assessments for any of these changes. Most were implemented without subsequent re-testing by TasRail or ADE and, when re-testing did occur, there was no record kept

of the tests conducted or outcome. In fact, the many changes introduced with generation 3 diminished the value of confidence built from in-service experience of the previous RCE generations.

More broadly, TasRail did not perform or require detailed system analysis in order to verify its safety. To ensure that a system is dependable, engineers need to understand how faults or software errors can appear, and how they can manifest in all operating conditions and modes. Different techniques can be used to estimate or predict the likelihoods of different kinds of failures, and evaluate the potential effects in a technical and operational sense (Dunn 2002). Similarly, potential undesirable outcomes can be traced back to a range of potential causes to identify areas of concern.

When the results are combined to form a comprehensive view of the overall safety of a system, it can culminate in a 'safety case,' described by the United Kingdom Ministry of Defence (2007) as:[88]

> A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment.

For the argument to be compelling and valid, all feasible safety concerns should be addressed by the safety case. Neither TasRail or ADE produced a safety case (or equivalent argument) for the use of the RCE, and important elements of the application and environment were not considered in its design. The use of systems safety assurance activities would have been much more likely to identify that, in some circumstances, RCE failure modes could result in an unsafe state, or provide external risk controls if the risk could not be effectively managed another way.

Most importantly, there was no record of the degree to which safety-critical functions were checked for effectiveness at any point throughout the generation 3 RCE system's development and commissioning. Given the nature and duration of the tests, they were very likely basic functional tests, which are mostly uninformative about the dependability of the system as a whole, particularly when software is involved (National Research Council 2007). For example, there were no documented assurance activities to prove that the ADE-assessed critical safety function (that is, the emergency stop) was adequately reliable.

Summary

In summary, TasRail commissioned the manufacture of, and continued to use, safety-critical locomotive RCE without systematic assurance of its safety. This was because TasRail did not:

- fully engage with the development process from initial design through to commissioning, or understand the extent of design changes associated with the introduction of the generation 3 RCE (which reduced its capability to prevent, identify and resolve design and integration problems)
- explicitly identify and impose safety requirements
- verify that the overall system met a specified level of safety.

In other words, TasRail relied on ADE to provide a product that was fit for purpose without seeking independent clarification of the claims made by ADE regarding the engineering standards met by the RCE or the safety validation process used. As a result, the RCE was provided and used for the TasRail cement train operation without a compelling argument for its safety.

---

[88] Often, the term 'safety case' is used in a broad sense to encompass all elements of an operation including safety management system(s). In this report, however, the term is used in a more restricted sense, referring to the use of the remotely-controlled cement train application and environment.

Safety implications of remotely-controlled trains

Introduction

As well as with the design of the RCE itself, there were also additional safety aspects to be considered when using remotely-controlled trains. TasRail had utilised RCE to operate its cement train service in a broadly consistent way since about 1999. RCE was the primary means of operation at all times, being used to control the train even when the driver was stationed in the locomotive cabin.

This section discusses how the use of RCE introduced key differences when compared to conventional train operation (which required a driver directly operating the controls of a locomotive positioned at the front of the train at all times). The change in control system added significant complexity to the control of the train, and presented additional challenges that needed to be managed.

Potential for remote control equipment to fail to an unsafe state

A driver operated remotely (off the train) for the majority of the cement train's service cycle, during which the in-cabin emergency brake controls, as a means to place the train in a safe state, were not available. Therefore, for the majority of the time, it was critical that the RCE remained responsive to driver commands or would always fail to a safe state.

TasRail's cement train system depended heavily on the RCE being fail-safe, and it was designed to have that result; that is, so that any hardware or software failures would always result in a safe state. However, uncertainty is an unavoidable consequence of having computers (or any complex design) as parts of hazardous but reasonably safe environments (Littlewood and Strigini 1995). There is always the potential for a complex system to fail in unpredictable ways; no system can ever be guaranteed to work acceptably all the time and it is impossible to predict all the sources of failure (Neumann 1994). Therefore, the potential for the RCE to enter unsafe failure modes was always present, simply as a result of its computer-based architecture.

It is important to account for the potential for a system to operate in (or fail to) an unsafe state in the design of how equipment integrates into the overall system and add or adjust external elements if the safety risk remained too high; that is, adjust the architecture of the broader system to accommodate the potential for critical subsystems to fail (Dunn 2002). At the time of the runaway accident, there was no backup or redundant system to assert control in the event of an unforeseen RCE failure mode, and the RCE itself did not have a proven level of system safety integrity.

An alternative approach was taken in the 2005–06 series of reports by the United States Federal Railroad Administration (FRA), which recommended limits on locomotive power, train length, speed and grades for remotely-controlled trains, effectively constraining their use to yards and short distances.

TasRail had implemented a secondary safety system in response to the generation 1 RCE entering an unsafe state in February 2010. This was an independent remote stop mechanism to remove traction power and apply emergency brakes, which could be used in case of RCE failure. Even though the independent remote stop mechanism did not have an assured level of reliability, it provided a risk control that was functionally independent of the RCE, lessening the reliance on RCE being fail-safe.

The generation 2 RCE had a safety feature—the dual direction fault interlock—designed to address the specific failure mode encountered in February 2010. When the generation 2 RCE was introduced into service, the independent remote stop mechanism was removed, even though the dual direction fault interlock only addressed a subset of potential causes of the system entering an unsafe state. This indicates that neither ADE nor TasRail recognised at the time that there could be other reasons for the system to enter an unsafe state.

Analysis of recorded data indicated that the generation 3 RCE entered a potentially unsafe state at Caroline Creek in May 2018. During this event, the RCE ceased responding to driver commands and the train's brake pressures were changing in an uncontrolled manner that could have led to the brakes being released. This showed that the fail-safe design intent was not dependable. In safety terms, this event was likely a precursor to the Railton runaway accident.

In summary, the generation 3 RCE did not have high levels of proven system dependability, either through extensive in-service experience or the application of structured system safety assurance principles, so there was a realistic potential for it to fail to an unsafe state. However, there was no design redundancy or secondary means to assert control in the event of an RCE failure condition that resulted in it being unresponsive or making spurious commands.

Suppressed or absent safety functions

Vigilance control and overspeed protection functions were safety features present on the TR class locomotive. However, they were suppressed when it was configured as a trailing locomotive (in 'trail cut-out' mode), as was required when the RCE was in use.

As previously discussed, although a similar vigilance function was active on the RCE transmitter when the train was under RCE control, it relied on a communication link between the transmitter and receiver to function effectively. The penalty brake application induced by a vigilance penalty, and the time delay before a reset was permitted after a penalty occurred, were also different (less) than for the locomotive system.

With regard to overspeed protection, a similar function, a GPS speed restriction, was offered by ADE. However, it was not requested by TasRail or implemented in the delivered version of the generation 3 RCE.

Certain indications and controls that were normally available to the driver in non-remotely-controlled operations were also not available when the RCE was in use. Some were not available when the driver was operating from the driver's van or outside the train locomotive cab, and others were not available at all. These included:

- The brake pipe flow indicator was not available at all, as the locomotive's electronic airbrake was set to trail cut-out mode for RCE operation.
- Locomotive brake cylinder pressure was not displayed when operating from the driver's van or outside the train locomotive cab. Instead control pipe pressure was displayed as a proxy on the RCE transmitter and a light would also illuminate. However, this did not provide an accurate indication of the locomotive's actual brake cylinder pressure (such as during automatic brake applications where the brake cylinders may be charged without the presence of control pipe pressure).
- The emergency engine stop button was not available when operating from the driver's van or outside the train locomotive cab. There was no alternative method available for the driver to stop the locomotive engine when operating from these locations.

Non-recording of key data parameters

The use of recorded data is often a critical aspect of incident and accident investigation, and the data available from the locomotive's event recorder enabled the ATSB to reconstruct much of the runaway and derailment sequence.

However, no RCE data was recorded, which limited analysis to that which could be inferred from locomotive responses only. This contributed to the ATSB being unable to determine or replicate important aspects of the runaway sequence, such as RCE modes and commands and identify the fault state that the RCE had encountered.

As discussed previously, the use of RCE represented a change in the train's control system when compared to a non-remotely-controlled (conventional) train. The driver operated the RCE transmitter rather than the locomotive controls, and the RCE had its own system for effecting

brake commands. This added additional complexity to the control of the train as commands were being relayed between systems (between the transmitter, receiver, air box and locomotive).

The increased complexity meant that additional monitoring was needed in order to interpret system command and response behaviours. However, TasRail did not add to or modify the data recording capability for the remotely-controlled cement train. The recording configuration was the same as that used on TasRail's non-remotely-controlled trains when hauled by a TR class locomotive.

Although recording of key parameters would have assisted further investigation of the runaway accident, it also had the potential to assist TasRail and ADE in identifying issues with the RCE behaviour encountered prior to the accident, during both testing and precursor events, such as that which occurred at Caroline Creek in May 2018. TasRail later reported that recording of parameters relating to RCE would have assisted in both fault finding and rectification during the implementation of generation 3 RCE. It is likely that access to sufficient recorded parameters would have helped TasRail and ADE to have identified that the RCE had failed to an unsafe condition, and either addressed the underlying reasons for it or implemented alternative means to ensure safety if the RCE entered this state in the future.

It was apparent that TasRail was aware of the limitations of not recording key parameters on the generation 3 RCE, and had initiated enquiries to obtain a data-recording capability after commissioning the RCE. However, it had not addressed the issue by the time of the accident. Further discussion about the importance of and requirements for recording RCE functions is provided in *Recording of remote control equipment functions*.

Risks associated with propelling operations

Derailments can occur from wheel lift and flange climb, due to insufficient vertical wheel load or increased lateral force to the rail head. To prevent these outcomes, slack within a train is gradually 'stretched out' (draft force) from a locomotive hauling rolling stock behind it. Conversely, buff (compressive) forces associated with propelling operations increase both of these forces and the risk of derailment.

Although propelling at main-line speeds is an uncommon practice, another motive power configuration with the potential for similarly-increased buff forces, called distributed power,[89] is widely used (in Australia and internationally). The RISSB *Code of practice: Distributed power freight trains* (July 2018) recognised that distributed power operations have the potential to 'generate train forces exceeding safe limits' (both compressive and tensile) and recommended that operators intending to use distributed power conduct analysis to manage these forces.

When TasRail operated its cement trains in a propelling configuration, the driver had access to an emergency brake handle that could vent the brake pipe from the driver's van, initiating a brake application. Use of this handle was an appropriate action to take in some emergency situations, such as when risk of a level crossing collision existed or during an RCE fail-to-unsafe event. However, tests conducted by the ATSB showed that, if the driver's van emergency handle was used while the locomotive was under power, there was potential for the locomotive to continue pushing against the brake application, further increasing the buff (compressive) forces in the couplings between wagons. This risk was also present if a derailment or collision occurred and an RCE emergency brake command was not immediately enacted.

TasRail advised that the cement train had never derailed in almost 20 years of remotely-controlled train operations, and of course the 21 September 2018 runaway and derailment was not due to the propelling configuration. However, the risk of derailment was increased due to the use of propelling compared to that which existed for non-remotely-controlled train operations. TasRail did not formally assess this risk or appear to have considered its implications. Further, there was no

[89] Distributed power: the practice of placing locomotives at several locations within a train as distinct from placing all locomotives at the front of the train.

formal instruction given to drivers regarding the unique train handling risks associated with the cement train's propelling configuration.

Summary

The use of RCE when operating trains provides advantages but also provides a range of potential challenges that need to be identified and managed to ensure the safety of operations. TasRail had conducted 2 risk assessments related to remotely-controlled train operation in 2014. However, these relied on the RCE as a reliable 'fail safe' risk control and did not consider risks that the use of RCE introduced.

By the time of the runaway accident in September 2018, TasRail had not formally assessed the risk of many of the safety implications presented by the use of RCE with the cement train service. It had used several generations of RCE for about 19 years to perform this task, so it is likely that over this time the unique application of this technology became normalised without underlying hazards being thoroughly explored. It was only when generation 3 was introduced that some of these inherent limitations became more pronounced.

In summary, although TasRail had used RCE for about 19 years, it did not identify or fully assess the safety implications of remotely-controlled train operations, or those of TasRail's specific implementation. These included the:

- potential for remote control equipment to fail to an unsafe state
- suppression or absence of some safety functions of the TR class locomotive
- nonrecording of key data parameters to facilitate effective fault and incident analysis
- increased risk of derailment as a result of motive power located only at the rear of the train.

Change management limitations

Introduction

The need for a new generation RCE was identified in early 2015 and it became clearer by the end of 2015, when TasRail were informed that the generation 2 RCE's radiofrequency spectrum allocation was required to be vacated by April 2017. At this time, ADE advised TasRail that the current-generation RCE was not compatible with the new radiofrequency spectrum allocation.

TasRail recognised that the development of generation 3 RCE was a change and initiated its change management process, including developing multiple business cases and an initial impact assessment (IIA) in November 2016. A revised business case was submitted in January 2017 and the equipment was ordered from ADE in late May 2017. There were subsequently unforeseen delays during development, requiring repeated extension requests, and it is reasonable to expect that the project team experienced significant time pressures to finalise the RCE acquisition once the process did commence.

In addition, there were a number of problems associated with TasRail's application of its defined change management processes, and also the design of the change management process itself. These are discussed in the following sections.

Management of change to generation 3 remote control equipment

The IIA was the main driver of the change management process, assessing the project level at commencement and determining the process to be followed. It also assessed the impact and size of the change, including potential impact to safety.

The IIA assessed the project as a 'significant change'. Although the project was first assessed as a P1 change, the IIA was revised in January 2018 to reclassify it as a P2 change. The reason for this was not documented, and contradicted TasRail's general treatment of the change as like-for-like, but it was probably appropriate given the potential negative impact to safety.

TasRail's processes dictated that such projects carry out 33 documented activities. On the IIA, the record of project management assurance requirements and approvals (indicating that a project is formally approved from the outset) was blank. Overall, of the 33 documents that should have been produced during the project, only a third of the required documents were produced and almost half of these were incomplete. There were no records of executive approvals for the 6 gates that nominally required them, yet the project was able to continue.

In addition, although TasRail's corporate governance and risk management process required a reassessment of both risk and its controls when a 'significant change' was identified, this was not done. Other safety-related steps not undertaken during the project included:

- change management plan
- stakeholder engagement and communications
- technical investigations / preliminary designs
- acceptance for testing
- acceptance for operations.

At project commencement, TasRail's project and change management processes were in draft form. They were not fully implemented until the end of July 2017 while the project was underway. This may have had a bearing on TasRail's ability to monitor and control the project during a period when these processes were being applied in practice for the first time.

In summary, the actions and documents required for each phase in TasRail's change management process either were not conducted, were incomplete, or did not contain the required formal approvals. As a result, important safety-related steps were not completed.

Assurance of change management activities

The generation 3 RCE project was able to proceed largely outside of TasRail's change management process primarily because the checks and balances within the broader system did not detect that this was happening. Specifically:

- There were no mechanisms by which non-completion of activities, documents or approvals would prevent progression of the project.
- TasRail had an audit program to ensure compliance, which this was limited to 12 selected projects per year. The generation 3 RCE was not chosen to be audited, and other audit requirements did not apply to this system.
- Funding for the equipment was (at least in this case) not dependent on the process having been followed.

In essence, the change management processes only nominally required that certain activities were conducted; and the mechanisms in place to detect when activities were not conducted and halt the project or alert people who could intervene were ineffective.

Identification of relevant safety assurance activities

TasRail had engineering design, verification, validation, and acceptance procedures, including those specifically for safety-critical items of rolling stock that would be considered relevant to a technical project such as the development of the generation 3 RCE. The procedures included requirements that technical specifications be developed and risk assessment and failure modes and effects (FMEA) analysis be performed. They also provided guidance on the level of technical expertise that should be involved.

However, there were no links to these procedures from elsewhere within the TasRail system of documents. In particular, there was no requirement to either follow or consider these procedures from within the change management process. Therefore, even if the change management process been fully followed for the project, the relevant safety and engineering assessment activities (with a significantly greater potential to prevent or identify safety-related problems) would

not necessarily have taken place. There was also the potential, albeit slight, that the relevant design assurance and acceptance activities would not be conducted in other projects, including the acquisition of new locomotives or other types of rolling stock.

As an example of where the absence of links between documents may affect the effectiveness of the change management process, there was no requirement or prompt for the person who completed an IIA to consider TasRail's definition of 'safety critical' (as written in the engineering processes) when determining whether a negative implication to safety existed.

Further, TasRail's change management process did not consider whole-of-life system management; that is, from initial planning and design to system decommissioning. This may have prevented the limited monitoring and review of risk associated with ongoing operation of generation 3 RCE after it was commissioned and had the potential to affect other projects as well.

