Rail Accident Investigation Branch

Rail Accident Report

Runaway and collision of a road-rail vehicle near Raigmore, Inverness
20 July 2010

Department for Transport

Report 10/2011
July 2011

This investigation was carried out in accordance with:

- the Railway Safety Directive 2004/49/EC;
- the Railways and Transport Safety Act 2003; and
- the Railways (Accident Investigation and Reporting) Regulations 2005.

Any enquiries about this publication should be sent to:

RAIB	Email: enquiries@raib.gov.uk
The Wharf	Telephone: 01332 253300
Stores Road	Fax: 01332 253301
Derby UK	Website: www.raib.gov.uk
DE21 4BA	

This report is published by the Rail Accident Investigation Branch, Department for Transport.

Runaway and collision of a road-rail vehicle near Raigmore, Inverness, 20 July 2010

Summary

At about 23:39 hrs on 20 July 2010, a machine operator was placing a road-rail excavator onto the railway near Drumrosach farm, near Raigmore, Inverness. As the machine was being placed on the track it began to run down the gradient. The people who were in attendance were unable to stop the machine before it gathered speed.

The machine ran for 0.88 miles (1.41 km) with the machine operator on board, and then collided, at between 40 and 50 mph (64 to 80 km/h), with the rear of a stationary freight train which was standing on the bridge over the line that runs between Inverness and Aberdeen.

In the collision, the machine operator was thrown out of the cab and landed on top of the rear wagon of the freight train, sustaining serious injuries. The excavator was derailed by all wheels and the leading axle of the rear wagon became derailed. Both the excavator and the freight wagon sustained damage.

The RAIB's investigation identified that the excavator was placed into an unbraked condition while being manoeuvred onto the track. This is likely to have occurred due to a combination of operator errors and a transient single point failure of the machine's control system. The machine operator was then unable to slow, derail or stop the excavator as it ran away.

The RAIB has made four recommendations relating to modifications to the design of the excavator, a review of the safety requirements that are specified for this type of machine, and a review of the training of people who control this type of machine on site.

Preface

1 The sole purpose of a Rail Accident Investigation Branch (RAIB) investigation is to prevent future accidents and incidents and improve railway safety.

2 The RAIB does not establish blame, liability or carry out prosecutions.

Key Definitions

3 All dimensions and speeds in this report are given in metric units, except speed and locations on Network Rail, which are given in imperial dimensions, in accordance with normal railway practice. In this case the equivalent metric value is also given.

4 The report contains abbreviations and technical terms (shown in *italics* the first time they appear in the report). These are explained in appendices A and B.

5 All mileages in this report are measured from the zero point at Perth.

6 In this report, a *road-rail vehicle* (RRV) is described as having a front or steering end. The other end of the RRV is known as the rear or fixed end.

The Accident

Summary of the accident

7 At about 23:39 hrs on 20 July 2010, a *machine operator* was *on-tracking* an excavator, a Liebherr A900C ZW type 1033 high-ride road-rail vehicle (RRV) onto the railway near Drumrosach farm, near Raigmore, Inverness (figure 1).

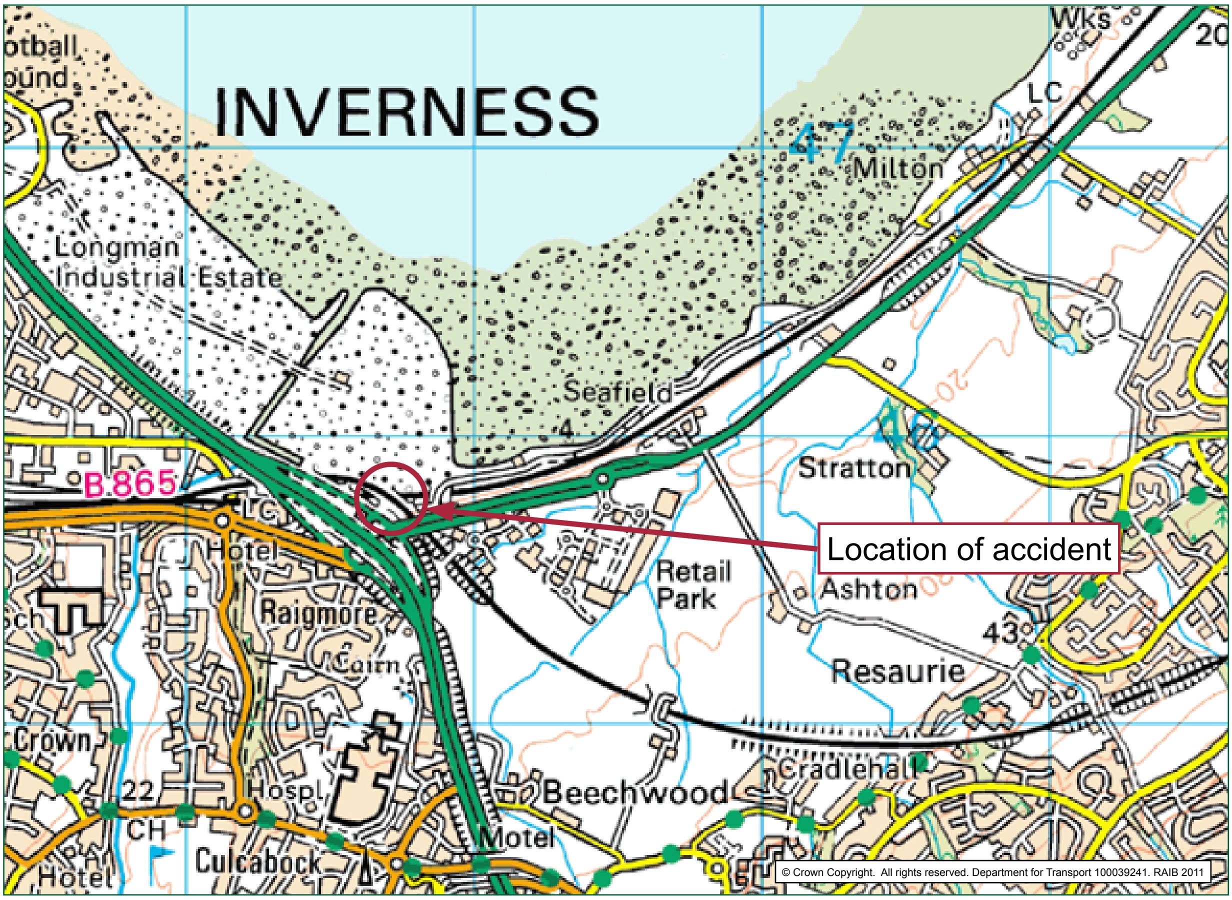


Figure 1: Extract from Ordnance Survey map showing location of accident

8 RRVs are vehicles that can operate both on railway track (rail mode) and the road (road mode). On-tracking an RRV is the operation of changing from road to rail mode. Off-tracking is the operation of changing back to road mode. This operation is normally carried out at a place on the railway that is designated for this purpose: a road-rail access point (RRAP).

9 The machine operator was preparing to start planned maintenance work on the track within an *engineering possession* of the line.

10 The RRAP at Drumrosach farm had been installed where the railway is on an average falling gradient of 1 in 60 towards Inverness (figure 3). As the machine was being on-tracked on the *down* line it began to run down the gradient. The operator, who was in the cab, and the *machine controller*, who was on the ground near the track, were unable to stop the machine before it gathered speed.

11 The machine ran for 0.88 miles (1.41 km) with the machine operator on board, passing signal I381 at danger and running 0.11 miles (0.18 km) outside the possession. The RRV then collided, at between 40 and 50 mph (64 to 80 km/h), with the rear of a stationary freight train which was standing at a signal outside the possession (figure 2). The collision occurred on the down line at 116 miles 69 chains, on the bridge over the line that runs between Inverness and Aberdeen.

Figure 2: The accident site showing the RRV and the rear wagon of the freight train

12 In the collision, the machine operator was thrown out of the RRV cab and landed on top of the rear wagon of the freight train, sustaining serious injuries which required hospital treatment. The RRV was derailed by all wheels and the leading axle of the rear wagon became derailed.

13 Both the RRV and the freight wagon sustained damage.

Organisations involved

14 Network Rail owns, operates and maintains the railway infrastructure.

15 Network Rail was responsible for the track maintenance planned for 20 July 2010 and one of its staff acted as the RRV machine controller.

16 Hydrex Equipment (UK) Ltd (Hydrex) owns and maintains the A900C ZW type 1033 RRV (fleet number 6878) and had hired it, and the machine operator, to Network Rail.

17 Liebherr Group (of which Liebherr-Great Britain Ltd is part), is a German-based manufacturer of construction machinery, earth movers, mobile cranes and RRVs. Liebherr Group specifically designed and built the A900C ZW type 1033 high-ride RRV for use in the UK.

18 Liebherr-Great Britain Ltd (Liebherr) sold the machine involved in the accident to Hydrex in May 2009.

19 Interfleet Technology (Interfleet) was appointed by Liebherr to act as the Vehicle Acceptance Body (VAB) for the type 1033 RRVs used in the UK. Its task was to assess the compliance of the RRV with the relevant railway standards and issue approval certificates.

20 Network Rail, Hydrex, Liebherr and Interfleet freely co-operated with the investigation.

Location

21 The accident occurred at 116 miles 69 chains on the down main line between Aviemore (83 miles 31 chains) and Inverness (118 miles 3 chains) (figure 3).

22 Between Culloden (111 miles 20 chains) and Inverness the railway is double track with a pair of crossovers at Cradlehall (116 miles 45 chains)

23 The signalling (at Inverness and extending to south of Culloden Moor) is three aspect colour light, controlled from Inverness Signalling Centre.

24 The average gradient between the 114 *mile post* and the site of the collision is 1 in 60 (falling towards the site of the collision).

25 The down line at the RRAP at Drumrosach farm (115 miles 79 chains) has a gradient of 1 in 50 and a *cant* of 70 mm. The RRAP is constructed from wooden timbers laid horizontally to provide a firm surface for an RRV to manoeuvre on when on-tracking. This timber surface extends to cover both the *up* and down lines and the space between them. A level ballast shoulder in the down *cess* area provides level access to the RRAP (figure 4). A large hinged gate is provided for railway access and a 100 metre farm track leads up to the railway.

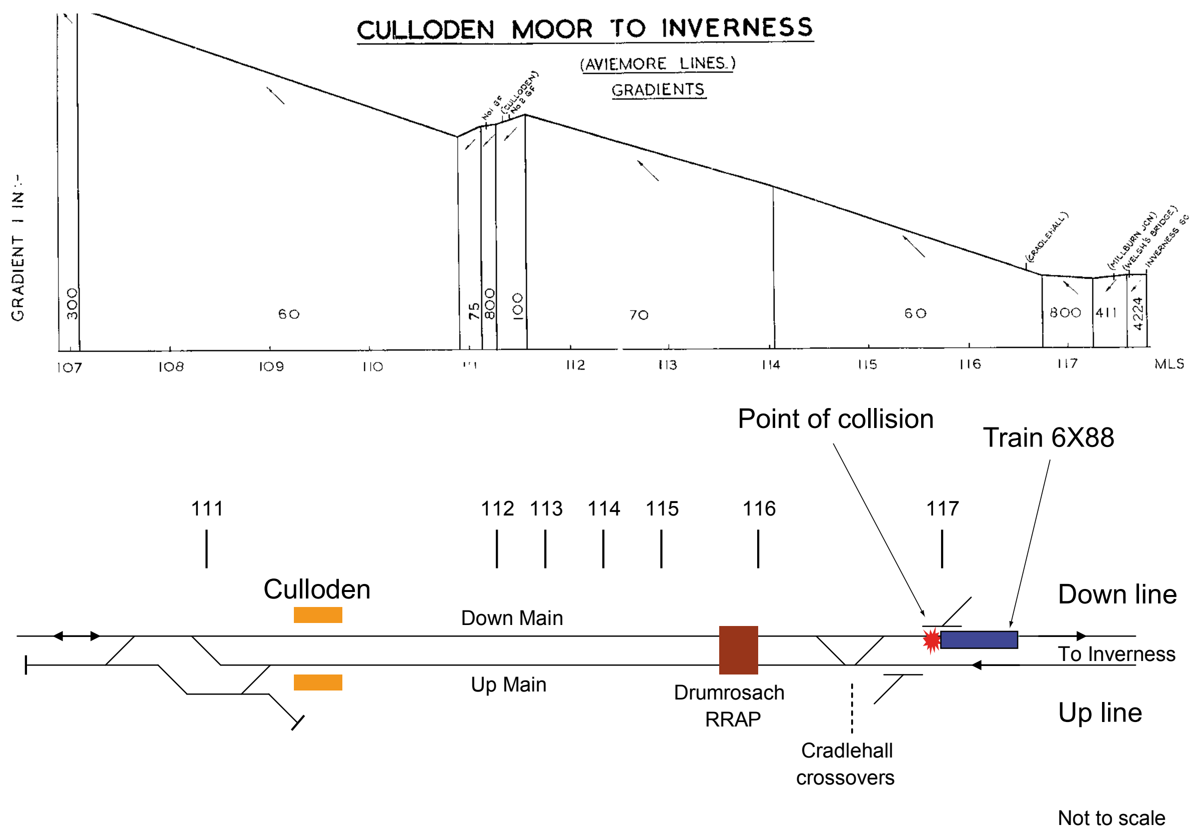


Figure 3: Track plan between Inverness and Culloden showing the RRAP and the accident site with associated gradient information


Figure 4: Drumrosach RRAP (picture taken from down line side cess)

External circumstances

26 At the time of the runaway, light rain was falling in the Inverness area, including Drumrosach farm RRAP. The temperature was 14° Celsius. The weather conditions did not contribute to the accident.

27 The RRAP was dark. It did not have any lighting installed and there were no other light sources nearby other than the lights on the RRV. The absence of external light may have affected the sequence of events leading up to the accident.

The train involved

28 The RRV collided with a stationary freight train that was carrying steel pipes. This train, reporting number 6X88, was standing (with the locomotive's engine switched off) at signal I387 on the approach to Welsh's Bridge Junction at Inverness.

29 The train consisted of a locomotive and 11 loaded BFA type bogie wagons, with 14 empty RRA type twin axle flat wagons intermixed between the loaded wagons. All the RRA type wagons (including the rear most one) were used as '*runners*' between the BFA wagons to accommodate the pipes, which were longer than the wagons they were loaded on.

The road-rail vehicle

30 At the time of the accident, 41 type 1033 RRVs were being operated in the UK. Hydrex owned 35, J Murphy & Sons owned five and Aspin Foundations Ltd owned one (figure 5).