Identification of potential safety impacts of change

Although the generation 3 RCE project could be considered small when compared with some of the projects undertaken by a rail operator (such as major infrastructure changes or the introduction of a new locomotive type), in safety terms a small project can still have a substantial impact. Even though the project was ultimately classified as significant (P2), the defined processes would not always result in the appropriate classification on the basis of safety in other circumstances.

The template IIA form directed assessors to classify a change as small or significant on the basis of 9 questions. The only question that had direct relevance to safety was whether there were 'any negative safety implications associated with the initiative'. In this case, the assessor answered 'no' and the project was classified as significant on the basis of other factors such as cost.

Such a question is inherently subjective, but more so in the absence of clear definitions. The significance of a proposed project with minimal strategic and business impacts could hinge on an individual's understanding of its 'negative safety implications' with no guidance as to what this means. As stated previously, the definition of 'safety critical' was in a separate document not linked to the IIA or other change management documents.

Also, the IIA form did not require an assessor to list or otherwise identify specific hazards, or to carry out any safety analysis activities beforehand. The change management process also did not require a hazard or risk identification activity prior to completing an IIA. This could lead to the incomplete consideration of hazards.

In addition, a change that did not qualify as significant under any of the other questions could then proceed as a small change with minimal control or oversight, even though the potential to impact safety could still be substantial.

The questions and guidance for determining safety of a significant change were similarly limited, potentially leading to under-classification. However, this would normally be less of a problem because all 'significant' projects required safety-related activities like risk assessments and risk action plans.

Summary

In summary, TasRail had a detailed change management process in place, and had documented that the project to develop the generation 3 RCE was a significant change. However, the project, a significant change with unique operational risks, proceeded without many of the activities required by TasRail's change management process being completed. Furthermore, even had the defined process been followed, TasRail's systems for management of change had a limited capability to:

- assure pre-determined activities, approvals, and documentation were completed throughout progression of a change
- identify the need for relevant safety assurance activities

- assure the determination of whether a change had the potential to impact safety.

Processes for fault tracking and analysis

Introduction

It is obviously most effective and safer for problems with the design and integration of a system to be identified and managed prior to its implementation into normal operations. Nevertheless, even after implementation, there are opportunities available to identify and manage problems.

This section discusses TasRail's management of fault reports and other issues that arose during the first months of generation 3 RCE operation (that is, after it was commissioned in February 2018 and prior to the runaway in September 2018).

In-service tests

There was no formal process for TasRail drivers to verify RCE safety functionality before continuing operations after an RCE failure occurred. ADE did not stipulate a requirement, apart from after a cold start, and drivers advised the ATSB that tests were generally only conducted after a prolonged locomotive and train shutdown had occurred.

Although periodic functionality checks existed, the RCE was not required to be checked in a similar fashion to a locomotive, although it replicated many locomotive commands. Further, in-service periodic testing of RCE safety functions, such as the RCE transmitter emergency stop switch and vigilance and tilt functions, were not performed by drivers, nor did TasRail require them to be.

Fault reporting and follow-up

Although multiple TasRail staff were involved in addressing reported generation 3 RCE faults, the extent of their responsibility in this regard was unclear and there did not appear to be anyone identified to lead the fault report analysis and management process.

Exacerbating the limited asset ownership and oversight was the absence of a formal process for reporting or addressing faults specifically related to the new RCE. More specifically:

- There was no procedure or dedicated form for drivers to record generation 3 RCE faults.
- A shift form partially tracked RCE faults, but only in relation to time delays.
- Drivers advised the ATSB that, unless an RCE fault was persistent or caused a significant time delay, it was unlikely they would report or log the fault.
- Although the network control officers (NCOs) would log emergency alarms from RCE failures and RCE faults reported to them by drivers, there was no defined escalation process.

It is certain that drivers encountered more faults with the generation 3 RCE than was formally reported or recorded. TasRail had some awareness of under-reporting of RCE faults; however, it is unclear how, or whether, it addressed this problem.

Further, of those faults that were reported, there was evidence of misdiagnosis or a lack of information available to define what the faults were and why they were being encountered. For example:

- The control fault mode response had been changed, which made its response similar to the previous generation's communication failed mode response. This change, and the visual similarity between how the two fault modes were displayed on the transmitter (CNF or COMF), introduced the potential for confusion between the 2 modes, leading to misdiagnosis by drivers and other staff.
- The origin of control fault mode occurrences, where identified, was not investigated or determined.

- Uncommanded emergency brake applications, similar to that observed during the runaway on 21 September 2018, were reported by drivers. These were not attributed to any known fault or penalty condition.
- Fault modes that required a cold start of the RCE receiver to reset were reported. However, there were no documented fault conditions that required a cold start to clear. This indicated that an unidentified failure mode was occurring.

Even though the type, origin, and cause of some of the reported faults and recovery actions were unknown or unexplained, further investigation before operation recommenced was not common.

When faults were further investigated, the limited information available (both immediately available and recorded) was a barrier to the identification, analysis, diagnosis and thereby correction of reported RCE faults by both TasRail and ADE. Problems with the recording of relevant RCE data are discussed further in *Recording of remote control equipment functions*.

In addition, other limitations also existed in the follow-up of RCE fault reports, separate to the limited data availability. For example:

- Only some logged RCE faults were forwarded by TasRail to ADE to review. Outcomes from these reviews were not formally documented.
- TasRail specifically consulted with ADE regarding driver reported safety concerns, at which point ADE assured TasRail that the RCE met fail-safe requirements. However, it did not support this claim with evidence and TasRail did not attempt to verify the claim.

Although TasRail recorded at least 100 remote-control failure events (in addition to much more common communication failed mode events) from January to September of 2018, only one was identified as a safety concern and captured in TasRail's risk management system. Even then, this was done due to the issue of limited trackside access, not a concern over the safety of the RCE during the failure. That events were not treated as safety concerns was further indication that TasRail believed that the reported failures resulted in a safe state and that the RCE was a failsafe system.

Prior fail-to-unsafe event

One reported fault event occurred while the cement train crossed Caroline Creek in May 2018, 4 months before the runaway involving train no. 604. Although TasRail requested ADE to analyse this event, it is unclear what response ADE provided to explain it. ADE was unable to explain the cause of the event to the ATSB.

Analysis of the event conducted by the ATSB indicated that the RCE had not enacted the behaviour expected for the documented fault modes and had therefore not failed to a safe state. The unknown state that the RCE entered was only recovered after an uncommanded locomotive engine restart resulted in a receiver reboot. The analysis concluded that both the behaviour of the generation 3 RCE while a fault state was present, and that external systems were required both to maintain locomotive brakes and cold start the RCE receiver, were indications that the state the RCE was in had the potential to be unsafe.

Although the available data was not sufficient to determine why the RCE had entered this fault condition, the responses recorded during this event were not consistent with the intent of the RCE as having been designed with the objective of being fail-safe. This was not addressed by either TasRail or ADE and the generation 3 RCE was allowed to continue in service.

Summary

In summary, TasRail did not have a reliable process to systematically identify, track and analyse reported faults on its remotely-controlled trains in order to identify their potential safety implications. The repeated instances of the RCE 'failing', albeit without consequence, were not acknowledged as indicators of a potential safety problem: numerous operational issues may be indicators of design or process issues, which can indicate latent safety flaws.

Overall, the absence of a formal oversight structure that could monitor safety trends in relation to repeated reported faults significantly limited TasRail's ability to identify and manage problems with the generation 3 RCE prior to the runaway.

Notification of change to the regulator

Notification of change

Accredited RTOs are required to notify ONRSR of certain types of changes to their operations. Notifications provided ONRSR with visibility of changes that could affect safety, allowing ONRSR to initiate regulatory activity if needed.

Through published guidance material, ONRSR encouraged RTOs to contact them if clarification was needed as to whether a given change was notifiable. TasRail's risk and compliance manager did so for the generation 3 RCE project in December 2017, prior to RCE testing and commissioning.

As already noted, the concept that the generation 3 RCE project was like-for-like was an accepted view within TasRail. It is therefore reasonable that the compliance manager, who only had limited involvement in the project, also held this view when they described the change as like-for-like with the addition of a dynamic brake to the ONRSR rail safety officer.

The ONRSR rail safety officer made a record of this conversation that is consistent with an understanding that it was simply an identical replacement unit, or at most a very minor change, repeating the term 'like-for-like.' On this basis, the ONRSR rail safety officer advised the TasRail manager that it was not a notifiable change.

Consequently, associated with the limited internal communication about the extensive changes from generation 2 to generation 3 RCE, TasRail did not submit a formal notification of change for generation 3 RCE to ONRSR. This limited the regulator's visibility of the change and, as a result, regulatory oversight of the project was not initiated. It is likely that, had ONRSR had greater awareness of the extent of the change, its oversight activities would have helped both ONRSR and TasRail identify limitations with TasRail's change management processes (discussed in *Change management limitations*).

Guidance on the regulatory requirements for a notification of change

Under Australia's co-regulatory rail regulation framework, RTOs are granted 'operational flexibility to establish and implement standards, rules and methods of operation' to meet regulatory requirements. ONRSR provided legislative interpretations, guidance and compliance expectations to ensure consistent application of the regulatory requirements without constraining this operational flexibility.

Guidance on the change notification process included an overview of the process, brief interpretations and examples for some of the 12 notifiable items under regulation 9(1)(a), and a recommendation that RTOs contact ONRSR for clarification where required. However, overall there was minimal guidance information provided for interpreting what types of changes required notification, including for changes related to item 3 ('a change to a safety critical element of existing rolling stock'), either for RTOs or for ONRSR's rail safety officers.

Three important terms were used in the item 3 requirement:

- change
- safety-critical
- element of existing rolling stock.

However, these terms had the potential to be interpreted differently by different parties, particularly given the minimal guidance information provided by ONRSR.

More specifically, the term ‘change’ alone does not convey the extent of functional, physical, or software changes for which a notification of change is justified. It could mean:

- a replacement item that is identical to the original
- an item that is very similar to the original in terms of its function and mechanism of operation
- an item that had identical functions but different mechanisms of operation, or
- an item that could be used to functionally replace the original, but had additional or changed functions and/or mechanisms of operation.

The differences between the new and replacement item could vary in importance and extent, and some changes could require modifying procedures or retraining of operators (in terms of how to use the equipment and/or underlying system knowledge). Moreover, even a small change to one function could inadvertently affect other functions in unexpected ways, particularly in complex systems. It is therefore important to be clear about the nature and extent of changes that require closer attention.

The term ‘safety-critical’ also had the potential for different interpretations. In the absence of a consistent definition, there is a potential for ‘safety-critical’ to be interpreted to refer to any item that could result in catastrophic consequences if it failed, rather than something that has a non-trivial contribution to safety. ONRSR provided guidance (in the *Notification of change fact sheet*) indicating the term meant equipment ‘whose failure could substantially contribute to a major accident.’ Dunn (2002) stated:

> The term “safety-critical” usually brings to mind nuclear plants, oil refineries, airliners, and other high-visibility applications where loss of safety can kill or injure in large numbers. ..[but] most safety-related system applications do not fall into the high-visibility category.

ONRSR’s guidance was consistent with this view, identifying safety-critical elements as those ‘whose failure could substantially contribute to a major accident.’ However, the same guidance stated that these elements are identified by the RTO’s safety management system, and ONRSR separately advised the ATSB that there was ‘scope for an operator [RTO] to interpret this [term] in the context of their own railway operations.’

TasRail defined ‘safety-critical’ as ‘any element whose failure or malfunction may result in death or serious injury to people, or loss or severe damage to equipment or environmental harm.’ A minimum severity of consequence would therefore needed to meet TasRail’s definition, but not necessarily a major accident.

The former *Transport (Rail Safety) Regulation 2010 (Qld)* applied the term to ‘any part of the rolling stock that could cause, or affect the impact of, an accident or incident if the part failed to operate properly.’ ONRSR’s interpretation supplied to the ATSB during the investigation was similarly broad, using the term ‘safety critical’ to refer to the potential for the equipment to cause, contribute to, or fail to mitigate an unsafe outcome, regardless of the seriousness of that effect. These broader definitions are more likely to capture elements that are safety-related even if their failure might not result in catastrophic outcomes.

Finally, the term ‘element of existing rolling stock’ was not clear for the purpose of the regulation. During the investigation, ONRSR advised the ATSB that, as the RCE controlled the movement and operation of a locomotive, it was to be considered an ‘element of the rolling stock’. The TR class locomotive was obviously rolling stock (a ‘vehicle that operates on or uses a railway’), and the components of the locomotive were ‘elements’ of existing rolling stock. However, although it is a valid argument that the RCE is a piece of equipment that attaches to and controls a locomotive (vehicle), there was the potential for RCE to not be viewed as a literal component of the locomotive.

ONRSR’s internal *Notification of change procedure*, which provided context for rail safety officers when giving effect to regulation 9(1)(a), did not provide interpretations or guidance for the application of these 3 terms (‘change’, ‘safety-critical’, and ‘element of existing rolling stock’).

Ultimately, in the absence of clarifying guidance to aid in the interpretation of these terms, there was no assurance that individual officers would interpret the terms in a manner that was consistent and optimal for the regulation's (and ONRSR's) safety intent. This increased the potential for different rail safety officers interpreting the legislation differently and giving conflicting or incorrect advice to RTOs.

Australian Standard AS 4292.3 (*Railway safety management, part 3: rolling stock*) provided guidance on what should be considered 'safety critical items' on rolling stock, but this standard has been withdrawn and the information was not reproduced among the RISSB products that superseded it or any guidance material provided to industry by ONRSR.

With regard to the generation 3 RCE, as it was the primary driver control interface, a failure could cause (or affect the impact of) an accident. Therefore, the RCE must be considered the type of equipment for which a change would be notifiable to ONRSR.

The ONRSR rail safety officer recorded the change as being 'a like for like replacement of the existing unit which has been in operation for some time and due for routine replacement.' This description is consistent with that of a routine equipment swap, not normally considered a significant change, and the officer did not know of any design or functionality differences with the previous equipment. Therefore, it is likely that the rail safety officer's understanding of the nature of the change was a key consideration in their decision not to require a notification of change in December 2017, rather than whether the equipment was safety-critical or an element of existing rolling stock. Given that this type of change would not normally require notification to the regulator, it is unlikely that the limited guidance provided by ONRSR to TasRail and the rail safety officer had an effect on the outcome in this instance.

In summary, the guidance provided by ONRSR about the requirement to submit a notification of change included limited detail about the extent or type of changes that necessitated a notification. In addition, with regard to 'a safety critical element of rolling stock', it did not provide detail with regard to the interpretation of 'safety critical' and the applicability to equipment that may not be inherently part of rolling stock (such as RCE). This situation was exacerbated after 2018 when some of the limited guidance provided by ONRSR for interpreting notification of change requirements (including a definition of 'safety critical') was removed in the transition from published guidance documents to an online portal.

Recording of remote control equipment functions

As discussed in *Non-recording of key data parameters*, the absence of recorded RCE data led to difficulties in fault finding and rectification throughout the use of the generation RCE and limited the determination of important aspects of the 21 September 2018 runaway sequence. It also potentially prevented TasRail and ADE from developing a full understanding of the Caroline Creek event and identifying strategies to minimise the likelihood of a further fail-to-unsafe event.

The use of an event recorder on all TasRail trains, including the cement train service, was required by a condition in TasRail's notice of accreditation issued by ONRSR. The use of event recorders was not mandated by any other means, and the use of a condition on a notice of accreditation for this purpose was not common.

The condition on TasRail's notice of accreditation stated that all 'leading locomotives or other vehicles used as the leading vehicle' were to be fitted with an event recorder. The reason why the condition was originally included by the Tasmanian rail regulator, and whether it was specifically introduced for the operation of remotely-controlled trains, could not be determined. ONRSR advised the ATSB that 'an event recorder fitted anywhere in the consist, that is recording the key parameters' would meet the intent of the condition. The question of whether the RCE constituted a 'leading locomotive' could be made on the basis of physical characteristics (the RCE is not a locomotive, and the locomotive was not always at the head of the train) or functionally (the RCE functions as a leading locomotive from a control perspective), but the distinction is not critical. An event recorder needs to record enough information to reconstruct enough of an accident or

incident sequence to determine what went wrong; in the case of TasRail's cement trains using RCE, this core purpose was not met.

ONRSR did not further define or explain what it considered 'key parameters' and TasRail also did not define what parameters were required to be recorded. Effectively, the condition could be met without recording the key parameters that would fulfil the core purpose of an event recorder.

An Australian standard for rolling stock event recorders (AS 7527:2015) described event recorder requirements and the parameters an event recorder should monitor to capture a minimum set of appropriate data. When compared to this standard, the data recorded during operation of TasRail's cement train service under RCE control did not include the following:

- controls being directly operated by the driver
- the vigilance function when performed by the RCE transmitter
- all changes to the operational status of a remotely-operated vehicle
- all control messages and status messages received and transmitted by a remotely-operated vehicle.