Figure 5: The Liebherr A900C ZW type 1033 high ride RRV

31 The type 1033 is known as a high-ride RRV (UK rail gear classification: 'Type 9B')[1]. Machines of this type have rail wheels that are driven and braked by friction forces transmitted through the tyres of the road wheels[2]. The rail wheels have no direct traction or braking, and can rotate freely when they are not in contact with the road wheels. Each set of rail wheels is mounted on a hinged chassis which is raised and lowered hydraulically. When a set of rail wheels is lowered, they lift the adjacent set of road wheels clear of the ground. Contact between the road and rail wheels is not made until the rail wheels have almost completed their travel. The machine has two pairs of driven road wheels, one steerable and the other fixed[3]. Each pair of wheels has both inner and outer tyres (figure 5). The inner tyre is used for driving the rail wheels. The RRV also has an operator's cab, in which are the control panels for the road and rail functions (the rail control panel is known as the ZW system). The type 1033 RRVs have a software based control system for the machine's road, rail and lifting systems.

[1] There are also low-ride type RRV's (Type 9C), where the traction and braking forces are transmitted to the road wheels with the load shared between the road and rail wheels, and direct drive machines (Type 9A), where the traction and braking forces are transmitted directly to the rail wheels (ie the rail wheels are self-powered).

[2] The friction forces used to rotate or brake the rail wheels on the majority of high-ride RRVs are provided by pressing the rubber tyres – on the road wheels – into contact with the tread of the steel rail wheel. For clarity in this report, contact of a road wheel with a rail wheel means contact of the rubber tyre with the tread of the rail wheel.

[3] The steerable road wheels are locked in the straight ahead position immediately after the RRV has successfully on-tracked.

32 The software control system includes an *interlock* function designed to prevent the RRV from getting into a simultaneous free-wheeled state on all of its rail wheels during on- and off-tracking. It uses inputs from *potentiometers* mounted on the machine's main frame and connected to each rail chassis through mechanical linkages to convert the angle of each rail chassis relative to the machine frame into a variable voltage input into the control system[4].

33 The software interlock function is intended to prevent the machine getting into a configuration where the rail wheels are supporting the machine on the rails, but are not in contact with the road wheels. The machine operator is prevented from lowering or raising the second set of rail wheels until the first rail set have been lowered and are in contact with the road wheels (and thus braked) or raised with the road wheels in contact with the ground (and thus braked). The control system is designed so that the operator cannot raise or lower both sets of rail wheels at the same time.

34 The software system also uses the potentiometer output to continuously monitor the position of the rail chassis, which gives an indication of the amount of deformation of the road wheel pneumatic tyres by the rail wheels (known as *squash*) both during travel and operation. When this calculation is carried out in automatic mode (paragraph 35), the machine adjusts the squash automatically.

35 When the RRV has been successfully on-tracked, the machine operator should select the 'automatic' function on the rail (ZW) control panel. This function immediately repositions the rail chassis to maintain a squash of about 20 mm on all wheels and uses inputs from the potentiometers to maintain the squash at this figure while the machine is operating in rail mode.

36 The RRV has an extending boom and dipper arm, on which different bucket and other attachments can be fixed. The RRV involved in the accident had a small clam shell bucket hung from the dipper arm by a flexible connector[5].

37 The machine involved in the accident was built in 2009. Before type 1033 machines were introduced onto Network Rail infrastructure, Interfleet assessed their compliance with the Railway Industry Standard applicable at the time, RIS-1530-PLT issue 1 'Railway Industry Standard for Engineering Acceptance of On-Track Plant and Associated Equipment', issued by the Rail Safety & Standards Board (RSSB). Interfleet issued the *certificates of engineering acceptance* and the *certificates of conformance* for vehicle maintenance. Interfleet were employed by Liebherr to undertake this work.

38 Documentary evidence indicates that the RRV had been maintained by Hydrex in accordance with the manufacturer's service intervals, and no major defects were noted in its logbook. It had last been maintained on 15 July 2010. This was a planned weekly maintenance examination which involved the checking of fluid levels, a visual check for damage, checking of tyre wear, damage and pressures and a test of systems such as lights, horns etc. The only remedial action required following this examination was the topping up of hydraulic oil, which was carried out during the examination.

---

[4] Each potentiometer consists of a semi-circular track of conducting material, with a wiper contact attached to a central spindle. As the wiper moves, the resistance of the circuit which is made through the track and the wiper varies in proportion to the length of track material in the circuit, and hence in proportion to the angle of the wiper spindle.

[5] The clam shell bucket can be opened /closed and rotated in the horizontal plane by the machine operator. The bucket is connected to the dipper arm by a flexible connector and is free to move under the effect of gravity.

39 The machine operator had also recorded that he had completed pre-use inspection checks every time he used the machine (the last dated 18 July 2010) with no problems found.

40 The tyres on the machine involved in the accident were all in good condition although three of them, all fitted as inner tyres and therefore used for driving the rail wheels, were not of the type specified by the manufacturer. However, these three tyres were of the correct size. The tyre pressures of all inner and outer tyres were measured immediately after the accident and were found to be approximately six bar; two bar below the manufacturer's specified pressure of eight bar.

Staff involved

41 The machine operator was employed by Hydrex, and had over sixteen years experience of operating RRVs and other types of plant.

42 The machine controller was employed by Network Rail in infrastructure maintenance, based in Inverness, and had 30 years experience on the railway. He had over 2 years experience as a machine controller and had had general experience in on and off-tracking RRV type machines during this period. He had been machine controller for the Liebherr type 1033 RRV on a number of occasions, in the weeks before the accident.

43 On 20 July 2010, the roles of RRV machine controller, *controller of site safety* (COSS), *engineering supervisor* (ES) and *person in charge of the possession* (PICOP) were all undertaken by the same person, who was employed by Network Rail. In this report, this person is called the machine controller.

Events preceding the accident

44 The following account is based on witness statements from those directly involved in the accident.

45 On 14 July 2010, the RRV (and machine operator) involved in the accident had become available, at short notice, to Network Rail's maintenance organisation. Network Rail then decided to utilise the RRV for previously planned maintenance work at Inverness during the week commencing 19 July 2010.

46 On 19 July, the RRV (with the same operator and machine controller involved in the accident) was used for maintenance work in a possession between Tomatin and Cradlehall crossovers, near Inverness. This also involved the use of a trailer (connected to the RRV) to transport two rails. After the work was completed the trailer was off-tracked at Drumrosach RRAP followed by the RRV. The RRV was then driven on its road wheels and parked approximately 100 metres from the railway boundary near farm buildings at Drumrosach Farm.

47 The following day, 20 July, at approximately 21:00 hrs, both the machine operator and machine controller met near to the railway at Tomatin. The machine operator left his van there and both men then travelled in the machine controller's van to Cradlehall.

48 At Cradlehall, the machine controller (who was also undertaking PICOP, ES and COSS roles – paragraph 43) organised the laying of *protection* in readiness for the granting of the *T3 possession* (between Tomatin and Cradlehall). At 23:12 hrs, the signaller at Inverness gave permission to the machine controller to place the protection (figure 6).

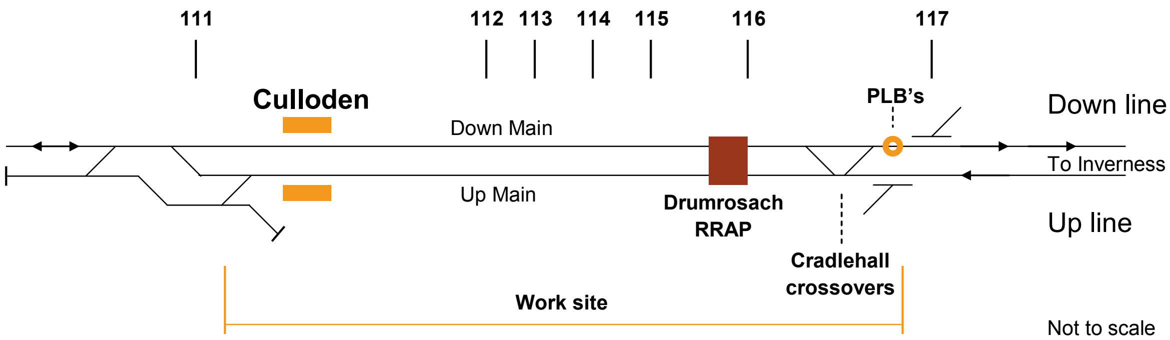


Figure 6: Track plan showing the possession and worksite limits for 20 July 2010

49 The machine controller then placed *possession limit boards* and *detonators* at the correct positions, and at 23:20 hrs, the signaller granted the machine controller the T3 possession. The machine controller and operator then travelled to Drumrosach Farm in the machine controller's van.

50 At Drumrosach Farm, the machine controller gave permission for another machine which was to work in the possession, a road-rail survey vehicle, to be on-tracked. This vehicle was successfully on-tracked onto the down line at the RRAP and driven immediately towards Culloden, where it was to meet other staff to carry out planned rail maintenance work at about the 111 mile post.

51 The machine controller (with assistance from the operator) then completed a Machine Site Arrival Check list (ref: Network Rail, Train Operations Manual, TMC08, issue 6, Appendix A 'Part A – Machine Controller Checklist RRV/RMMM') on the Liebherr RRV machine. The checks included the following:

- operator's fitness to work;
- correct briefings undertaken;
- correct on/off-tracking facilities available;
- lifting plan correct and other lifting checks;
- operator completion of pre-start checks on the RRV; and
- controller's witness of successful functional brake test.

52 Even though all the checks on the list had been ticked as 'yes', some of them (such as the check on stopping distance in rail mode) could not have been completed until after the RRV had been successfully on-tracked. However, witness evidence indicates that the operator carried out some of the other checks.

53 At 23:30 hrs, the machine controller gave the machine operator permission to on-track at the RRAP. While the RRV drove towards the RRAP, the machine controller completed his PICOP, ES and COSS paperwork, intending to join the operator at the RRAP to assist in the on-tracking process.

54 At approximately 23:36 hrs, the machine operator began to on-track the RRV on the down line at the RRAP, with the front (steerable) wheels pointing downhill towards Inverness. The machine controller was not present at that time. Two minutes later, at 23:38 hrs, the machine controller arrived at the RRAP and both men had a brief conversation: the machine controller told the operator that the rear (Culloden end) rail wheels of the RRV were not on the rails but sitting on the wooden surface of the RRAP.

55 Following this conversation (at 23:39 hrs) the operator placed the rear rail wheels onto the rails. He did this by placing the clam shell bucket (attached to the end of the boom arm) onto the ballast[6] in the four foot of the down line (just off the uphill end of the crossing) and lifting the rear end of the vehicle upwards and into line with the railway track. Finally he lowered the rear end of the RRV down onto the rails. The rear rail wheels made contact with the rail, and as soon as the bucket was lifted clear of the ballast, the machine started to roll away towards Inverness.

56 Both the machine operator and controller were unable to stop the machine before it gathered speed, and upon realising this, the machine controller made a telephone call to the signaller to warn him of the runaway.

Events during the accident

57 As the RRV started to roll away towards Inverness in a free-wheel state, the machine operator immediately swung his cab to face the direction of travel. He then quickly lowered the boom and dipper arm so as not to hit a farm road bridge that was 70 metres from the RRAP. During this time the operator applied the brake many times, with no effect. The machine controller began to follow the RRV on foot, as fast as he could.

58 Although the machine was in a free-wheel state the operator found that he could not raise or lower the rail wheels[7]. The upper part of the RRV (the boom and dipper arms and the rotation of the cab) was not affected and responded normally to the operator's commands.

59 After the RRV had travelled under the road bridge, the operator immediately used the clam shell bucket to try to slow or stop the machine by dropping and dragging the bucket onto the sleepers between the rails. However, the momentum of the machine was too great to be overcome by the use of the bucket and the speed of the RRV continued to increase. The operator tried this method again several times before the point of collision, but with little or no effect.

60 The operator also switched the engine of the RRV off and on again (he hoped this might have the effect of re-booting the internal software systems), but this had no effect on the free-wheeled state of the machine. Although the operator could control the upper part of the RRV, the rail controls were still locked because the interlocks of the RRV were still active.

61 As the RRV approached the crossovers at Cradlehall (116 miles 45 chains), the operator lifted the boom and bucket to clear the points and to avoid damage to the track.

[6] The method of using the boom arm, with the attachment to raise one end of the RRV upwards, to manoeuvre is not permitted by Hydrex or Liebherr. It is a high risk activity which could result in the RRV tipping over.

[7] The rail controls were locked because the interlock function detected that each wheel set was partly deployed and prevented movement of the other end, thus disabling all operator raise/lower controls.

62 The RRV struck and passed the possession limit boards (and exploded the protecting detonators) at 116 miles 60 chains. At about this time the operator saw the tail lamp of a freight train ahead, and swung the cab 90° to face the up line, so that the cab door of the RRV was facing the direction of travel.

63 At approximately 23:42 hrs, the RRV collided, at between 40 - 50 mph (64 - 80 km/h), with the rear of the stationary freight train which was standing at signal I387 outside the possession (figure 2). The collision occurred on the down line at 116 miles 69 chains, on the bridge over the line between Inverness and Aberdeen.

64 In the collision, the machine operator (who was not wearing a seatbelt) was thrown out of the RRV cab, and landed on top of the rear flat wagon. All wheels of the RRV were derailed, together with the leading axle of the rear wagon.

65 About four minutes later, the machine controller arrived at the collision point. The engine of the RRV was still running. The controller immediately made an emergency call to the signaller and at 23:58 hrs, the signaller called the emergency services.

Consequences of the accident

66 The operator received serious injuries both as he was ejected from the RRV cab, and also on landing on the rear flat wagon of the freight train.

67 The front of the RRV was damaged and distorted by the force of the impact with the stationary wagon. The machine's near-side rear (fixed end) road wheel was also damaged where it had struck the girder of the underbridge during the derailment.

68 The RRV cab sustained some minor damage.

69 Despite this damage, the RRV remained functional. It was fully tested and on- and off-tracked with the RAIB in attendance once it had been separated from the wagon of the freight train.

70 Damage to the train was limited to the rear wagon. The trailing end drawhook, coupling area and headstock of the wagon were badly crushed, and the underframe was buckled.

71 The rear three loaded wagons of train 6X88 showed signs of the large pipes which made up the train's load having shifted during the collision. The pipes on the rearmost loaded wagon moved 0.45 metres, the pipes on the 2nd from rear loaded wagon moved 0.30 metres and the pipes on the 3rd from rear loaded wagon moved 0.05 metres. One restraining strap had broken. The pipes themselves were not damaged.

72 There was 'chipping' damage to some of the concrete sleepers between the RRAP and the point of collision, caused by the bucket of the RRV being put down and dragged along, and a small number of track clips were knocked out.

Events following the accident

73 The emergency services arrived at 00:04 hrs on 21 July and the machine operator was taken to hospital. As part of the rescue, the fire brigade switched off the engine of the RRV.