In summary, although ONRSR required TasRail to have an operating event recorder fitted to its trains, this requirement did not necessitate that key parameters of the RCE (and the driver's operation of the train) were recorded. Had the condition been more specific or functional in nature, it could have led TasRail to introduce a more effective recording capability for its RCE operations. Nevertheless, more consideration by TasRail of the contents of AS 7527 when introducing the generation 3 RCE (or before) would also have helped to address the situation.

System safety in the Australian rail industry

As outlined in this analysis, there were numerous latent safety concerns with the use of the ADE RCE in TasRail's cement train service. These largely arose through the limited application of safety management and safety engineering methodologies to a complex system. While the principles of safety management systems are widely applied across the rail industry, this and other recent ATSB investigations have found that safety engineering is sometimes not applied where it is needed.

The Australian Rail Safety National Law (RSNL) required organisations that procured or supplied rolling stock to ensure safety 'so far as is reasonably practicable,' including provisions for safety testing of equipment. However, although testing may be sufficient to ensure safety when systems are relatively simple, there are challenges in assuring the safety of software-based and other complex systems, in part due to difficulties in modelling complex interactions between system elements.

Key areas where equipment developers have had difficulty include specifying the requirements, designing and implementing a system to achieve the dependability requirements, and gaining confidence that the goals have been attained (Littlewood and Strigini 1995). From a practical perspective, it is difficult to decide the type, quality, and quantity of evidence required and the methodologies used to develop arguments about safety (Hawkins 2013). There is a considerable body of research in these areas and a wide variety of standards and guidance documents to aid in the system safety approach (see Appendix B).

Systems engineering is a way to manage complexity in design, including the potential for the developers themselves to make errors (Leveson 2016, Neumann 1994). These principles are the basis for system safety, which is a way of managing safety in a structured way. Dunn (2002) describes this as 'a distinct set of engineering and management principles, criteria, and techniques that not only help to define safety requirements but how the design process should be structured and conducted in order to realise a safe system.'

Even for simple systems, following a structured approach like this helps the RTO and equipment developer to understand how the equipment fits within the rail system and how it can affect safety.

It greatly reduces the number of ‘unknowns’. Dunn (2002) stated that safety-critical design and evaluation methods could be applied across the ‘full range of computer system applications’ from ‘the fly-by-wire airliner where large numbers of human lives are at stake down to the small manufacturing facility where human injury or product damage represent the worst-case safety outcome.’

As an example of the approach, Edwards (1997) described how a United Kingdom rail operator maintained safety assurance when commissioning a new product:

> The [operator] needs to be assured that the use of a product is not going to import levels of risk that would compromise their existing safety performance. To provide this assurance the ‘sponsor’ of a product needs to demonstrate that the design, manufacture and installation was carried out in a systematic manner. Hazards were identified, risks assessed and suitable and sufficient control measures have been selected and imposed and further, that the work was carried out under a proper quality and safety management regime.

Edwards named several standards that detail assurance processes for different systems or parts of systems:

- safety-related system (IEC 1508)
- rail system (EN 50126)
- railway signalling control and protection system that uses software (EN 50128)
- safety-related railway signalling electronics (EN 50129).

Of these, EN 50126 (*Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*) is the most directly applicable to the safety of remotely-controlled trains. It stated that it is applicable to:

> … all railway applications and at all levels of such an application, as appropriate, from complete railway systems to major systems and to individual and combined subsystems and components within these major systems, including those containing software.

There are other standards that are broadly similar, and EN 50126 is presented here as one example of the type of standard that can be applied to attain a nominal level of system safety assurance in rail. It has not yet been issued as an Australian standard, so has limited visibility within the Australian rail industry.

Another problem is that to fully understand this 670-page standard in practice requires specialist knowledge, and to apply it may require a level of human resources that are simply not available to, or too costly for, small organisations. This type of detailed and complex standard cannot be easily tailored for simple application, even though the broadest principles can still be useful.

When implemented in full, many of these system safety practices come at a significant cost—well into the millions of dollars even for relatively small projects. For this reason, it is very important to use standards that are appropriate to the application. This means the level of detail in the standard should be enough to overcome the safety needs of the application, but not so much as to make the project unviable.

In addition, standards are inherently expensive: Hobbs (2020) estimated a cost of about US$3,000 for a single-user license to read IEC 61508, adding that this may be a barrier between small organisations and legal copies of important standards.

Furthermore, someone with even a moderate level of system safety expertise might not recognise the significant differences between a claim that a product meets a standard, an assertion or certificate from a non-accredited independent body, and certification from a body that itself has been accredited to issue certification for that standard. This means that some operators might think that a system or device meets, or was developed in full accordance with, a standard when it does not. To alleviate this risk, operators can attain certification from an accredited body, or by producing or reviewing a document that sets out how each element of the standard has been met, or why it has not (for example, if an element is optional or not applicable).

At the time of 21 September 2018 runaway, the Australian standards relating to rolling stock safety were mostly what is known as 'specification' standards; that is, focusing on the characteristics of the end product (such as dimensions) rather than the process of design. There was no explicit regulatory requirement for developers of rail equipment to demonstrate an objective evaluation of design safety or apply system safety principles during development. An RTO could apply specification standards and not broader process standards, such as those that are used for design safety assurance.

This approach has limitations. It is simpler to prove adherence to a specification than to a process but a specification may have limited application. For example, a specification for rail track geometry cannot be applied to anything else. Specification standards also have limited effectiveness when applied to complex systems. Process standards tend to focus more on principles and process, enabling developers and operators to cope with higher levels of complexity.

There has been an increasing global emphasis on system safety in rail, and the Australian rail industry has increasingly applied systems engineering principles over the past decade, particularly in NSW and Victoria (Welschen and others 2021). However, Welshen and others also noted that the Australian transport sector lacked national direction in the application of systems engineering compared with the defence sector or that provided in other countries.

In 2013, system safety guidance material specific to the rail industry was collated into an *International Engineering Safety Management Handbook*,[90] which was aimed at 'clearly outlining the activities involved in making a system or product safe and providing the evidence that it is safe.' The extent to which this and other guidance reached the Australian rail industry is unclear. At the time of the runaway, there was no equivalent guidance with high visibility and relevance to the Australian rail industry. In addition to the runaway involving the TasRail cement train no. 604, the runaway involving the BHP iron ore train in November 2018 also involved problems with the integration of complex systems associated with the non-application of a systems engineering framework.[91]

Of the standards that were highly visible and applicable to the Australian rail industry, AS 7501 (*Rolling stock compliance certification*) was relatively simple to apply but, in addition to being optional, did not directly lead RTOs to develop a safety case or perform safety analyses. This was done in AS 7702 (*Rail equipment type approval*), but this standard primarily did not apply to rolling stock. Similarly, ONRSR's guidance on major projects listed several activities that could be beneficial for smaller projects that are still complex and safety-critical, such as the development of the generation 3 RCE.

By contrast, the manufacture and modification of transport category aircraft (which includes almost all commercial passenger or cargo aircraft) has been governed by regulations requiring equipment, systems, and installations to be designed to reduce the likelihood of unsafe failure conditions to a specified amount.[92] Compliance must be shown by analysis and, where necessary, tests that consider:

- possible modes of failure including malfunctions and damage from external sources
- the probability of multiple failures and undetected failures
- the resulting effects in different operating phases and conditions, and
- warning cues, corrective actions, and fault-detection capability.

---

90 Available at https://www.intesm.org/

91 ATSB RO-2018-018 *Runaway and derailment of loaded ore train M02712, near the 211 km mark south of Port Hedland, Western Australia, on 5 November 2018*.

92 In Australia, Civil Aviation Safety Regulation 25.001 requires aircraft to meet European or United States regulations, which include the relevant system safety requirements under EASA CS 25.1309 or FAR 25.1309 respectively.

Where these rules applied, there was generally associated guidance to show acceptable means of compliance. For example, in the United States, Advisory Circular 25.1309 provided extensive details about technical considerations that should be made and lists several aviation system safety standards that can be used to show compliance. [93]

In conclusion, although standards, legislative requirements, and guidance for rail safety were recognised and applied in Australia, they were of limited value in the development and operation of complex systems. Conversely, the standards and guidance for system safety available at the time of the runaway were either:

- too abstract, complex, costly and/or impractical for widespread recognition and acceptance by the Australian rail industry
- not required to be applied to rolling stock (AS 7702), or
- not applicable to projects that were complex but not 'major' (*ONRSR Guideline – Major Projects*).

If an RTO or equipment developer intended to apply system safety principles, there were still numerous challenges in attaining justified confidence in its success, which were difficult even for experts to overcome. Finally, under Australia's co-regulatory rail safety framework, there was no explicit regulatory requirement to apply system safety processes in the Australian rail industry, and minimal guidance other than for 'major' projects.

[93] ATSB AO-2008-070 *In-flight upset - Airbus A330-303, VH-QPA, 154 km west of Learmonth, WA, 7 October 2008* includes a discussion on the application of safety analysis methodologies within a system safety assurance framework.

Findings

ATSB investigation report findings focus on safety factors (that is, events and conditions that increase risk). Safety factors include 'contributing factors' and 'other factors that increased risk' (that is, factors that did not meet the definition of a contributing factor for this occurrence but were still considered important to include in the report for the purpose of increasing awareness and enhancing safety). In addition 'other findings' may be included to provide important information about topics other than safety factors.

Safety issues are highlighted in bold to emphasise their importance. A safety issue is a safety factor that (a) can reasonably be regarded as having the potential to adversely affect the safety of future operations, and (b) is a characteristic of an organisation or a system, rather than a characteristic of a specific individual, or characteristic of an operating environment at a specific point in time.

These findings should not be read as apportioning blame or liability to any particular organisation or individual.

From the evidence available, the following findings are made with respect to the runaway and derailment of TasRail freight train in Devonport, Tasmania on 21 September 2018.

Contributing factors

- While the driver was conducting loading operations at Railton (from outside of the train), the remote control equipment (RCE) entered a spurious fault condition (involving the application of emergency braking) that was almost certainly associated with the RCE's response to rapid movement of the RCE transmitter's direction controller. This likely led to the RCE entering a persistent unresponsive state in which the train's brakes were not applied, allowing the train to roll away.
- **The TasRail cement loading facility at Railton had a downhill grade to the main line, and no devices to protect against a runaway.** (Safety issue)
- After the train rolled away from Railton, the remote control equipment's receiver did not apply the train's brakes as designed when outside radio communication range. The train's brakes remained in a released (unapplied) state until the derailment.
- **The Air Digital Engineering generation 3 remote control equipment (RCE) had several safety-related design and integration problems, which were readily identifiable. These included:**
  - **unintended activation-and-release of emergency braking on the locomotive**
  - **recovery from an emergency brake application and certain penalty states that was inconsistent with locomotive braking system timeout controls**
  - **the potential to enter a persistent unsafe state during initialisation, which was unrecoverable without external intervention**
  - **the absence of a means to detect and respond to an emergency brake application from a source external to the RCE**
  - **the vigilance and driver-commanded emergency stop functions being unavailable in the absence of an active radio communications link.** (Safety issue)
- **Although Air Digital Engineering had safety as a design objective and safety elements were included in the remote control equipment, system safety assurance activities appropriate to its application were not conducted.** (Safety issue)
- **TasRail commissioned the manufacture of, and continued to use, redesigned safety-critical remote control equipment for operating a locomotive without systematic assurance of its safety, leading to excessive reliance on the manufacturer. This was because TasRail did not:**
  - **fully engage with the development process from initial design through to commissioning, or understand the extent of design changes associated with the**

introduction of the generation 3 RCE (which reduced the capability to prevent, identify and resolve design and integration problems)
  - **explicitly identify and impose safety requirements**
  - **verify that the overall system met a specified level of safety.** (Safety issue)
- **Although there were no previous accidents attributable to TasRail's use of remote control equipment (RCE) over 19 years, TasRail did not identify or fully assess the safety implications of remotely-controlled train operations, or those of TasRail's specific implementation. These included the:**
  - **potential for remote control equipment to fail to an unsafe state without external risk controls**
  - **suppression or absence of some safety functions of the TR class locomotive, including overspeed protection and some indications provided to drivers**
  - **non-recording of key data parameters to facilitate effective fault and incident analysis**
  - **increased risk of derailment as a result of motive power located only at the rear of the train.** (Safety issue)
- Associated with the limited internal communication about the extensive changes from the second to the third generation remote control equipment, TasRail did not submit a notification of change to the Office of the National Rail Safety Regulator. As a result, regulatory oversight of the project was not initiated.
- **Although TasRail had a detailed change management process in place, and had documented that the project to develop the third-generation remote control equipment was a significant change, the change management process had a limited capability to:**
  - **assure pre-determined activities, approvals, and documentation were completed throughout progression of a change**
  - **identify the need for relevant safety assurance activities**
  - **assure the determination of whether a change had the potential to impact safety.** (Safety issue)
- **TasRail did not have a reliable process to systematically identify, track and analyse reported faults on its remotely-controlled train or to identify their potential safety implications.** (Safety issue)
- **There was limited practical guidance specifically for the Australian rail industry for the application of system safety assurance processes to the development of complex and safety-critical rail systems.** (Safety issue)

Other factors that increased risk

- Although TasRail had documented that the project to develop the generation 3 remote control equipment was a significant change, most pre-determined activities required to be conducted for that type of change were not performed during the project.
- **The guidance provided by the Office of the National Rail Safety Regulator about the requirement to submit a notification of change included limited detail about the extent or type of changes that necessitated a notification. In addition, with regard to 'a safety critical element of rolling stock', it did not provide detail with regard to the interpretation of 'safety critical' and the applicability to equipment that may not be inherently part of rolling stock (such as remote control equipment).** (Safety issue)
- **TasRail's processes for ensuring immediate network control actions in response to emergencies (such as runaway and authority exceedance) fundamentally relied on the experience and knowledge of network control officers and did not include the provision of procedures, tools and checklists detailed enough to support the effective**

management of specific types of incidents that require a time-critical response. (Safety issue)

- Although the Office of the National Rail Safety Regulator required TasRail to have an operating event recorder fitted to its trains, this requirement did not necessitate that sufficient parameters of the remote control equipment (RCE) were recorded for optimal outcomes of internal and external safety investigations into events involving use of the RCE.

Other findings

- The driver, TasRail network control and other staff, and emergency services conducted a prompt and effective response to minimise consequence as the runaway train descended into Devonport.

Safety issues and actions

Central to the ATSB's investigation of transport safety matters is the early identification of safety issues. The ATSB expects relevant organisations will address all safety issues an investigation identifies.

Depending on the level of risk of a safety issue, the extent of corrective action taken by the relevant organisation(s), or the desirability of directing a broad safety message to the rail industry, the ATSB may issue a formal safety recommendation or safety advisory notice as part of the final report.

All of the directly involved parties were provided with a draft report and invited to provide submissions. As part of that process, each organisation was asked to communicate what safety actions, if any, they had carried out or were planning to carry out in relation to each safety issue relevant to their organisation.

The initial public version of these safety issues and actions are provided separately on the ATSB website, to facilitate monitoring by interested parties. Where relevant, the safety issues and actions will be updated on the ATSB website as further information about safety action comes to hand.

Absence of runaway protection at Railton

Safety issue description

The TasRail cement loading facility at Railton had a downhill grade to the main line, and no devices to protect against a runaway.

Issue number:	RO-2018-014-SI-14
Issue owner:	TasRail
Transport function:	Rail: Infrastructure
Current issue status:	Closed – Adequately addressed
Issue status justification	The ATSB is satisfied that the installation of a radio-operated, self-restoring catch point at Railton has adequately addressed the safety issue.

Proactive safety action taken by TasRail

Action number:	RO-2018-014-PSA-05
Action organisation:	TasRail
Action status:	Closed

On 30 November 2020, TasRail completed installation of a radio-operated, self-restoring catch point at the western end of the Railton siding.

On 15 July 2022 TasRail advised that it had also:

> …completed a risk assessment of the entire operating network in relation to runaway protection. The risk assessment included associated gradient analysis in relation to the operation or storage of rolling stock at loading, unloading, shunting, stabling and storage locations where rolling stock may move in an uncontrolled manner and run away.

Remote control equipment design and integration problems

Safety issue description

The Air Digital Engineering generation 3 remote control equipment (RCE) had several safety-related design and integration problems, which were readily identifiable. These included:

- unintended activation-and-release of emergency braking on the locomotive
- recovery from an emergency brake application and certain penalty states that was inconsistent with locomotive braking system timeout controls

- the potential to enter a persistent unsafe state during initialisation, which was unrecoverable without external intervention
- the absence of a means to detect and respond to an emergency brake application from a source external to the RCE
- the vigilance and driver-commanded emergency stop functions being unavailable in the absence of an active radio communications link.