74 At 07:00 hrs on 21 July, a member of Hydrex staff was given permission by the RAIB to move the cab and boom arm (that were obstructing the up line) back into line with the machine chassis so that trains could start running on the up line. Police witnessed this operation. At 09:58 hrs, trains began running only on the up line under single line working arrangements.

75 On 22 July, at 02:15 hrs, the rear wagon of the freight train was re-railed and soon after, at 03:10 hrs, the RRV was switched on and its on-board memory on the machine display unit was analysed. This was done under the control of the RAIB. The data on the display unit did not show any active error codes or any codes associated with the operation and deployment of the rail wheels. Following this, the RRV interlock functions were tested[8] under supervision of the RAIB (and appeared to operate correctly) before being on-tracked where it had derailed. At 04:07 hrs, the RRV was driven back along the down line to Drumrosach RRAP, where it was successfully off-tracked and taken into quarantine under Police escort.

76 At 05:46 hrs, with the freight train now clear of the line, the down line was reopened.

[8] In order for one of the rail axles to be moved and the interlock function overridden, an engineer's key (paragraph 159) had to be used.

The Investigation

Sources of evidence

77 The following sources of evidence were used:

- witness statements;
- data from the RRVs onboard memory on the machine display unit (which records fault codes and the number of each type that have occurred since the system was last reset);
- survey of Drumrosach RRAP, measurements and photography;
- site survey of the point of collision, measurements and photography;
- telephone voice recordings from Inverness signalling centre;
- BTP and Highlands & Islands Fire & Rescue logs;
- detailed testing of the RRV and its components on a railway siding and in the laboratory, and analysis of the results;
- training and competence records;
- documents and information supplied by Network Rail, Liebherr, Hydrex and Interfleet;
- weather reports and observations at the site; and
- a review of previous RAIB investigations that had relevance to this accident.

Key facts and analysis

Background information

High-ride road-rail vehicles – run away risk during on/off-tracking

78 When a high-ride RRV is operating in road mode, the road wheels are in contact with the ground and provide the braking. When lowering the rail wheels at one end, while on-tracking, a transient condition occurs in which no braking is provided at that end of the vehicle. This happens because the rail wheels, not yet in contact with the road wheels, contact the rail and lift the road wheels at that end off the ground (figure 6). The same transient condition occurs while off-tracking: contact is lost between the rail wheels and the braked road wheels before the road wheels contact the ground.

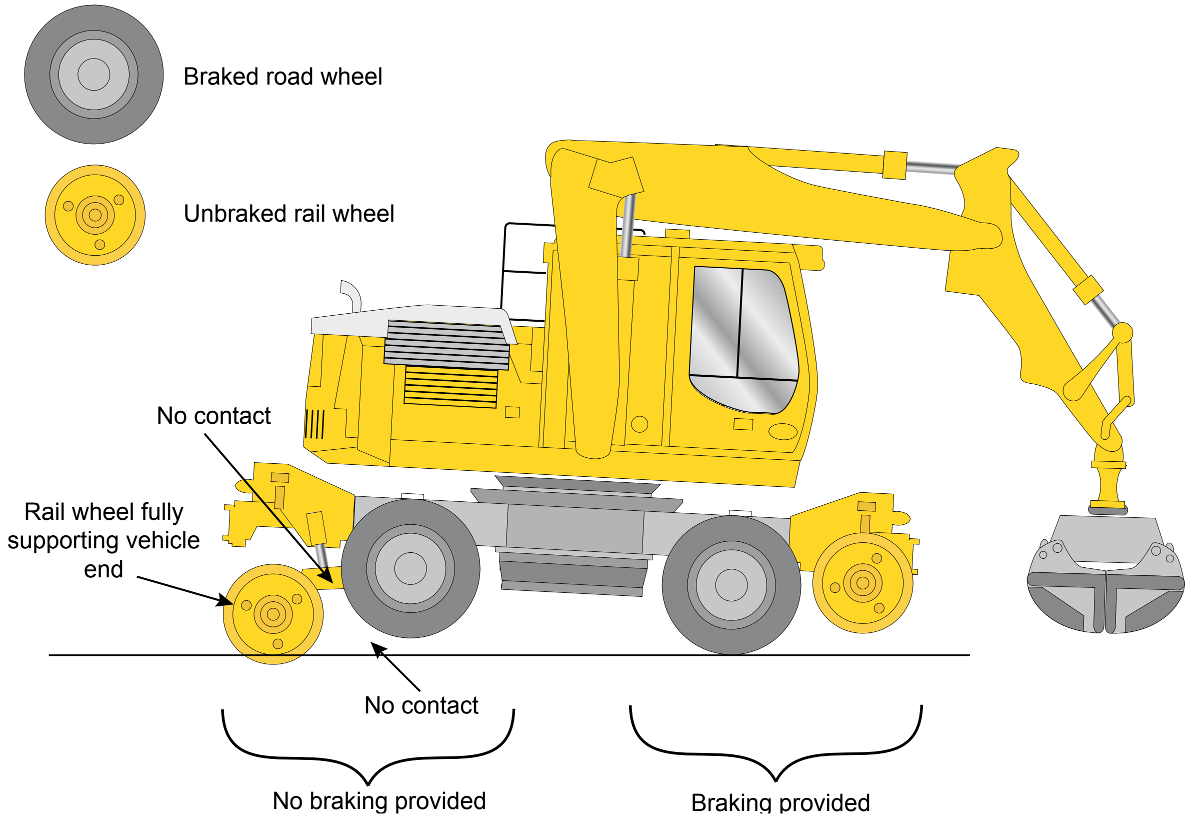


Figure 7: High-ride RRV - transition condition that results in no braking being provided at one end of the machine during on/off-tracking

79 This transient condition is an inherent feature of the high-ride design, if the rail wheels are not independently braked. When the machine is on or off-tracked on an incline, prevention of a runaway relies on there being sufficient braking at the other end of the machine (subsequently referred to as the *holding end*). If there is no brake force at the holding end, a point is reached, as the rail wheels are lowered (or raised), when all braking is lost and, even on a modest gradient, the RRV will start to run away.

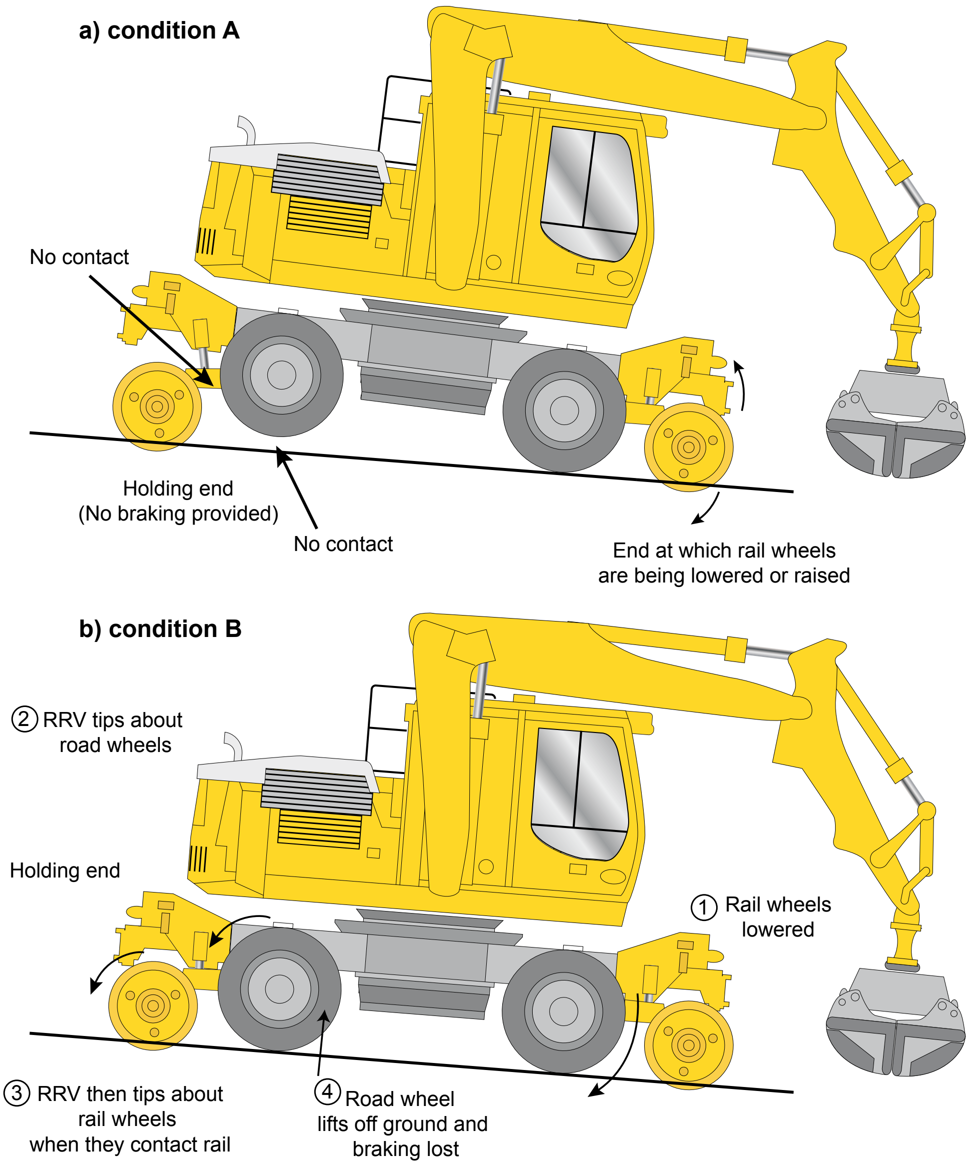
80 Given the above, there are two conditions which can lead to a runaway:

- Condition A

  The holding end is left in the transient condition with no braking provided (road wheels lifted off the ground, rail wheels not sufficiently in contact with the road wheels) when the rail wheels at the opposite end are lowered (or raised) (figure 8(a)).

- Condition B

  The road wheels at the holding end are on the ground, and carrying their full load, but the rail wheels are left close to (or just touching) the rail. With reference to Figure 8(b), when the rail wheels at the opposite end are lowered (1), the RRV first tips about the road wheels at the holding end (2), but it then tips about the adjacent rail wheels as they come into contact with the rail (3). This lifts the road wheels that were providing the braking off the ground (4)[9].



Figures 8a and 8b: High-ride RRV - on/off-tracking runaway conditions

[9] For practical reasons, the rail wheels on high-ride RRVs are usually located outboard of the road wheels. This makes them prone to contacting the rail when the RRV tips as the opposite end rises.

81 The following control measures can prevent the two conditions occurring during on/off-tracking :

- a check that at the holding end **either** the rail wheels are in full contact with the road wheels, **or** the road wheels are in full contact with the ground and the rail wheels are fully clear of the rail; and
- confirmation that the above state remains until the rail wheels on the opposite end are fully lowered (or raised), and therefore once again in contact with the road wheels.

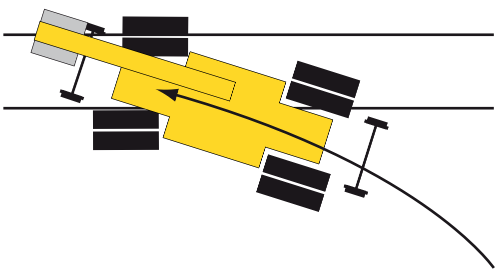
82 Network Rail requires RRVs to comply with the railway industry standard, RIS-1530-PLT 'Engineering acceptance of possession-only rail vehicles and associated equipment'. The RRV involved in the accident was assessed and approved against issue 1 of RIS-1530-PLT. Clause 5.17.1.1 d required a 'documented system' for on- and off-tracking that had been assessed to ensure that 'no inadvertent movement' occurs that causes a loss of braking. The standard did not require RRVs to be fitted with control systems that prevented this 'inadvertent movement', although compliance with the standard could be achieved by fitting such a control system.

83 The Liebherr type 1033 RRV had a software operating system that included a rail axle interlocking function designed to prevent the RRV from getting into a free-wheeled state on its rail wheels (paragraph 32).

84 This interlock function was intended to enhance the safety features of the machine so that it complied with standard RIS-1530-PLT without the need for additional operating procedures.

Road-rail vehicle on-tracking method

85 The following diagrams (figure 9a - h) show the correct sequential method of on-tracking a type 1033 high-ride RRV. This method is considered by the rail industry to be 'best practice'.



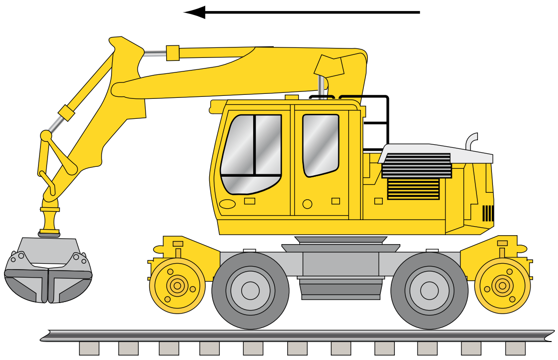


Figure 9 a & b - Rail mode is selected on the ZW box. The RRV is then driven onto the RRAP, front end first. The machine controller should be present.

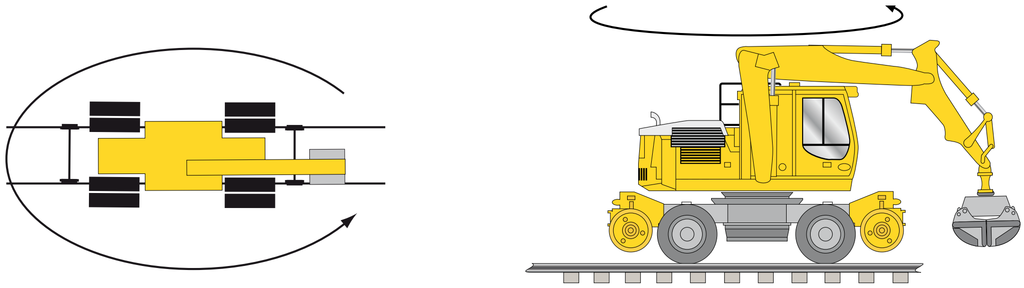


Figure 9 c & d - The cab is swung to the rear of the RRV and the rear rail wheels are lined up with the track using the road wheels to manoeuvre the machine.

Figure 9e
The rear rail wheels are lowered onto the track to lift the rear road wheels from the ground. An air gap between the wheels is deliberately allowed at this time. In this position the interlock function prevents the front rail wheels from moving.