Issue number:	RO-2018-014-SI-16
Issue owner:	Air Digital Engineering (ADE)
Transport function:	Rail: Rollingstock
Current issue status:	Closed – No longer relevant
Issue status justification:	TasRail advised that it had withdrawn all remote-control technology and ADE advised that the generation 3 remote control equipment has not been offered to, or used by, any other rolling stock operators. ADE advised that it would re-evaluate the generation 3 remote control equipment under system safety design principles if it were to be used for future operations. Accordingly, the safety issue is no longer relevant.

Proactive safety action taken by Air Digital Engineering

Action number:	RO-2018-014-PSA-06
Action organisation:	Air Digital Engineering
Action status:	Closed

On 5 July 2022 Air Digital Engineering (ADE) advised:

> In the future, with any continuation work of the RCE [remote control equipment] product, ADE would appropriately address the points the ATSB has raised. This would also lead to a re-evaluation with reference to AS [Australian Standard] 61508 of the RCE as well as the consideration of new technologies for the practical implementation of a calculated SIL factor using new microprocessor architecture selection, for example two out of two voting processes for the benefit of design safety assurances.
>
> The integration problems and other matters of software / hardware arrangement may be addressed by software design with the necessary testing and documenting in accordance with the AS 61508 standard and changes to hardware also in accordance with the same standard. This could include further references to associated standards that have evolved since the original IEC [International Electrotechnical Commission] 61508 Draft publication in the mid 1990"s as well as the publications mentioned within the ATSB's draft report and also, taking into account the report's referencing under: System safety in the Australian rail industry.

Remote control equipment system safety assurance

Safety issue description

Although Air Digital Engineering had safety as a design objective and safety elements were included in the remote control equipment, system safety assurance activities appropriate to its application were not conducted.

Issue number:	RO-2018-014-SI-02
Issue owner:	Air Digital Engineering (ADE)
Transport function:	Rail: Rollingstock
Current issue status:	Closed – Adequately addressed
Issue status justification:	TasRail advised that it had withdrawn all remote-control technology and ADE advised that the generation 3 remote control equipment has not been offered to, or used by, any other rolling stock operators. ADE advised that it would re-evaluate

	the generation 3 remote control equipment under system safety design principles if it were to be used for future operations. Accordingly, the safety issue is no longer relevant.

Proactive safety action taken by Air Digital Engineering

Action number:	RO-2018-014-PSA-06
Action organisation:	Air Digital Engineering
Action status:	Closed

On 5 July 2022 Air Digital Engineering (ADE) advised:

> In the future, with any continuation work of the RCE [remote control equipment] product, ADE would appropriately address the points the ATSB has raised. This would also lead to a re-evaluation with reference to AS [Australian Standard] 61508 of the RCE as well as the consideration of new technologies for the practical implementation of a calculated SIL factor using new microprocessor architecture selection, for example two out of two voting processes for the benefit of design safety assurances.
>
> The integration problems and other matters of software / hardware arrangement may be addressed by software design with the necessary testing and documenting in accordance with the AS 61508 standard and changes to hardware also in accordance with the same standard. This could include further references to associated standards that have evolved since the original IEC [International Electrotechnical Commission] 61508 Draft publication in the mid 1990s as well as the publications mentioned within the ATSB's draft report and also, taking into account the report's referencing under: System safety in the Australian rail industry.

Remote control equipment commissioning process

Safety issue description

TasRail commissioned the manufacture of, and continued to use, redesigned safety-critical remote control equipment for operating a locomotive without systematic assurance of its safety, leading to excessive reliance on the manufacturer. This was because TasRail did not:

- fully engage with the development process from initial design through to commissioning, or understand the extent of design changes associated with the introduction of the generation 3 RCE (which reduced the capability to prevent, identify and resolve design and integration problems)
- explicitly identify and impose safety requirements
- verify that the overall system met a specified level of safety.

Issue number:	RO-2018-014-SI-03
Issue owner:	TasRail
Transport function:	Rail: Rollingstock
Current issue status:	Closed – No longer relevant
Issue status justification	TasRail advised that it had withdrawn all remote-control technology. The withdrawal of all remote-control technology negates the need for safety action to directly address each aspect of the safety issue as the system in question is no longer in use.

Proactive safety action taken by TasRail

Action number:	RO-2018-014-PSA-07
Action organisation:	TasRail
Action status:	Closed

On 15 July 2022 TasRail advised that it had withdrawn all remote-control technology.

See *Management of safety-related change* (RO-2018-014-SI-05) for additional safety action undertaken by TasRail to provide safety assurance to future projects.

Safety implications of remote control of trains

Safety issue description

Although there were no previous accidents attributable to TasRail's use of remote control equipment (RCE) over 19 years, TasRail did not identify or fully assess the safety implications of remotely-controlled train operations, or those of TasRail's specific implementation. These included the:

- potential for remote control equipment to fail to an unsafe state without external risk controls
- suppression or absence of some safety functions of the TR class locomotive, including overspeed protection and some indications provided to drivers
- non-recording of key data parameters to facilitate effective fault and incident analysis
- increased risk of derailment as a result of motive power located only at the rear of the train.

Issue number:	RO-2018-014-SI-07
Issue owner:	TasRail
Transport function:	Rail: Rollingstock
Current issue status:	Closed – No longer relevant
Issue status justification:	TasRail advised that it had withdrawn all remote-control technology. The withdrawal of all remote-control technology negates the need for safety action to directly address each aspect of the safety issue, including the need to record additional data parameters beyond those recorded by existing systems on the TR class locomotives. Accordingly, the safety issue is no longer relevant.

Proactive safety action taken by TasRail

Action number:	RO-2018-014-PSA-07
Action organisation:	TasRail
Action status:	Closed

On 15 July 2022 TasRail advised that it had withdrawn all remote-control technology.

See *Management of safety-related change* (RO-2018-014-SI-05) for additional safety action undertaken by TasRail to provide safety assurance to potential future operations involving remotely-controlled trains.

Management of safety-related change

Safety issue description

Although TasRail had a detailed change management process in place, and had documented that the project to develop the third-generation remote control equipment was a significant change, the change management process had a limited capability to:

- assure pre-determined activities, approvals, and documentation were completed throughout progression of a change
- identify the need for relevant safety assurance activities
- assure the determination of whether a change had the potential to impact safety.

Issue number:	RO-2018-014-SI-05
Issue owner:	TasRail
Transport function:	Rail: Freight
Current issue status:	Closed – Adequately addressed
Issue status justification	The ATSB is satisfied that TasRail's amended change management processes adequately addresses the safety issue.

Proactive safety action taken by TasRail

Action number:	RO-2018-014-PSA-08
Action organisation:	TasRail
Action status:	Closed

On 15 July 2022 TasRail advised the following in terms of the assurance of progression of a change:

> In order to address these issues, TasRail has implemented a revised Management of Change System's Project Delivery Process which provides step-by-step instructions to Change Leads on how to deliver a change/project from conceptualisation through to finalisation. The Project Delivery Process includes key points where safety assurance activities and safety impacts are to be identified, assessed, mitigated, and verified.
>
> The Project Delivery Process has key hold points embedded within it as mandatory "checks" to ensure appropriate governance. Some of these include:
>
> - Review and approval by the accountable (risk) delegate of the Initial Change Assessment (ICA), which is the tool to assist Change Leads/delivery teams in assessing the risk and impact of a proposed change. The ICA has a multi-stage assessment approach to determine the type, complexity, and size of a project, which in turn drives the risk and impact. The tool provides Change Leads with the ability to undertake quantitative assessments of the proposed changes inclusive of business capability and safety impacts. The ICA will provide recommendations regarding the use of Technical Advisors depending on the level of technical complexity.
> - Review and approval by the accountable (financial) delegate of the Project Business Case, which is the document to justify the implementation of a change and includes risk management and project planning components.
> - Review and approval by the appropriate delegate of any Acceptance for Testing requirements, which includes the approval of any pre-prepared, reviewed and endorsed Testing/Commissioning Plans.
> - Review and approval by the appropriate delegate of any Acceptance for Operation requirements, which includes the verification that all interfacing and integration activities, as specified in the Project's Requirements Management System, has been undertaken.
> - Review and approval by the appropriate delegate of any Handover requirements, which includes the verification that all Requirements Management System items are completed and compliant.
> - Various points through the project delivery for stakeholder review, endorsement, and approval, inclusive of any external Technical Advisors and/or Independent Safety Assessors.
>
> In addition to these mandatory check points, the Project Delivery Process makes note that additional checkpoint approvals may be required for individual projects, and such governance processes should be determined on a project-by-project basis based on risk and impact to the business.

TasRail advised the following in terms of the need for relevant safety assurance activities and the determination of whether a change had the potential to impact safety:

> It should be noted that the system itself does not identify the need for relevant safety assurance activities but provides a consistent platform for the business to be able to assess projects and

determine if safety assurance activities are required. It does this by providing guidance to delivery teams about what and when certain activities (safety assurance being one) should be considered and managed. It is an embedded requirement of the system, that the personnel assessing, undertaking, reviewing and authorising Management of Change be competent in the areas that they are involved.

TasRail additionally advised:

> [The newly-developed Management of Change System] provides detailed guidance and tools to assist Change Leads in ensuring safety assurance activities are considered, planned and verified throughout the implementation of a change.
>
> The Management of Change System achieves this through the following:
>
> - the Integrated System Framework Manual provides information on System Safety Management (Section 5.12) inclusive of Safety Assurance elements, documentation, speciality engineering, Safety in Design and information regarding competency for personnel carrying out various safety assurance activities;
> - the Project Delivery Process provides step by step instructions to Change Leads on how to deliver a Change/Project from conceptualisation through to finalisation. This Project Delivery Process includes key points where Safety Assurance activities and Safety Impacts are to be identified, assessed, mitigated and verified;
> - risk assessment and risk management activities, in line with TasRail's risk management framework, are embedded in the process from the initial assessment of the change (mandatory Risk Assessment and also secondary Impact Assessment if residual risks are greater than low) through the planning, design and implementation of the change with drumbeat monitoring, update and management of the project risk assessment required; and
> - the use of a Requirements Management System with minimum inclusions provides Change Leads and delivery teams with a holistic way of capturing all requirements inclusive of safety requirements and then creating a platform to verify each individual requirement to ensure that the change has met deliverables.
>
> Finally, TasRail [has conducted] training for approximately 90 of its employees who will use, or be exposed to, the Management of Change System so that they have a proper understanding of the system and its requirements.

ATSB comment

The ATSB notes that TasRail's wide-ranging new processes address each aspect of the safety issue in detail. In addition to the benefits described by TasRail in its response to this safety issue, the processes:

- follow the systems engineering V-model, requiring safety arguments to be made, updated and managed throughout the life of a contract or project, supported by documented evidence in a safety assurance report
- require system safety management through the specification, verification and validation of requirements, including quantitative safety requirements, which are addressed through the use of safety assurance plans, a hazard log, safety assurance reports, and engineering assurance registers
- require an independent safety advisor to be engaged based on technical or safety complexity of the project.

Such activities necessarily require close engagement with the development process when using vendors or contractors and are likely to provide reliable, documented safety assurance to all types of activities.

Processes for fault tracking and analysis

Safety issue description

TasRail did not have a reliable process to systematically identify, track and analyse reported faults on its remotely-controlled train or to identify their potential safety implications.

Issue number:	RO-2018-014-SI-15
Issue owner:	TasRail
Transport function:	Rail: Freight
Current issue status:	Closed – Adequately addressed
Issue status justification	The ATSB is satisfied that TasRail's processes for fault tracking and analysis, including the assignment of responsibility to a specific manager, will adequately address the safety issue across TasRail's operations.

Proactive safety action taken by TasRail

Action number:	RO-2018-014-PSA-01
Action organisation:	TasRail
Action status:	Closed

On 25 March 2021 TasRail advised it was implementing a new asset management system.

On 15 July 2022 TasRail detailed some of the capabilities of this system:

> TasRail has addressed this issue through a requirement that all reports related to remote operations from drive to control be reported through its risk management software *Risk Wizard*. This software will provide a repository for all reports relating to remote operations from drivers to Network Control. This is because *Risk Wizard* sends a text message to a large number of people in the organisation, providing visibility over the incidents.
>
> These incidents will be routinely discussed at morning meetings, and then transferred to the asset management system *Maximo* (which is a new system, which TasRail is in the process of implementing). This will ensure that system faults are systematically tracked to resolution. This approach provides for transparency and technical review and will be managed by a dedicated resource—the Engineering and Reliability Manager.
>
> These systems will be utilised when TasRail re-instates remotely controlled equipment.

System safety assurance guidance for the Australian rail industry

Safety issue description

There was limited practical guidance specifically for the Australian rail industry for the application of system safety assurance processes to the development of complex and safety-critical rail systems.

Issue number:	RO-2018-014-SI-01
Issue owners:	Rail Industry Safety and Standards Board (RISSB) Office of the National Rail Safety Regulator (ONRSR)
Transport function:	Rail: Other
Current issue status:	Closed – Adequately addressed
Issue status justification:	The standard and guidance developed by RISSB directly address the availability, relevance, and practicability concerns of the other standards and guidance previously generally available in Australia. Further, the fact sheets published by ONRSR show a greater regulator emphasis on these approaches in general.

	Although compliance with such standards is not yet mandatory, ATSB recognises that there are practical limits to how rapidly systems safety methodologies can be widely adopted.

Proactive safety action taken by the Rail Industry Safety and Standards Board

Action number:	RO-2018-014-PSA-02
Action organisation:	Rail Industry Safety and Standards Board (RISSB)
Action status:	Closed

Although not directly in response to this accident, the Rail Industry Safety and Standards Board (RISSB) has published standards and guidelines since the accident that helped address this safety issue.

In November 2018, RISSB issued Australian Standard AS 7472 (*Railway operations – management of change*) to assist rail transport operators (RTOs) in fulfilling change management responsibilities. The standard included several elements relevant to projects such as the generation 3 remote control equipment (RCE) project, including:

- definition of 'change' was given as: 'the process of causing a function, practice, system, asset or object to become different somehow to what is at present…' and '…includes anything that has the potential to alter existing risks or introduce new hazards'
- engagement of sufficient expertise on the change management team, for example, engineering, safety and technical specialists
- requirement to review the impact of the change on the RTO's accreditation, including conditions and restrictions
- review and where required amendment of SMS documentation (for example, manuals, procedures and designs)
- application of relevant standards and codes of practice to the change, or recognition a new standard may need to be developed
- consideration of impacts to engineering and operational interfaces (including human factors)
- independent validation of the change where safety impact was determined as significant
- obtainment of appropriate internal and external approvals
- identification and rectification of emerging issues during implementation
- documentation of changes during the implementation period and reassessment of risks
- post-implementation review of the change including effectiveness of the process and emergence or change to risks.

In January 2019, RISSB issued the *Rolling Stock Safety Assessment* guideline as 'an aid to rail industry describing common practice for the safety assessment of rolling stock and approvals.' It set guidance for:

- providing rolling stock safety assessment awareness in rolling stock lifecycle
- preparing and undertaking a safety assessment and safety assurance case toward regulatory compliance
- addressing stakeholder responsibilities for safety in the rolling stock lifecycle.

The guideline listed several systems and safety engineering standards, including EN 50126 *Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*, as normative references.

In June 2020, the RISSB-developed AS 7473 (*Complex system integration in railways*) was issued and was freely available to RISSB member organisations. It stated:

> The objective of this Standard is to establish an industry approach for managing:
>
> a. the risks associated with integrating complex systems;
>
> b. the design and implementation of complex system interfaces; and,
>
> c. the planning, conducting and reporting on system integration testing (SIT).
>
> This Standard defines an approach to support the preparation and execution of system integration for rail projects in Australia. It provides processes to support the definition, control and optimization of integration processes used within an organization or project that can be applied by the adopter when delivering railway systems.
>
> This Standard is targeted at railway systems integrators such as operators, delivery authorities, prime contractors and alliances, or other bodies involved in integrating systems for or into a railway environment. Specifically, activities that result in changes or creation of railway configuration or operation.

AS 7473 listed 2 systems and safety standards as normative references: EN 50126 and ISO/IEC 15288 (*Systems and software engineering - System life cycle processes*).

In 2021, RISSB issued standard AS 7474 (*Rail industry – System safety)* to 'provide a clear standard for management of System Safety that addresses Australian legislative requirements and is readily scalable for the scope of rail projects undertaken within Australia.' It stated:

> The System Safety Assurance standard is to provide key requirements for the elimination or minimisation of safety-related risks, so far as is reasonably practicable (SFAIRP) associated with the planning, design, build, installation, testing and commissioning, operation, maintenance and disposal of rail assets including rollingstock, track and supporting infrastructure.