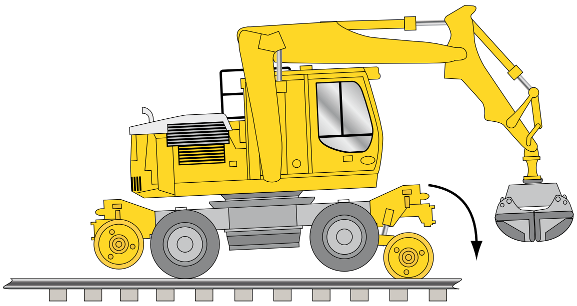


Figure 9f
The cab is swung to the front of the RRV and the front rail wheels are lined up with the track (if not already done under fig 9c), using the front (steerable) road wheels to manouvre the machine.

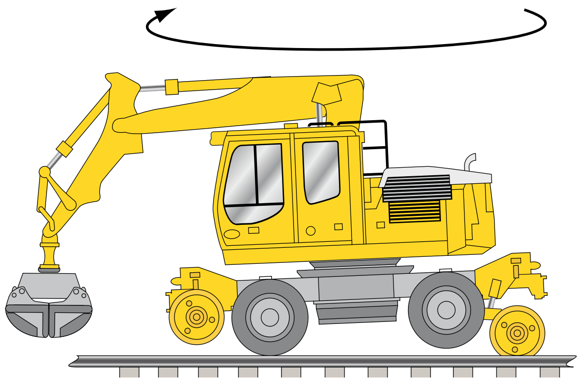


Figure 9g
The rear rail wheels are fully lowered to maximum road/rail wheel 'squash'. In this position, the interlock function will now allow the front rail wheels to be moved.

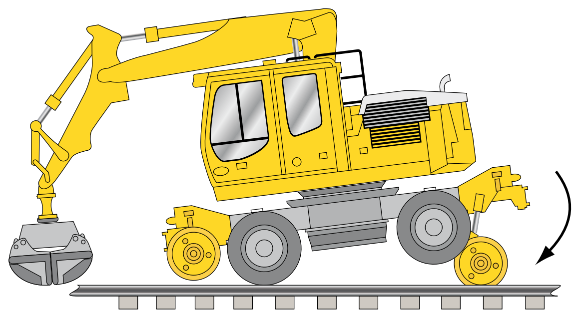


Figure 9h
The front rail wheels are now fully lowered to the maximum road/rail wheel 'squash'. The machine operator now selects 'automatic' on the ZW box. This reduces the squash to approximately 20mm on all wheels. The machine is now ready to travel along the rails.

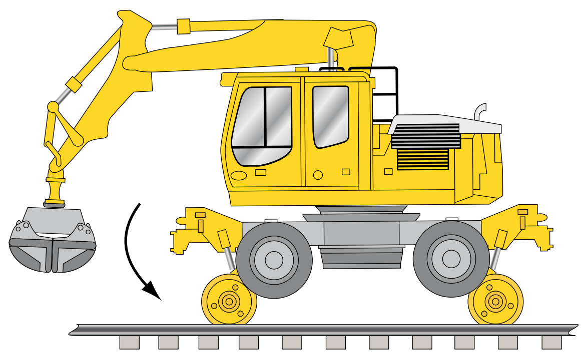


Figure 9a - h: High-ride RRV - correct method of on/off-tracking

Competence and fitness of the staff involved

The machine operator

86 The operator held a valid Construction Plant Competence Scheme (CPCS) card (issued by the Construction Skills Certification Scheme (CSCS)) for proficiency in using plant in road mode, including excavator 360° machines (of which the 1033 machine was an example).

87 The operator had also undergone training designed to meet the competence standards adopted by Network Rail and developed by the Rail Plant Association[10]. These included a core module (covering the Railway Rule Book module OTP [www.rgsonline.co.uk]) and specific modules relating to generic machine types eg 'operate road rail excavator'. The operator was also issued with Network Rail and CPCS log books to record his experience, which he had filled in.

88 Since 2009, Network Rail has included machine operators in the *Sentinel Scheme*[11]. Trainers and assessors have to be registered with the scheme and operators are registered on a National Competency Control Agency (NCCA) database and must carry a valid Sentinel competency card.

89 On 28 May 2009, the operator had been given a one day familiarisation training course on the Liebherr A900C ZW type 1033 high-ride RRV, and was assessed as competent to operate the machine. He was reassessed as competent on this machine on 22 December 2009. The Hydrex certification issued to the operator for the specific Liebherr machine is called an Authority to Work (ATW) card.

90 The operator's Sentinel card was endorsed with 'OTP (on-track plant) operator'. The competence relating to specific plant was detailed on a secure counterpart document also issued by Sentinel. This stated that the operator was competent in the operation of an excavator/crane. The counterpart also listed various attachments for the excavator, including trailers, which the operator was competent to use.

91 The machine operator had worked with the machine involved in the accident from when it was new (May 2009), continuously until March 2010. There was then a two and a half month period when he worked with another Liebherr RRV of a similar high-ride type. From 19 June 2010, he resumed using the original RRV and worked with this machine full-time until the day of the accident.

92 The machine operator's written entries in his Network Rail log book of 'shifts completed' stops on 16 June 2010 because the book was full. No entries had been made for any work undertaken from that date onwards in a new log book or on any other temporary written record. Space for 'shifts completed' was available in the operator's CPCS log book, but this book had also not been used since 16 June 2010. It is a requirement of the CPCS scheme that a record of shifts is completed and countersigned by the machine controller. However, the reason for the log book is to demonstrate that the person can meet the minimum experience requirements within the CPCS. The machine operator had completed more entries than the minimum required which would allow re-assessment to take place at the required time.

---

[10] The Rail Plant Association (RPA) is a limited liability company and was launched in 1999. The main purpose of the RPA is to look after the interests of its members who hire specialist plant and equipment for use on the railway infrastructure.

[11] Sentinel is the system used by Network Rail for managing the competence of staff working in certain safety critical roles.

93 The operator did not have any safety related incidents relevant to this accident.

94 Immediately before the day of the accident, the machine operator's work pattern had been[12]:

- 14 July – 23:00 hrs to 07:00 hrs
- 15 and 16 July - off
- 17 July – 23:00 hrs to 07:00 hrs
- 18 July - 23:59 hrs to 05:00 hrs
- 19 July – 21:00 hrs to 06:00 hrs
- 20 July – 21:00 hrs to 23:42 hrs (time of the accident)

95 The RAIB has calculated the machine operator's Fatigue Index value[13] (at the end of his previous shift; 06:00 hrs on 20 July) as 50, and his Risk Index value[14] as 1.39. However, prior to starting work he had had a period of rest. These values were based on his work shift and rest pattern (including travelling time). They indicate that the machine operator had been exposed to a work pattern likely to cause fatigue above the level considered good practice within the railway industry, and that the risk of an incident occurring due to fatigue was slightly higher than average. However, the operator was used to working night shifts and was employed by Hydrex to work a continual pattern of night shifts, which he had done for many years. At the time of the runaway, he was less than three hours into his shift and there was no evidence to suggest that he was fatigued at this time.

96 Following the accident, the machine operator was not tested for non-permitted drugs and alcohol either at site, or later in hospital, because of the serious nature of his injuries. However, there is no evidence to suggest that drugs or alcohol were factors in the causation of the accident.

The machine controller

97 The machine controller also carried a valid Sentinel competency card, endorsed with the competencies for the roles that he was required to undertake on the night of the accident: PICOP, ES, COSS, and Machine Controller RRV.

98 The competence relating to specific plant was detailed on a separate counterpart document also issued by Sentinel. This stated that the controller was competent as machine controller RRV (360° excavator). The controller had also been issued with a Network Rail log book which is supposed to be used to record experience. This had been mislaid by the controller (and had not been checked by his manager) and so no record of his experience could be produced.

---

[12] Travelling times are not shown, but incorporated into the index calculation.