This Standard is intended to provide a scalable set of requirements intended to support designers, manufacturers, transport operators and State entities in demonstrating and assuring that new or modified rail assets are safe in accordance with the Australian legislative framework. The standard provided a brief, accessible overview of the following system safety elements:

- system safety organisation
- system safety lifecycle / framework
- system safety activities
- system safety outcomes.

Proactive safety action taken by the Office of the National Rail Safety Regulator (ONRSR)

Action number:	RO-2018-014-PSA-03
Action organisation:	Office of the National Rail Safety Regulator (ONRSR)
Action status:	Closed

Although not directly in response to this accident, the Office of the National Rail Safety Regulator (ONRSR) has published guidance information since the accident that helped address this safety issue. In March 2019, ONRSR published a safety message titled *Importance of a System Engineering Approach*, which stated:

> Following recent incidents and observations the Office of the National Rail Safety Regulator (ONRSR) is reminding all operators of the importance of a system engineering approach.
>
> With various subsystems - such as track, signalling, rolling stock, electrification, stations, depots, and control centres - closely interlinked, any change in one may affect the operation of another. As such, it is important to carefully consider the interfaces and how the subsystems interact with each other (including how these systems work together with people).
>
> It is essential to understand the hazards when making system changes or introducing new products into a system and the effect such a change will have on the overall risk profile of the railway.

One particular area operators should pay attention to is the acceptance of products or systems based on cross-acceptance. That is, where a product or system is deemed safe because it has been applied safely on another railway or because it is compliant with appropriate standards.

Whilst cross acceptance can be an indication of performance, it cannot be taken as evidence that a product will perform safely in the particular railway system it is introduced to. As part of a robust engineering change process it is, therefore, important to understand the potential hazards a product or system may present in the environment it is introduced to - and the effects it might have on the overall safety risk of the railway.

Operators should demonstrate that they use appropriate systems engineering processes and safety assurance processes (e.g. EN50126/8/9 for complex systems) in their design and procurement approach. This can be achieved through the creation of a systems engineering management plan which specifies the procedures to identify and record stakeholders, system requirements and safety needs.

On 3 August 2020, ONRSR also published 2 related fact sheets:

The *Safety Critical Software Assurance* fact sheet is designed to help rail transport operators ensure their safety management systems address the complexity of software systems along with its compliance and safety risk. It features a series of international lessons learned to illustrate key points.

The *Systems Integration* fact sheet focuses on the importance of a robust approach to systems integration in the context of major projects and other initiatives that are delivering complex and/or multifaceted safety systems. The aim of the resource being to ensure new technologies work together safely with existing railway infrastructure and rolling stock.

Notification of change regulatory requirements and guidance

The guidance provided by the Office of the National Rail Safety Regulator about the requirement to submit a notification of change included limited detail about the extent or type of changes that necessitated a notification. In addition, with regard to 'a safety critical element of rolling stock', it did not provide detail with regard to the interpretation of 'safety critical' and the applicability to equipment that may not be inherently part of rolling stock (such as remote control equipment).

Issue number:	RO-2018-014-SI-11
Issue owner:	Office of the National Rail Safety Regulator (ONRSR)
Transport function:	Rail: Other
Current issue status:	Open – Safety action pending

Proactive safety action taken by the Office of the National Rail Safety Regulator (ONRSR)

Action number:	RO-2018-014-PSA-09
Action organisation:	Office of the National Rail Safety Regulator (ONRSR)
Action status:	Monitor

On 7 October 2022, ONRSR advised that it was 'planning to add additional guidance with regards to safety critical elements when *The ONRSR Way* is next updated (anticipated to be released in 2023).'

ATSB comment

The ATSB anticipates that additional guidance for the criteria for notification of change will help ensure that ONRSR is notified of important safety-related changes, and accordingly will monitor progress on the ONRSR safety action.

Emergency procedures coordination and completion

Safety issue description

TasRail's processes for ensuring immediate network control actions in response to emergencies (such as runaway and authority exceedance) fundamentally relied on the experience and knowledge of network control officers and did not include the provision of procedures, tools and checklists detailed enough to support the effective management of specific types of incidents that require a time-critical response.

Issue number:	RO-2018-014-SI-13
Issue owner:	TasRail
Transport function:	Rail: Operations control
Current issue status:	Closed – Adequately addressed
Issue status justification	The ATSB is satisfied that TasRail's emergency management checklists (for runaway, derailment, and overrun of limits authority) adequately address the safety issue.

Proactive safety action taken by TasRail

Action number:	RO-2018-014-PSA-04
Action organisation:	TasRail
Action status:	Closed

In February 2021, TasRail implemented 3 checklists to assist in ensuring consistent and sound decisions by network control officers during time-critical emergency responses. These were:

- NA-FRM-800 *Network control – rolling stock runaway checklist*
- NA-FRM-801 *Network control – derailment checklist*
- NA-FRM-802 *Network control – overrun of limits of authority checklist.*

Safety action not associated with an identified safety issue

Whether or not the ATSB identifies safety issues in the course of an investigation, relevant organisations may proactively initiate safety action in order to reduce their safety risk. The ATSB has been advised of the following proactive safety action in response to this occurrence.

Additional safety action taken by TasRail

Shortly after the accident, TasRail indicated that it would be reducing the overspeed limit on the TR class locomotive from 88 km/h to 75 km/h. This reflected the maximum track speed on the TasRail network of 70 km/h.

In September 2019 TasRail presented its internal findings and lessons to the rail industry in a forum co-ordinated by the Rail Industry Safety Standards Board (RISSB) titled ‘Lessons Learned from Investigations’.

General details

Occurrence details

Date and time:	21 September 2018 – 0909 EST	
Occurrence class:	Accident	
Occurrence categories:	Runaway, Derailment	
Location:	Devonport, Tasmania	
	Latitude: 41º 10.816' S	Longitude: 146º 21.805' E

Train details

Track operator:	TasRail	
Train operator:	TasRail	
Train number:	604	
Type of operation:	Freight	
Consist:	1 x TR class locomotive, 16 x THFY cement wagons (14 x loaded), 1 x Driver's van DV1	
Departure:	Railton, Tasmania	
Destination:	Devonport, Tasmania	
Persons on board:	Crew – 0	Passengers – n/a
Injuries:	Crew – 0	Public – 2 (minor)
Damage:	Substantial	

Glossary

ACMA	Australian Communications and Media Authority
ADE	Air Digital Engineering
ANCS	Advanced Network Train Control System. The safeworking system used on the TasRail network, which used GPS tracked electronic track warrants and authorities.
AS	Australian Standard
CHU	Cab handle unit. Manipulated by the driver, this sent electronic airbrake requests to the POU to enact.
COMF mode	Communication failed mode. Fault mode of the RCE in which traction power was removed and the train's brakes applied after an interruption of communications between the RCE transmitter and RCE receiver.
CNF mode	Control fault mode. Fault mode of the RCE in which traction power was removed and the train's brakes applied where the RCE receiver or locomotive response did not replicate the driver's RCE transmitter command.
Driver's van	A reclaimed Y-class locomotive with no engine or traction motors, used for the driver to observe the track ahead while propelling the consist with the remotely-controlled locomotive at the rear of the train.
EMV	Emergency magnet valve. Assists in localised rapid brake pipe exhaust in the event an emergency rate reduction of the brake pipe was detected.
Emergency brake	The application of maximum braking effort throughout the train by venting the automatic brake pipe, or in the case of brake pipe rupture.
Emergency stop	A function provided by the RCE to apply emergency braking and command the removal of traction power, among other actions. Emergency stop mode (a software mode) could be driver-initiated, or RCE-initiated (in the event of a fault). Some RCE hardware faults would result in the application of emergency brake only, without the RCE entering emergency stop mode.
Fail-safe	The capability (or design approach intended to provide the capability) of a system such that any failure always results in a safe condition.
FMEA	Failure modes and effects analysis. A systematic approach to document the potential effects of component failures in a system.
LCD	Liquid crystal display. A type of flat panel display.
MR1	Main reservoir no. 1. The locomotives primary store of pressurised air. Fed by the locomotive air compressor and supplying air to all subsequent systems, including main reservoir no. 2 and the main reservoir equalising pipe.
MR2	Main reservoir no.2. A secondary source of air pressure on the locomotive fed by main reservoir no. 1 through a one-way valve, this air was used on a non-remotely-controlled train to recharge the brake pipe, charge the control pipe and brake cylinders.
MREQ	Main reservoir equalising pipe. This allowed a continuous supply of air from main reservoir no. 1. Its intend function was to achieve consistent pressure in the main reservoir no. 1 throughout all locomotives on a train. On an RCE equipped train, this air was also used to recharge the brake pipe and charge the control pipe.

ONRSR	Office of the National Rail Safety Regulator
PCS	Power control switch. Automatically removed traction power and dynamic brake from the locomotive when low brake pipe pressure was detected.
POU	Pneumatic operating unit. Located in the locomotive's engine room, it enacted the air pressure responses for the train's electronic airbrake system.
RCE	Remote control equipment. This consisted of a transmitter (for driver commands), a receiver box, and air box as well as associated multiple unit cable, airbrake hoses and radio antennas.
RISSB	Rail Industry Safety and Standards Board
RSNL	Rail Safety National Law
RTO	Rail transport operator. Encompassed both rail infrastructure managers (track, signalling etc.) and rolling stock operators (locomotives, wagons etc.).
Safe state	A state or mode that a system can enter, usually following a failure, which is associated with an acceptable level of risk.
SAL	System for automated locomotive computer control. A proprietary system in the TR class locomotive that included the capability to monitor and control locomotive traction power, record and indicate faults, and allow diagnostic testing.
Selcall	Selective calling on a radio system, whereby receiving systems would selectively answer a radio transmission based on the sequential audio tone transmitted.
SIL	Safety integrity level. A number from 1 (the lowest) to 4 (the highest) which specified the probability of a system meeting its safety functions under all stated conditions within a stated period of time.
SMS	Safety management system. A systematic approach to organisational safety encompassing safety policy and objectives, risk management, safety assurance, safety promotion, third party interfaces, internal investigation and SMS implementation.
VX vent valve	A valve designed to locally vent the brake pipe on detecting a rapid rate (emergency) of brake pipe descent. Two were fitted to the TR class locomotive.

Sources and submissions

Sources of information

The sources of information during the investigation included:

- TasRail (rolling stock operator and rail infrastructure manager)
- Air Digital Engineering (RCE manufacturer)
- Progress Rail Services (TR class locomotive manufacturer)
- Wabtec Australia (electronic airbrake system and wagon braking system manufacturer)
- the Office of the National Rail Safety Regulator
- Tasmanian Government (Department of State Growth)
- Tasmania Police
- the driver of train no. 604
- network control centre personnel
- members of the generation 3 RCE project team
- accident witnesses
- front-of-train closed-circuit television
- recorded data from the locomotive's 2 recording devices
- rail industry standards, guidelines, codes of practice
- engineering and system safety standards
- legislative instruments
- data and observations from extensive post-accident testing of the train and RCE.

References

Dismukes RK & Berman BA 2010, *Checklists and monitoring in the cockpit: why crucial defences sometimes fail*, National Aeronautics and Space Administration Technical Memorandum NASA/TM-2010-216396.

Dunn WR 2002, *Practical Design of Safety-Critical Computer Systems*. Reliability Press, Solvang.

Ericson CA 2005, *Hazard analysis techniques for system safety*. John Wiley & Sons, New Jersey.

Federal Railroad Administration (FRA) 2005, *Safety of Remote Control Locomotive (RCL) Operations.* Report to Congress, Washington.

Federal Railroad Administration (FRA) 2006a. *A Comparative Risk Assessment of Remote Control Locomotive Operations versus Conventional Yard Switching Operations.* Technical Report DOT/FRA/ORD-06/09, Washington.

Federal Railroad Administration (FRA) 2006b. *Human Factors Root Cause Analysis of Accidents/Incidents Involving Remote Control Locomotive Operations*. Technical report DOT/FRA/ORD-06/05, Washington.

Federal Railroad Administration (FRA) 2006c. *Remote Control Locomotive Operations: Results of Focus Groups with Remote Control Operators in the United States and Canada.* Technical report DOT/FRA/ORD-06/09, Washington.

Hawkins, R, Habli I and Kelly T 2013. The Principles of Software Safety Assurance. In *31st International System Safety Conference*, Boston.

Hawkins RD and Kelly TP 2009. Software Safety Assurance – What Is Sufficient?. In *4th IET International Conference on Systems Safety*, London.

Hawkins RD and Kelly TP 2012. A framework for determining the sufficiency of software safety assurance. In *7th IET International Conference on System Safety*, Edinburgh.

Hobbs C 2020. *Embedded Software Development for Safety-Critical Systems* (2nd ed.). CRC Press, Boca Raton.

Kusumo R (2019) *A systems approach to safe system integration in major rail projects*, paper presented at the Rail Industry Safety and Standards Board (RiSSB) Rail Safety Conference in Melbourne, May 2019.

Leveson NG 2016. *Engineering a Safer World: Systems Thinking Applied to Safety*. The MIT Press, Cambridge, Massachusetts.

Littlewood B and Strigini L 1995. Validation of Ultra-High Dependability for Software-Based Systems. In *Predictably Dependable Computing Systems* (pp. 473-493). Springer, Berlin, Heidelberg.

McInerney, P 2001. *Special Commission of Inquiry Into the Glenbrook Rail Accident – Final Report.*

McInerney, P 2005. *Special commission of inquiry into the Waterfall rail accident – Final Report*.

Ministry of Defence (United Kingdom) 2007. *Safety Management Requirements for Defence Systems*, Defence Standard 00-56.

National Research Council 2007. *Software for Dependable Systems: Sufficient Evidence?*. The National Academies Press, Washington.

Neumann PG 1994, *Computer-related risks*. Addison-Wesley, New York.

Rail Industry Safety and Standards Board (RISSB) 2014, *AS7510.1: Braking systems part 1 – locomotive rolling stock*, RISSB, Spring Hill Queensland Australia

Rail Industry Safety and Standards Board (RISSB) 2015, *AS7527 – Rolling stock event recorders*, RISSB, Spring Hill Queensland Australia

Rail Industry Safety and Standards Board (RISSB) 2015 (2019 amendment), *AS7527 – Rolling stock event recorders*, RISSB, Spring Hill Queensland AustraliaRail Industry Safety and Standards Board (RISSB) 2018, *Code of practice: Distributed power freight trains*, RISSB, Spring Hill Queensland Australia

Smith DJ and Simpson KG 2010. *Safety critical systems handbook: a straight forward guide to functional safety, IEC 61508 (2010 Edition) and related standards, including process IEC 61511 and machinery IEC 62061 and ISO 13849*. Elsevier.

Welschen R, Bellon E, Brown C, Fullalove R, Kennedy G, Irvine K, Mumford N, Nadeem M, Nasr J, Tildesley E, Patel H, and Roodt D (2021), An Overview of Systems Engineering in the Australian Transport Sector. *Systems Engineering News Journal*, March.

Submissions

Under section 26 of the *Transport Safety Investigation Act 2003*, the ATSB may provide a draft report, on a confidential basis, to any person whom the ATSB considers appropriate. That section allows a person receiving a draft report to make submissions to the ATSB about the draft report.

A draft of this report was provided to the following directly involved parties:

- Air Digital Engineering (ADE)
- TasRail
- the Office of the National Rail Safety Regulator (ONRSR)
- the Rail Industry Safety and Standards Board (RISSB)
- the driver of train no. 604
- Wabtec Australia (the train braking system manufacturer).

Submissions were received from:

- Air Digital Engineering (ADE)
- TasRail
- the Office of the National Rail Safety Regulator (ONRSR).

The submissions were reviewed and, where considered appropriate, the text of the report was amended accordingly.

Appendices

Appendix A – Analysis of occurrence event information

Examinations at the accident site

On 25 September 2018, the remote control equipment (RCE) attached to the TR class locomotive TR11 was removed in the presence of the ATSB for removal for storage in a secure location. Prior to removal, a visual inspection was undertaken, with no obvious faults or problems detected.

Following the visual inspection, the air hoses connecting the TR class locomotive to the RCE equipment and aerial connections were progressively removed and insulation resistance tested. This included a standing wave ratio test of the RCE antenna and coaxial cable. This testing also did not identify any obvious faults or problems.

Overview of subsequent examination and testing

During 2 periods in October 2018, preliminary testing of the RCE involved in the accident with both locomotive TR11 and another TR class locomotive was undertaken. This included testing both with the ATSB in attendance and on its behalf. Tests included electronic airbrake transducer calibration and self-test diagnostics. Preliminary RCE fault response testing was also undertaken.

In late October 2018, further locomotive and RCE testing was undertaken by a consultancy firm that was engaged by TasRail to provide an internal report into the accident. The consultancy firm also undertook extensive testing of radio coverage and interference between Devonport and Railton and assessments of cyber security risk.

There was no data recorded that included RCE modes, driver control positions on the RCE transmitter, commands from the transmitter to the receiver, or commands from the receiver to the air box or locomotive. As a result, the ATSB analysis was based on other data recorded on the locomotive throughout the runaway sequence, as well as the driver's recollection.

Available documentary evidence related to the design and operation of the generation 3 RCE was reviewed, including the various modes, configurations and responses described with the RCE operation manual and its interface with the TR class locomotive and electronic airbrake system. The ATSB also carried out extensive interviews with TasRail, Air Digital Engineering (ADE), and the locomotive and braking system manufacturers.

However, the available data was insufficient to completely determine the runaway sequence and important aspects of RCE behaviour so the ATSB determined that further RCE testing was required.

Accordingly, additional testing was undertaken by the ATSB over a 2-day period in February 2020 with the assistance of TasRail. This testing was carried out with the RCE involved in the accident, another TR class locomotive, and a similar train configuration to that of the cement train. TasRail representatives and 2 rail safety officers from the Office of the National Rail Safety Regulator (ONRSR) also attended these tests.

The focus of these tests was software and hardware fault responses and RCE–locomotive–train integration. Part of these tests included fault and integration responses of the TR class locomotive. The testing included multiple onsite tests of the generation 3 RCE, in conjunction with different train consists, to gather information relating to possible failure scenarios and locomotive responses. Simulations reproducing some characteristics of the occurrence sequence were also undertaken, using available driver commands to replicate observed RCE and train behaviour. The testing was facilitated by both TasRail and ADE.

In addition to on-train tests, the RCE was tested separately to the locomotives and train consists in both October 2018 and February 2020, on the test bench at the RCE maintenance contractor's

premises. Part of these tests included software and hardware behaviour, physical inspection of the equipment (including air valves), and a test of the transmitter's battery.

ADE later reported:

> ADE has conducted a hardware & software analysis of its factory test system which is software, electronically and electrically identical to the RCE Gen 3 system on the locomotive at the time of the accident. ADE could not reproduce a condition that led to the events preceding the accident with regard to Brake Pipe changes ... ADE was primarily interested in trying to create and or identify the catalyst which set the [accident] sequence of events in motion [with regard to the rapid reverser movement[94] and potential persistent unsafe state during initialisation[95]].
>
> The testing was limited to putting the software and hardware under stress in as much as possible within the limitation of the equipment not being connected to a locomotive. This involved for periods of time (10 minutes) manually and consistently rapidly transmitting control commands putting the system under executional stress. It also included the consistent rapid changing of the reverser...

The testing concluded that:

- the locomotive, including its control and safety systems, operated as designed
- the locomotive electronic airbrake system operated as designed
- there was no evidence that cyber intrusion occurred.

Analysis of the recorded data for the runaway and derailment is presented below in Table A1, Table A2 and Table A3, with relevant parameters combined from the available data log's presented in Figure A1, Figure A2 and Figure A3.

[94] See *Unintended emergency brake application and release*.
[95] See *Software design*.

Remote control equipment failure

Table A1: Sequence during remote control equipment failure (0841:55 to 0843:55)

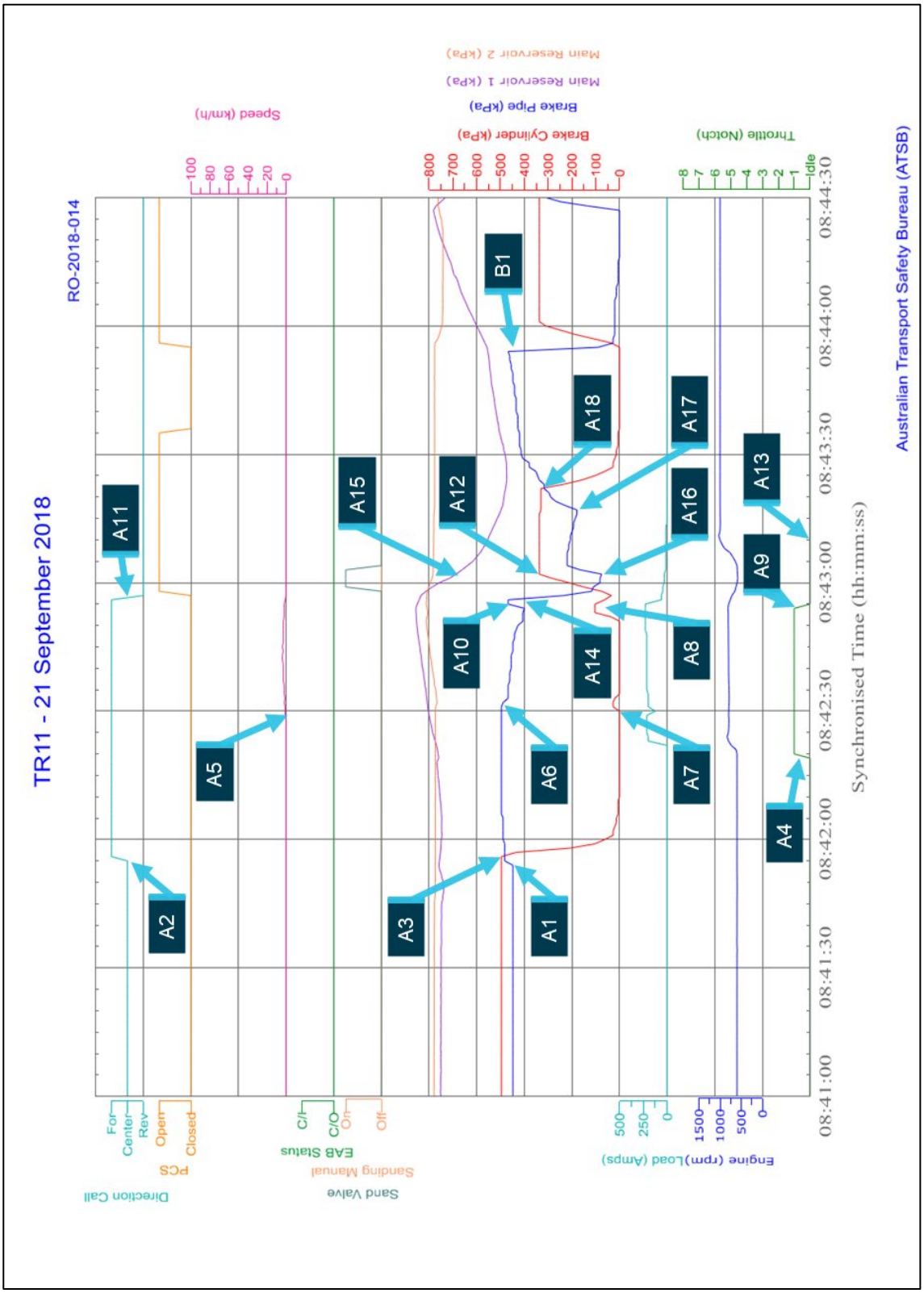
Time	Observation	Analysis
0841:55 to 0842:29	Label A1: brake pipe pressure increased Label A2: direction controller state changed from neutral to forward Label A3: locomotive brake cylinder pressure decreased Label A4: throttle increased Label A5: the train began to move	Responses are consistent with the driver's description that, after completing loading wagons 13 and 14, they moved the train forward to position the last 2 wagons for loading. Automatic and independent brake were released, direction selected, and power applied causing the train to move.
0842:32	Label A6: brake pipe pressure decreased Label A7: locomotive brake cylinder pressure increased momentarily then decreased	Responses are consistent with an automatic (train) brake application, where the locomotive brakes have been 'bailed-off' to prevent them from applying. Although an automatic train brake application was not described by the driver, the use of automatic brake in conjunction with 'bail-off' in this manner is normal to control movement at low speed. Therefore, it is likely that this was requested by the driver.
0842:52	Label A8: locomotive brake cylinder pressure increased, corresponding to a further decrease in brake pipe pressure	The observed behaviour is consistent with further application of the automatic train brake, without a corresponding bail-off command, resulting in the locomotive's brakes applying. The driver observed that the train would, and subsequently did, overshoot the intended stopping point. The driver did not describe requesting an increased brake application. However, increased braking effort is a consistent response when stopping a train.
0842:55	Label A9: throttle reduced to idle Label A10: brake pipe pressure increases	The observed behaviour is consistent with the driver responding to the overshoot and preparing to reverse the train by removing the throttle and releasing the automatic brake.
	Note: The observations and analysis (labels A1 to A10) above indicate that the train was responding to remote control commands, as the driver requested, during this time.	
0842:57	Label A11: direction controller state changed from forward to reverse	The driver recalled requesting the direction to change in preparation to reverse the train. The data was recorded at 1-second intervals and the direction controller state went immediately from forward to reverse without registering in neutral. This indicated that the change of direction request occurred in under 1 second, likely because the driver quickly selected the reverse direction in a straight sweep from forward, without pausing in neutral. This is the last observation consistent with the driver's requested commands.
0842:57	Label A12: locomotive brake cylinder pressure increased to 337 kPa	The driver advised that, in conjunction with the change in direction (label A11) they requested an independent brake application. Although the driver did not specify what level of independent brake application they requested, observation of previous applications during

		loading / unloading operations showed that they almost always resulted in about 500 kPa in the locomotive brake cylinders. The low brake cylinder pressure achieved on this occasion, not exceeding 337 kPa, indicated that it was likely that the RCE did not charge the control pipe in response to the driver's request. The locomotive brake cylinder pressure was the result of low brake pipe pressure only, consistent with an automatic brake application.
0842:57	Label A13: the throttle remained at idle when the direction controller state changed from forward to reverse (label K)	The driver advised that, in conjunction with change of direction (label A11), they requested a throttle application. However, the recorded data does not show a corresponding locomotive response, and the throttle continued to remain at idle through the rest of the sequence.
0842:57	Label A14: at the same time that the direction controller state recorded reverse (label A11), the brake pipe pressure decreased rapidly to about 100 kPa	The brake pipe pressure rapidly decreased to about 100 kPa, consistent with an emergency brake application. It is highly likely that this was the result of a dual direction fault interlock as it occurred in conjunction with the rapid change of direction, which is a known trigger for this response. When this state was detected, the RCE receiver responded by commanding a vent of the brake pipe through its emergency valve, initiating the rapid pressure decrease. The RCE emergency vent valve only remained open momentarily while the fault state was present. The locomotive's VX vent valves and emergency vent valve (EMV) likely responded to the momentary rapid pressure decrease and activated, venting the brake pipe at additional locations separate to the RCE.
0842:58 to 0843:26	Label A15: main reservoir no. 1 pressure decreased while main reservoir no. 2 pressure remained relatively constant	The loss of air pressure from main reservoir no. 1, without corelated loss from main reservoir no. 2, was consistent with an attempt by the RCE to charge the brake pipe.[96] Therefore it is likely that, once the RCE dual direction fault interlock cleared, it attempted to increase the brake pipe pressure in opposition to the locomotive's VX vent valves and EMV, which were both venting the brake pipe air. This resulted in the brake pipe pressure being maintained well below 350 kPa, but above zero (the expected result of an emergency vent).
0843:03	Label A16: brake pipe pressure increased, reaching a maximum of about 220 kPa before slowly decreasing again to about 180 kPa	The increase likely corresponded to the VX vent valves ceasing to vent brake pipe air. (The VX vent valves are self-regulating and cease to vent when a volume of air, called the control pressure volume, has vented.)
0843:18	Label A17: brake pipe pressure again increased	The second increase likely corresponded with the locomotive's EMV closing, consistent with its 20-second timeout after initial activation in response to a rapid brake

[96] The RCE equipment configuration used main reservoir no. 1 air, from the main reservoir equalising pipe (MREQ), to directly supply the brake pipe with pressurised air. The locomotive's brake system used main reservoir no. 2 air (which was itself fed from MR1 through a one-way valve) to do the same (when in command, see *Interface with locomotive*). Therefore, the source of a brake pipe pressure recharge (RCE or locomotive) could be determined based on the recorded behaviour of the main reservoir air pressure. If only main reservoir no. 1 pressure decreased, then the recharge was RCE-initiated, as was the case here.

		pipe pressure loss. This allowed the RCE to recharge the brake pipe without opposition. The maximum brake pipe pressure reached was 468 kPa.
0843:24	Label A18: locomotive brake cylinder pressure decreased as brake pipe pressure rose above about 320 kPa	The brake cylinder pressure did not begin to reduce in response to the initial rise in brake pipe pressure. Instead, it is likely that the brake cylinder pressure release was delayed until brake cylinder and brake pipe pressures had equalised, an action of the locomotive's electronic airbrake system.
	Note: The ATSB observed the behaviour described (labels A14 to A18) to occur repeatably during testing conducted after the runaway. This was triggered when the driver rapidly made a direction change request on the RCE transmitter.	

Figure A1: Combined data logger data during remote control equipment failure (0841:00 to 0844:30)



Source: ATSB

Initial runaway

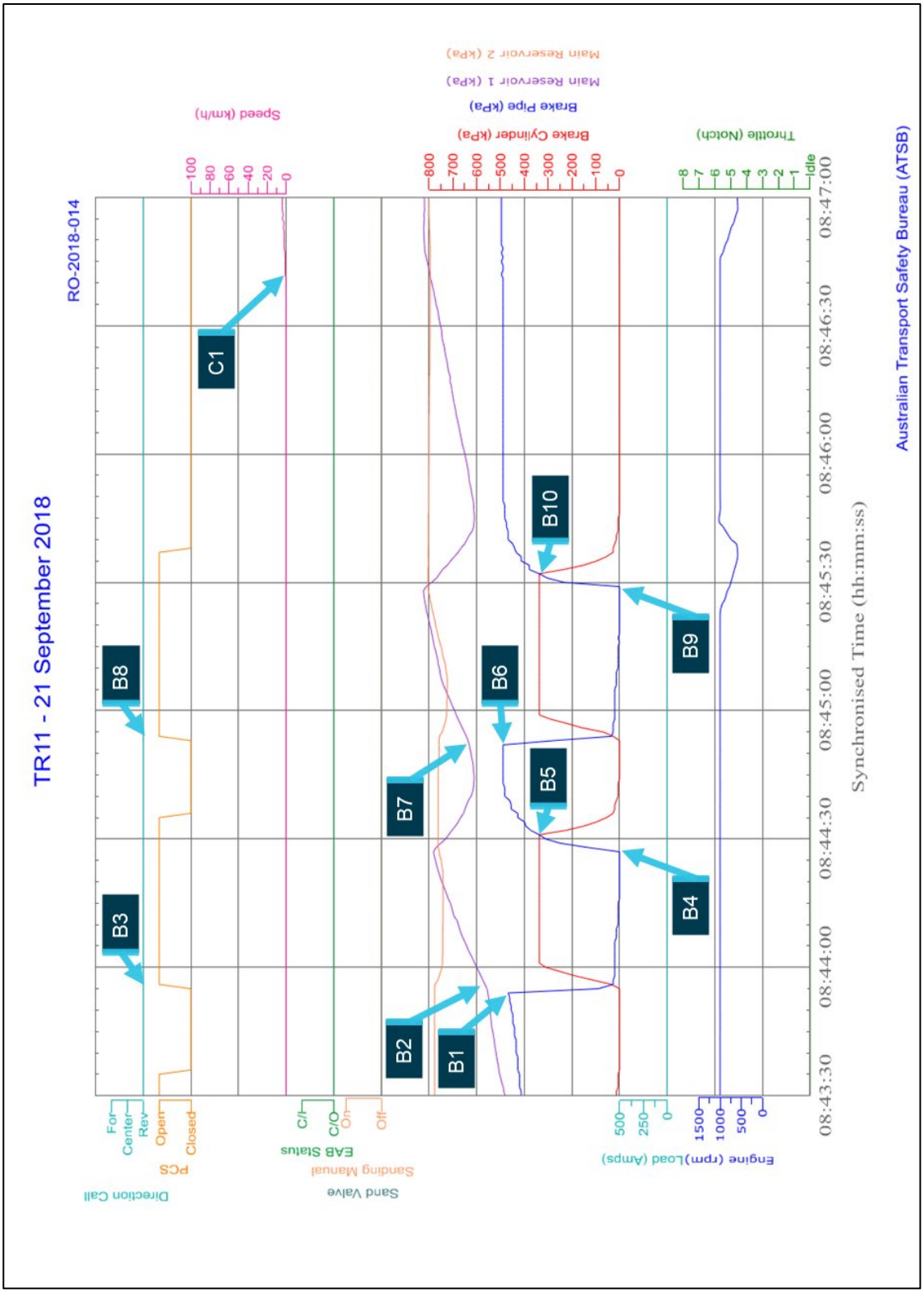
Table A2: Sequence of the initial runaway (0843:55 to 0846:42)

Time	Observation	Analysis
0843:55	Label B1: brake pipe pressure decreased rapidly to about 0 kPa in both Figure A1 and Figure A2 Label B2: main reservoir no. 1 pressure continued to increase Label B3: direction controller state remained in reverse	The brake pipe pressure rapidly decreased to about 0 kPa, similar to an emergency brake application. The locomotive's VX vent valves and EMV likely responded to the momentary rapid pressure decrease and activated, venting the brake pipe at additional locations separate to the RCE. The main reservoir no. 1 pressure did not decrease in response to this emergency vent. This indicated that, unlike the prior vent, the RCE did not attempt to recharge the brake pipe while the locomotive valves were open. Therefore, it is likely that the RCE initiated and maintained the emergency brake application. The direction controller state was maintained in 'reverse'. This behaviour was not consistent with the RCE's emergency mode or any other documented RCE fault condition.
0844:28	Label B4: brake pipe pressure increased rapidly from 0 kPa to above 480 kPa	The rapid rise of brake pipe pressure observed was consistent with the RCE air box supplying air to the brake pipe at the rear of the locomotive. Because the location of the pressure sensor was in front of the air supply, it was not a true measure of the brake pipe pressure throughout the train and instead increased more rapidly than was normal for a train of 220 m length. No reason could be determined for the RCE to initiate a recharge of the brake pipe at this time. The recharge resulted in a maximum brake pipe pressure of 489 kPa and no pressure in the locomotive brake cylinders. The rise in brake pipe pressure would have provided a release command to the brakes on the wagons (an automatic brake release command).
0844:32	Label B5: locomotive brake cylinder pressure decreased as brake pipe pressure rose above about 320 kPa	The brake cylinder pressure did not begin to reduce in response to the initial rise in brake pipe pressure. Instead, it is likely that the brake cylinder pressure release was delayed until brake cylinder and brake pipe pressures had equalised, an action of the locomotives electronic airbrake system.
0844:53 to 0845:33	Label B6: brake pipe pressure decreased rapidly to about 0 kPa Label B7: main reservoir no. 1 pressure continued to increase Label B8: direction controller state remained in reverse Label B9: locomotive brake pipe pressure increased rapidly from 0 kPa Label B10: locomotive brake cylinder pressure decreased as brake pipe pressure rose above about 320 kPa	The sequence of the third emergency brake application repeated the second emergency brake application (labels B1 to B5 above). ATSB analysis indicated: • The behaviour was not consistent with the RCE's emergency mode or any other documented RCE fault condition. • No reason could be determined for the RCE to initiate a recharge of the brake pipe. The brake pipe pressure recharged to 489 kPa. • The train was left with no brake applications commanded once the brake pipe pressure recharged, though effective release of the wagon brakes would have taken some time.

	Note: The condition observed at the end of the second and third emergency brake applications, with the brake pipe pressure at or near the release level, no brake cylinder pressure and with the direction controller state not in 'centre', was not consistent with any RCE penalty mode or the configuration of the controller required to recover from a penalty mode (the 'start position'[97]). The driver reported that, during this time, they: • believed that the RCE was in a communication failed mode • had configured the transmitter in the start position • attempted to reset the transmitter to re-establish a communication link with the receiver. The recorded information does not show evidence that the communication failed mode or the driver's commands were actioned by the RCE receiver or enacted by the locomotive.	
0846:42	Label C1: the train's speed began to increase, observable in both Figure A2 and Figure A3	With the brakes released, the train began to roll on the downhill grade toward Devonport.
Note: The ATSB conducted testing on a similar train consist to the cement train to examine the behaviour of the wagon brakes in response to the brake pipe behaviour recorded at the locomotive. The results of these tests showed that: • After the third emergency brake application the wagon brake system had sufficient air remaining to apply if commanded (that is, the train's brake system had not run out of air). This was determined by observation of the auxiliary reservoir pressure in wagons throughout the train, which showed sufficient pressure remained (wagons 1, 8 and 16 did not fall below 300 kPa, 280 kPa and 275 kPa, respectively) to apply the wagon brake cylinders to an effective level. • Wagon brake cylinders similar to those fitted to the cement wagons took over 80 seconds to fully release from about 300 kPa. Wagons to the rear of the train (being farther from the source of the brake pipe recharge) took longer than the front wagons to release. This was consistent with the delay of 72 seconds observed from the final release command to the train beginning to roll away.		

[97] Start position: a configuration in which the RCE transmitter controls were conditioned for a 'warm reset' (that is, direction in neutral, throttle idle, independent brake fully applied, automatic brake in at least the 'initial' position).

Figure A2: Combined data logger data during initial runaway (0843:30 to 0847:00)



Source: ATSB

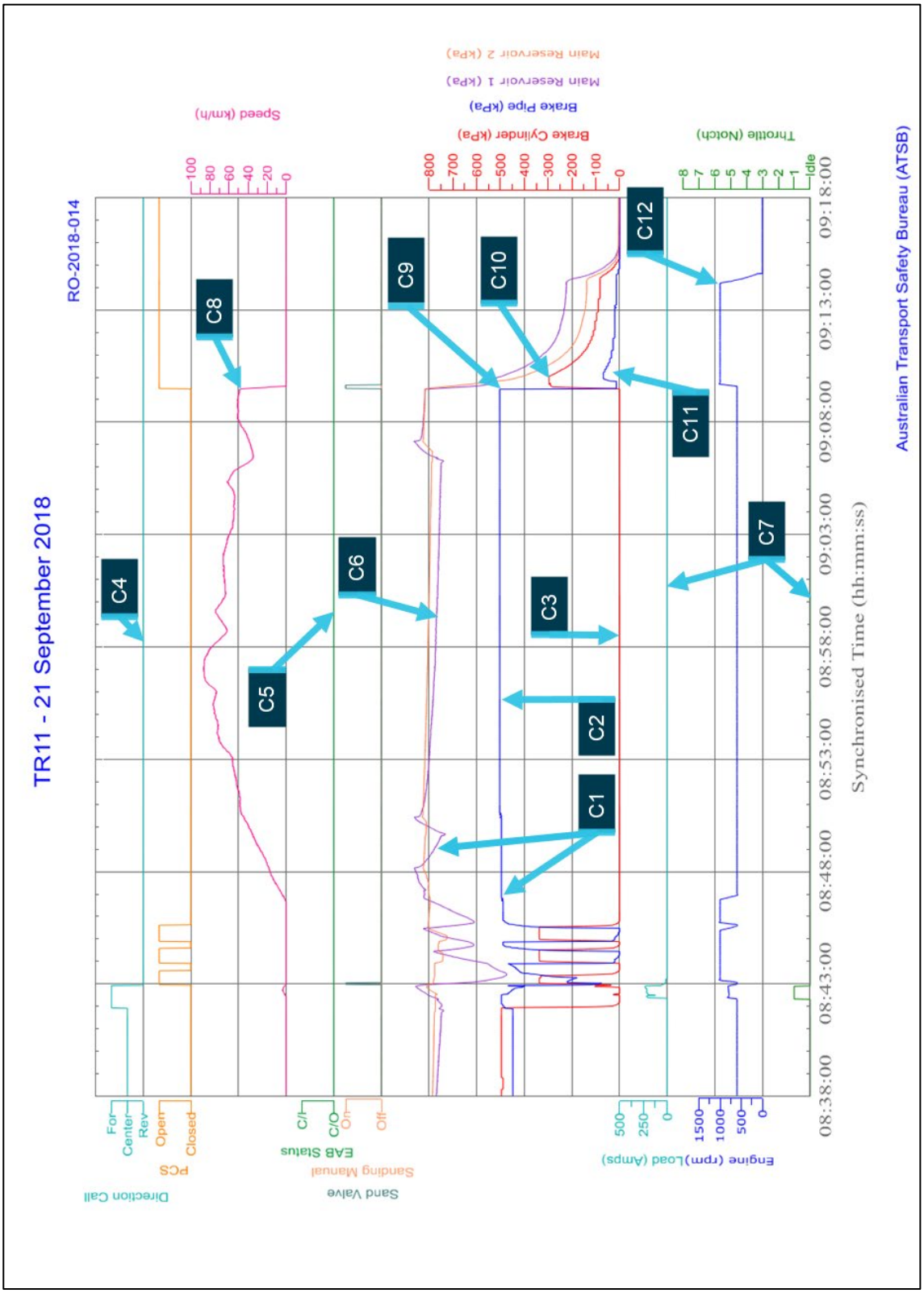
Continued runaway and derailment

Table A3: Sequence of continued runaway and derailment (0846:42 to 0914:24)

Time	Observation	Analysis
	The following observations (labels C1 to C7) occurred while the train was in motion during the runaway.	
–	Label C1: main reservoir no. 1 pressure decreased and then increased coincident with a gradual increase in brake pipe pressure from 489 kPa to 501 kPa	These observations together were consistent with the cement train wagon auxiliary reservoirs continuing to recharge from the brake pipe. Similar main reservoir no. 1 pressure behaviour was observed to occur after the third emergency brake cycle during ATSB simulations of the sequence and did not relate to any apply or release of train brakes.
0846:42 to 0909:29	Label C2: brake pipe pressure remained at the release level Label C3: no locomotive brake cylinder pressure was applied Label C4: direction controller state remained in reverse	The observations are not consistent with the expected configuration in the communication failed mode. Therefore, although the driver reported observing that the transmitter was not linked to the receiver, and the receiver (on the train) exited radio range with the transmitter (being held by the driver at Railton), this did not result in the RCE entering the communication failed mode. The reason that the RCE failed to enter this mode could not be determined.
0846:42 to 0909:29	Label C5: The electronic airbrake status (EAB status) remained cut-out (C/O) throughout the event sequence Label C6: main reservoir no. 1 pressure remained relatively constant with no large decreases	The configuration of the locomotive braking system (trail cut-out) and the behaviour of main reservoir no.1 indicated that the RCE receiver remained in control of the train's brake systems during the runaway. During this time, the RCE did not command brake application and there was no indication that it prevented any external brake application (for example, by the locomotive). That the locomotive remained in the 'trail cut-out' configuration (being controlled by the RCE) was supported by other parameters not being active; the equalising reservoir pressure and brake pipe charging flow (not shown). These parameters are only active when the locomotive is configured in 'lead cut-in', which was not the case.
0846:42 to 0909:29	Label C7: the throttle position remained in idle and no traction motor power (load) was recorded	The locomotive was not under traction power during the runaway and moved solely under the force of gravity on the downhill grade to Devonport.
0909:29	Label C8: train speed rapidly decreased to 0 km/h Label C9: brake pipe pressure rapidly decreased Label C10: locomotive brake cylinder pressure initially increased, then gradually decreased	The sudden stop occurred when the train derailed at Devonport. The brake pipe and brake cylinder behaviour were consistent with damage caused by the derailment. The brake pipe was likely damaged, causing it to rapidly leak, and the brake cylinders were likely also damaged as they initially applied but were unable to retain pressure. The locomotive's VX vent valves and EMV would have responded to the rapid leak of

		brake pipe pressure and activated, venting the brake pipe at additional locations separate to both the leak and the RCE.
0909:49	Label C11: the brake pipe pressure remained above 0 kPa and increased to about 68 kPa after the derailment	The brake pipe pressure did not reach 0 kPa even though it vented. Instead, it increased to 68 kPa after about 20 seconds, consistent with the EMV closing after timeout (the VX vent valves having already done so). This created more obstruction to brake pipe venting. That the pressure rose at this time indicated that the brake pipe was still being supplied with pressurised air. While it is more likely than not that the RCE was supplying air from main reservoir no. 1 in an attempt to recharge the brake pipe to the desired level, this was not visible within the recorded data as, unlike on previous occasions, both main reservoir no. 1 and main reservoir no. 2 air pressure were decreasing.
0914:24	Label C12: locomotive engine RPM decreases to zero	The locomotive's engine stopped, corresponding to an emergency shutdown of the TR class locomotive by emergency services at this time. This in turn caused the locomotive's compressor to stop, and remaining air pressure could no longer be maintained.

Figure A3: Combined data logger data during continued runaway and derailment (0838 to 0918)



Source: ATSB

Summary observations regarding occurrence sequence

Based on the available evidence, the ATSB observed that the following occurred during the occurrence sequence:

- The RCE became unresponsive to driver commands at the point of, or soon after, a fast direction change from forward to reverse.
- The RCE initiated a momentary emergency vent of the brake pipe, likely due to a momentary dual direction fault being detected. The emergency vent resulted in the locomotive's VX valve and EMV activating to exhaust the brake pipe further, which the RCE tried to oppose after the fault state cleared by supplying pressurised air from main reservoir no. 1 to the brake pipe.
- The RCE triggered 2 further emergency brake applications and releases.
- The RCE ultimately entered an unsafe state with the brakes on the train and locomotive fully released, allowing the train to roll away on the downhill grade towards Devonport.
- The RCE did not command a communication failed mode and apply the train's automatic brake, either when either the transmitter and receiver were unlinked, or once the receiver was out of radio range of the transmitter.
- The emergency brake applications and releases, and subsequent state with brakes released without a radio link, were not consistent with any documented fault condition behaviour.
- The RCE remained in an unsafe state, which caused the brakes on the train and locomotive to be maintained in a fully-released condition until the train's brake pipe was ruptured in the derailment.

Appendix B – Safety engineering concepts

Systems engineering

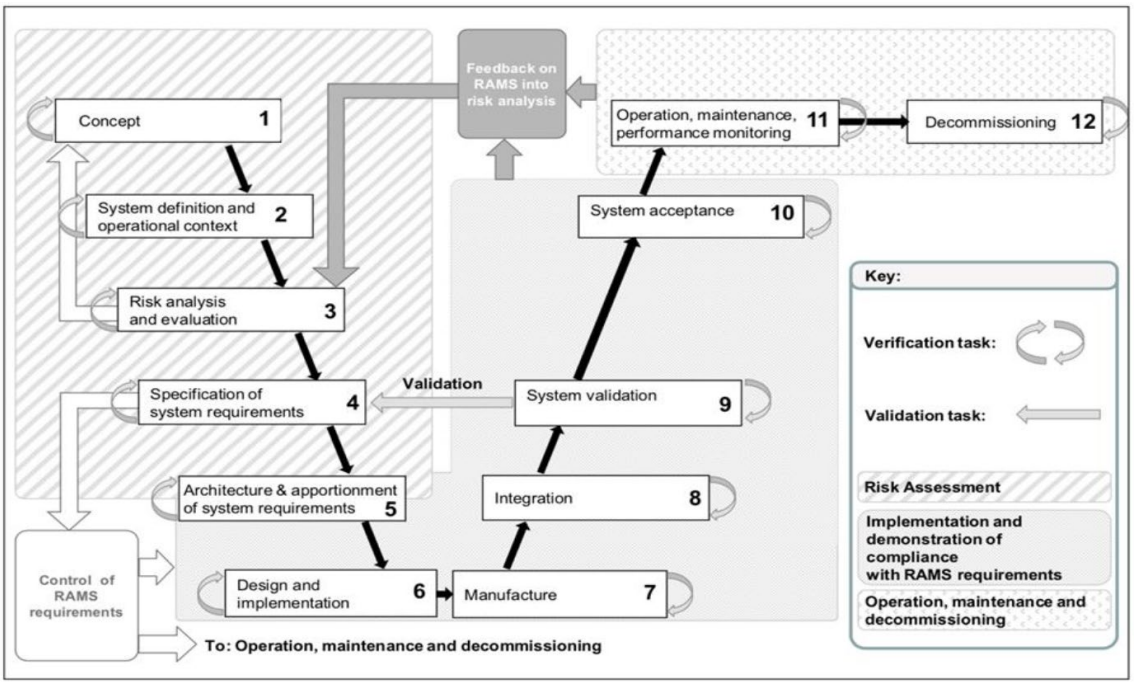
Systems engineering is a way to manage complexity in the development of a product or engineered system. It is a concept that began to form in the 1940s and was later given impetus by the United States National Aeronautics and Space Administration (NASA) as well as the United States military as a way to manage system complexity through control of the development process (Leveson, 2016). The process can be applied to the development of any product.

Leveson (2016) stated:

> Combining a systems-theoretic[98] approach to safety with system engineering processes will allow designing safety into the system as it is being developed or reengineered….A systems engineering approach to safety starts with the basic assumption that some properties of systems, in this case safety, can only be treated adequately in the context of the social and technical system as a whole.

The V-model (or vee model) is commonly used to describe the systems engineering process (for example, see Figure B1). In this model, the product's user defines a concept of operations or broad set of requirements that describe what the product should do. This description is broken down into a progression of increasingly detailed sets of sub-requirements. The higher-level requirements describe all aspects of what a product should do and how well it should do them, and the lower-level requirements describe the product's architecture and other detailed elements of design. The requirements drive the design; that is, design elements are chosen based on the best way to meet the requirements. The developers also need to devise ways to prove that the requirements have been met, which forces them to make the requirements verifiable. Safety can be, and often is, among the design objectives.

Figure B1: Systems engineering lifecycle V-model



Source: Systems Safety Assurance Guideline – RISSB, 18 September 2018

[98] A 'systems theory' of safety treats safety as a emergent property of interactions between system components and the environment, allowing it to be controlled by imposing constraints on the interactions (Leveson 2016).

Throughout this process, the user needs to be involved to help make the right choices. For example, if a particular requirement cannot be met, or if there are conflicting requirements, the user can decide which path to take based on what is most important.

Designing in this way has many benefits. It helps ensure that the various project goals are well-defined, leaving no important requirement undocumented. This in turn allows important choices to be made about the design early in the process, reducing later rework or undesirable product characteristics.

Once a design is finalised, the design and product passes through increasingly broader sets of verification and validation activities (such as testing) to show that the design does meet the requirements. Verification is the process of showing the final product meets the requirements (that is, the product was built correctly). Validation is the process of showing that the requirements met the user's needs (that is, the right product was built). If the requirements definition and design process were conducted well, there should be few or no 'unpleasant surprises' throughout the verification and validation process.

System integration refers to the progressive assembly of subsystems so that the broader system, as an integrated whole, is able to deliver the overarching functionality. A key component of system integration is defining system interfaces and assessing identified hazards associated with those interfaces. More specifically, as stated by Kusumo (2019):

> To ensure safe integration, the SRS [system requirements specification] for a system needs to consider the interface requirements between it and any subsystems and between it and any existing or legacy systems. In addition, these interface requirements for the new system need to include any Safety Related Application Conditions (SRACs) on the existing railway systems that will impact the new system…
>
> A system approach to designing railway systems that will ensure safe system integration involves a systematic analysis of the following:
>
> - Interface compatibility between connected railways systems (data, power and signal, etc.);
> - Risks associated with failures of interface between interconnected systems;
> - Risks of system failure which may compromise the overall safety of the railway operations;
> - Compliance with …SRACs from any existing or legacy systems; and
> - Verification that the identified risk controls have been incorporated in the system design.

Ultimately, the systems engineering process gives the user confidence that, firstly, their needs are well-defined, and secondly, that the product meets them. This is done through, as RISSB states, systematic, methodical, complete, and coherent methods and outcomes. These cannot be achieved without a detailed set of documents that record the process throughout.

Relevant systems engineering standards include:

- ISO/IEC/IEEE 15288 *Systems and software engineering - System life cycle processes*
- ISO/IEC/IEEE 24748 *Systems and software engineering - Life cycle management.*

System safety engineering

System safety engineering can be viewed as the application of systems engineering principles for the purposes of safety assurance (Leveson 2016). It is seen as a more technical process than developing and applying safety management systems but has many principles in common. As with safety management systems or systems engineering, this element can be implemented using a very wide range of different methodologies depending on many factors such as the activity type, organisation size and structure, and external interfaces.

There are numerous system safety methodologies published in Australian and international standards, guidelines, codes of practice, and the like, each with different scope, aims, approaches

and/or applications. Further, there is always overlap between them and with other SMS elements such as risk management.

The amount of detail in these standards and guidelines can range from general process-related information (such as how projects can be managed, types of assurance activities, and how these tie into other activities and the system life-cycle) to technical guidance on choosing and performing specific analysis methods (such as failure modes and effects analysis or functional hazard assessment) and numeric methods to estimate the reliability of safety functions.

Safety engineering is often split into 3 parts: system-level, hardware, and software safety engineering. Sometimes, the concept of 'functional safety' is applied, whereby 'safety functions' that address specific hazards are assigned; it is the reliance on active technical measures to address risk (as opposed to passive methods of addressing risk). 'Safety integrity' is a closely related concept, used as a measure of the reliability of safety functions.

Relevant system safety engineering standards include:

- IEC/AS 61508 *Functional safety of electrical/electronic/programmable electronic safety-related systems*
- EN 50126 *Railway Applications – the Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*
- EN 50128 *Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems*
- MIL-STD-882 *Department of Defense Standard Practice: System Safety*.

Software safety

Since software fails differently to hardware, many standards (including AS 61508 and EN 50128) provide specialised methods to make software both reliable and safe. The *Safety Critical Systems Handbook* (Smith and Simpson 2010) recommended that the software safety requirements should include a range of considerations including response times, equipment and operator interfaces, functions which force a safe state, and data corruption, under all modes of operation.

Software errors are not the only reasons software can behave in an unsafe way. Leveson (2011) asserts that:

> Nearly all the serious accidents in which software has been involved in the past twenty years can be traced to requirements flaws, not coding errors. The requirements may reflect incomplete or wrong assumptions.

Leveson adds that software may be highly reliable and correct and still be unsafe when viewed from a system perspective, when the system is derived from incomplete requirements, or when it has unintended and unsafe behaviour beyond what is specified in the requirements.

Standards selection and tailoring

Organisations should select standards appropriate to their purpose. For instance, a rail organisation would benefit from using a standard that is developed and endorsed by the rail industry as it is most likely to be a good fit from the outset, and standards sometimes have illustrative examples that are specific to the industry. A small organisation does not have the resources to apply the same level of rigour as a large organisation normally can, and any safety assurance processes would have to be simpler.

An organisation would normally select a methodology that most closely aligns with its functions and structure; this helps maximise the organisational depth of understanding of the methodology, which is critical for its application to be effective.

Having chosen a standard or methodology, it is important for an organisation to understand and define exactly how things will be done in its particular context. The concept of adapting a standard

to a particular application is known as ‘tailoring’. The organisation can also adapt its own processes to more effectively align with the chosen methodology.

Some standards provide guidance about how they can be tailored to different applications, often based on enterprise size and complexity.

Moore (2010) advised organisations to:

- start small, selecting processes that are coherent, cohesive, widely applicable and capable of adaptation
- start simple, selecting a standard that provides varying levels of detail that can be adapted to the situation and with information on where to get more detail
- choose standards that provide performance criteria that can be easily understood, and to enable a claim of full or tailored conformance
- choose standards that support adding processes, detail, and capability without causing incompatibility.

Relevant standards

Australian Standard 61508

Australian Standard (AS) 61508 is a functional safety standard that provides suppliers of components and subsystems with complete life-cycle processes to optimise system safety through risk- and performance-based measures. It provides a systematic analysis technique to identify hazards and numerically estimate safety integrity, allowing for the capability of a design to detect faults and any limitations in that capability. A system must meet separate requirements for system and hardware integrity to achieve a given safety integrity level.

The base standard (IEC[99] 61508, which is identical) was first published in December 1997 and then adopted as an Australian standard in August 1999.

Under AS 61508, safety requirements are divided into safety functions (functions that defend against hazards) and safety integrity (probabilities of safety functions being successful over time). The safety lifecycles for hardware and software are treated separately but both similarly require:

- a safety requirements specification
- safety validation planning
- design and development processes
- integration
- operation and maintenance procedures
- safety validation
- modification, and
- verification.

The standard has numerous documentation requirements to support these activities. The standard also lists several dozen ‘recommended’ and ‘highly recommended’ practices to be implemented depending on the product’s intended SIL.

European standard 50126

A European standard issued by CENELEC (the European Committee for Electrotechnical Standardization), EN 50126 *Railway Applications – the Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)* provides processes to assure systems-level engineering integrity through 4 overlapping lenses: reliability, availability, maintenance, and

[99] IEC: International Electrotechnical Commission, an organisation for the preparation and publication of international standards for all electrical, electronic and related technologies.

safety. It states that it is applicable to all fields within rail (command, control and signalling, rolling stock, and fixed installations) independent of the actual technology of the systems and subsystems. It can apply to new systems, new systems integrated into existing systems, and to some extent, modifications of existing systems.

It comprises 3 volumes:

- the generic process,
- system approach to safety,
- system approach to reliability, availability, and maintainability.

The first volume provides a generic safety management process that is supported by guidance and methods within the other volumes.

The second volume provides guidance and methods for the following areas:

- safety process
- safety demonstration and acceptance
- organisation and independence of roles
- risk assessment
- specification of safety requirements
- apportionment of functional safety requirements (this means finding ways to fulfil the requirements)
- design and implementation.

This standard has normative references to related standards such as EN 50128 and EN 50129, discussed below.

EN 50126 has been adopted as a national standard in several countries. An identical standard, IEC 62278, was first published in 2002.

European standard 50128

EN 50128 *Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems* is a functional safety standard that applies to rail products. It specifies the process and technical requirements for the development of software for use in railway control and protection applications. IEC 62279 is identical.

European standard 50129

EN 50129 *Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling* describes how to show that equipment with the potential to affect safety can be relied on for its functions that relate to safety (that is, how to develop a ‘safety case’). The standard is primarily applicable to railway signalling applications but states that it can also be applied to general-purpose or industrial equipment that is part of a safety-related electronic system. IEC 62425 is identical.

European standard 50657

EN 50657 *Railways applications - Rolling stock applications - Software on board rolling stock* specifies a process and technical requirements, adapted from EN 50128, for the development of software in rolling stock applications.

Appendix C – Rail Safety National Law National Regulations 2012 (NSW), Regulation 9(1)(a)

9 Prescribed conditions and restrictions

(1) For the purposes of section 67(2)(a) (*Determination of application*) of the Law, any accreditation granted to a rail transport operator is subject to the following conditions and restrictions:

(a) the operator must notify the Regulator in writing of any of the proposed decisions, proposed events or changes listed in column 2 of the table in accordance with the requirement specified in column 3 of the table with respect to that item:

Table

Item	Decision, event or change	When notification must be given
1	A decision to design or construct, or to commission the design or construction of, rolling stock or new railway tracks.	As soon as is reasonably practicable after the decision is made.
2	The introduction into service of rolling stock of a type not previously operated by the operator, or the re-introduction into service of rolling stock not currently operated by the operator.	At least 28 days before the date the operator intends to introduce or re-introduce the rolling stock into service.
3	A change to a safety critical element of existing rolling stock.	At least 28 days before the date the operator intends to bring the change into operation.
4	A change to 1 or more of the classes of rail infrastructure used in the operator's railway operations.	At least 28 days before the date the operator intends to introduce the new class of rail infrastructure into service.
5	A change to a safety standard for the design of rail infrastructure or rolling stock.	At least 28 days before the date the operator intends to adopt the change.
6	The decision to adopt a new safety standard for the design of rail infrastructure or rolling stock.	At least 28 days before the date the operator intends to adopt the new standard.
7	A change to the frequency of, or procedures for, the inspection or maintenance of railway infrastructure or rolling stock.	At least 28 days before the date the operator intends to bring the change into effect.
8	A change to the network rules relating to the conduct of the operator's railway operations.	In accordance with the provisions of Part 4 Division 4 of the Regulations.
9	A decision to introduce a new network rule relating to the conduct of the operator's railway operations.	In accordance with the provisions of Part 4 Division 4 of the Regulations.
10	A decision to change any work scheduling practices and procedures set out in the operator's fatigue risk management program.	At least 28 days before the date the operator intends to bring the change into effect.
11	The replacement, or a change in the contact details of any person appointed under regulation 8(b).	As soon as is reasonably practicable after it is known the replacement or change will occur.
12	A change in the operator's name or residential address, or the operator's business or trading name, or in the case of a body corporate, a change in the name or registered business address of the body corporate.	As soon as is reasonably practicable after the change is made.

Appendix D – Review of relevant Australian Standard 7527 event recording requirements

AS 7527 (*Rolling stock event recorders*) 'describes the requirements for event recorders installed in locomotive… rolling stock vehicles'. The standard specified what information was required to be recorded in order to achieve compliance with the standard. The table below provides a review of parameters that were identified as relevant to the 21 September 2018 runaway accident, the requirements detailed in AS 7527, and comment on their application to remote control equipment (RCE) operations.

Event recorder parameter	AS 7527 requirement	ATSB comment regarding application to TasRail cement trains
Vehicle speed, as displayed to the driver	Mandatory	Vehicle speed was recorded at the locomotive. However, this was not always the speed displayed to the driver (when in the driver's van or operating external to the train).
Position of the throttle or master controller	Mandatory	Throttle response was recorded at the locomotive. The position of the throttle lever was not recorded. The standard contained a further requirement for 'locomotive distributed power or passenger units operating in multiple' that the throttle position recorded be the position on the 'driven locomotive or cab'. While not specifically considering RCE, it did imply that the position recorded was to be that which the driver was directly controlling. When under remote control, this was the position on the RCE transmitter which was not recorded.
Direction of train travel as selected by the driver	Mandatory	Direction of travel was recorded at the locomotive. However, the recorded position was not the position on the RCE transmitter 'as selected by the driver'.
Brake activation level and duration on the leading driving vehicle	Mandatory	Brake pipe and brake cylinder pressure were recorded on the locomotive. However, the recording could not discriminate whether the RCE receiver and air box or the locomotive airbrake system activating the braking system.
Separately record the operation / application of each braking system fitted to the vehicle	Mandatory	When the locomotive was under conventional (non-remote) control, the position of the (automatic) brake handle was recorded. Correlation between this and the brake pressures (pipe and cylinder) permitted a level of determination regarding which system was responsible for a brake application. When operated by remote control, the position of the automatic brake lever on the RCE transmitter was not recorded. Therefore, when operated by remote control, there was no indication of which system was applying the brakes, other than through inference from brake pressure response (pipe and cylinder).
Operational status (active / inactive) of fitted 'deadman' devices	Mandatory	Operational status of the tilt function fitted to the RCE transmitter was not recorded.
Operational status of the vigilance system (on / off / isolated)	Mandatory	The operational status of the locomotive vigilance system was recorded when the locomotive was under conventional control. When under remote control, a vigilance function on the RCE transmitter was active instead, the operational status of which was not recorded.
Driver acknowledgement of vigilance system alarms	Mandatory	Driver acknowledgement of the locomotive vigilance system was recorded when the locomotive was under conventional control. When under remote control, a vigilance function on

		the RCE transmitter was active instead, driver acknowledgement of which was not recorded.
All penalty applications of the vigilance system	Mandatory	Penalty applications of the locomotive vigilance function were recorded when the locomotive was under conventional control. When under remote control, a vigilance function on the RCE transmitter was active instead, penalty applications of which were not recorded.
All changes to the operational status of the vehicle (e.g. unmanned automatic / manned automatic / manual)	Mandatory	The operational status was not recorded, other than through inference from other parameters. For instance, if the train was operating while the locomotive was configured in trail cut-out then it was likely under remote control.
All control messages received and transmitted by the vehicle	Mandatory	Control messages received and transmitted between the locomotive, RCE receiver and RCE transmitter were not recorded.
All status messages received and transmitted by the vehicle	Recommended	The status of the RCE receiver and RCE transmitter were not recorded
Main reservoir air pressure, as displayed to the driver	Recommended	Main reservoir air pressure (numbers 1 and 2) were recorded at the locomotive. However, when positioned in the driver's van, or operating external to the train, the driver did not have these pressures displayed.

Australian Transport Safety Bureau

About the ATSB

The ATSB is an independent Commonwealth Government statutory agency. It is governed by a Commission and is entirely separate from transport regulators, policy makers and service providers.

The ATSB's purpose is to improve the safety of, and public confidence in, aviation, rail and marine transport through:

- independent investigation of transport accidents and other safety occurrences
- safety data recording, analysis and research
- fostering safety awareness, knowledge and action.

The ATSB is responsible for investigating accidents and other transport safety matters involving civil aviation, marine and rail operations in Australia, as well as participating in overseas investigations involving Australian-registered aircraft and ships. It prioritises investigations that have the potential to deliver the greatest public benefit through improvements to transport safety.

The ATSB performs its functions in accordance with the provisions of the *Transport Safety Investigation Act 2003* and Regulations and where applicable, international agreements.

Purpose of safety investigations

The objective of a safety investigation is to enhance transport safety. This is done through:

- identifying safety issues and facilitating safety action to address those issues
- providing information about occurrences and their associated safety factors to facilitate learning within the transport industry.

It is not a function of the ATSB to apportion blame or provide a means for determining liability. At the same time, an investigation report must include factual material of sufficient weight to support the analysis and findings. At all times the ATSB endeavours to balance the use of material that could imply adverse comment with the need to properly explain what happened, and why, in a fair and unbiased manner. The ATSB does not investigate for the purpose of taking administrative, regulatory or criminal action.

Terminology

An explanation of terminology used in ATSB investigation reports is available on the ATSB website. This includes terms such as occurrence, contributing factor other factor that increased risk, and safety issue.