[13] The potential for fatigue arising from the above work pattern has been assessed using the Health and Safety Executive (HSE) Fatigue and Risk Index Calculator (version 2.2) available from www.hse.gov.uk. The output from the fatigue index is a measure of the probability of high levels of sleepiness. This is expressed as a value of between 0 and 100. A fatigue index of 20.7 corresponds to the average work shift and rest pattern, assuming typical values for the job type and breaks factor. A 'benchmark' fatigue score of between 30-35 for day or early shifts and 40-45 for night shifts relates to the probability of a person suffering high levels of sleepiness. The value given is an average for the whole duty not hour by hour. ORR guidance entitled, 'Managing fatigue in safety critical work', defines a night shift as a shift that usually starts between 22:00 hrs to 02:00 hrs and ends between 05:00 hrs to 08:00 hrs.

[14] The output from the Risk Index is in terms of the relative risk of an incident occurring. The value of 1.0 is an average risk of an incident for a Day/Day/Night/Night/Rest/Rest/Rest/Rest schedule on standard 12 hour shifts.

99 Immediately before the day of the accident, the machine controller's work pattern had been:

- 14 to 18 July - off
- 19 July – 21:00 hrs to 06:30 hrs
- 20 July – 21:00 hrs to 23:42 hrs (time of the accident)

100 The RAIB has calculated the machine controller's Fatigue Index value (at the end of his previous shift; 06:30 hrs on 20 July) as 40 and his Risk Index value as 0.87. However, prior to starting work he had had a period of rest. These values were based on his work shift and rest pattern (including travelling time) and indicate that the machine controller had been exposed to a work pattern likely to cause levels of fatigue within those considered to be good practice in the railway industry. The controller was used to working night shifts and was employed by Network Rail to work a continual pattern of night shifts, which he had done for many years.

101 Following the accident, the machine controller was drug and alcohol screened, in accordance with his employer's post incident procedure. The results did not reveal the presence of either prohibited drugs or alcohol

Identification of the immediate cause[15]

102 **The immediate cause of the accident was that the road-rail vehicle ran away from the RRAP in an unbraked condition on a downhill gradient.**

103 The machine operator was unable to slow or stop the RRV as it ran away.

104 Following the collision with the freight train, the rail wheels of the RRV were found to be not in contact with the road wheels, and therefore free to rotate. This condition was observed and recorded by the RAIB at the scene of the collision, before the interlock was overridden with an engineer's key (paragraph 75).

Identification of causal[16] and contributory factors[17]

The road-rail vehicle

Unbraked condition

105 **The RRV was placed into an unbraked condition. This is likely to have been as a result of a combination of operator actions and a single point failure[18] of the control system. This was a causal factor.**

---

[15] The condition, event or behaviour that directly resulted in the occurrence.

[16] Any condition, event or behaviour that was necessary for the occurrence. Avoiding or eliminating any one of these factors would have prevented it happening.

[17] Any condition, event or behaviour that affected or sustained the occurrence, or exacerbated the outcome. Eliminating one or more of these factors would not have prevented the occurrence but their presence made it more likely, or changed the outcome.

[18] A single point failure is a condition in which a defect or malfunction of a single component causes the system of which it is a part to stop working or behave in an unplanned way, and where there is no duplication or redundancy within the design of the system to alleviate the effects of such a failure.

106 The RRV was inspected and examined by the RAIB at the accident site before it was moved. At the front end of the RRV (the end that had collided with the flat wagon) there was an air gap of 80 mm between the road and rail wheels. At the rear end of the machine (ie the trailing end), there was a 20 mm air gap between the road and rail wheels. The construction of the machine is such that these gaps would not have been increased by the effects of the collision, and the dimensions are likely to have been the same during the runaway. During the examination and testing of the machine following the accident, no evidence was found of mechanical damage that would have caused these gaps to have been created or widened.

107 In normal operating circumstances, either end of the machine should have at least 20 mm of 'squash' between the road and rail wheels to provide the friction forces required for braking (paragraph 34). As there were air gaps on all four road/rail wheels of the RRV (and the rail wheels were able to rotate freely), any action by the machine operator to apply the brakes would have had no effect.

108 To try to understand the reasons for the air gaps on all four road/rail wheels of the RRV, the RAIB reviewed the following documents:

- Liebherr Service Manual Hydraulic Excavator A900 C – ZW Litronic, edition 12/2008, updated 05/2009; and
- Liebherr Operating Manual Hydraulic Excavator A900 C – ZW Litronic, edition 06/2009.

109 The service manual contained detailed electrical wiring diagrams of the RRV including control system parameter charts and tables for the rail wheel deployment and control systems interface. The manual also included mechanical and hydraulic system drawings. The operating manual described how the machine should be operated including the on and off-tracking procedure.

110 A key feature of the design, as shown by these documents, is that the control system, including the interlocking function, uses potentiometers (one connected to each rail chassis through mechanical linkages) to measure the angle of rail chassis movement. There are no other electrical inputs into the control system relating to rail wheel position or movement.

111 The use of one potentiometer per rail chassis (with no secondary or backup system) could lead to a single point failure. An open circuit, short circuit or high resistance either within the potentiometer itself or in the wiring of that circuit, could alter the input voltage detected by the interlock function of the control system. These types of failures could result in the position signal to the control computer being offset, so that the computer incorrectly detects the position of the rail wheels. The control system therefore relies on the correct voltage being received from the single potentiometer at each end of the RRV.

Examination and testing of the machine

112 The RAIB examined and tested the machine involved in the accident to establish how the machine had come to be in a free-wheel state. The RAIB devised an examination and test plan, which was fully consulted with Liebherr, Hydrex, Network Rail and the Office of Rail Regulation (ORR). The test plan covered the following areas:

- an examination of the machine to assess its condition;
- tests to identify and characterise:
  - machine display unit error codes and other software values;
  - input and output values of the control system;
  - squash values in relation to the interlock function;
  - potentiometer output and relation to the interlock function;
  - integrity of the wiring between the potentiometers and the control box;
  - potentiometer faults and their effect on interlock function;
  - conditions required to release the interlock function and generate fault alarms; and
  - operation of the machine's 'automatic' function.

113 The RAIB also developed a comprehensive set of operational scenarios to account for the ways in which the machine could have been on-tracked, and agreed these with the interested parties. Eleven on-tracking scenarios were devised and tested to establish how the machine behaved in each one.

114 As part of the development of the testing plan, certain factors were discounted as not requiring testing or further analysis. These were:

- Inner tyres – the three inner tyres that were not of the type specified by Liebherr were of the correct size, although their tread pattern differed from the tyres supplied by Liebherr;
- Low tyre pressures – although this did not affect the contact between the tyres and the rail wheels, the tyre pressures were lower than specified; and
- Low adhesion between wheel and rail – not relevant as the RRV ran away from the RRAP in a free-wheel state with significant air gaps between all four road and rail wheels (paragraph 104).

115 Three sets of tests and examinations were carried out, all of which were attended by representatives of RAIB, ORR, Liebherr and Hydrex. Representatives of Network Rail were only present at the first set of tests.

First set of test results

116 These tests, using the complete RRV, investigated the general characteristics of the electrical and control systems for the deployment and operation of the rail wheels of the RRV.

117 This showed that the interlock was active from before the rail wheels made contact with the rail until after they had achieved at least 10 mm squash on the road wheels. Although there was some deviation between the measurements on the front and back wheelsets, the functional effect was as expected – the interlock inhibited the raising or lowering of a set of rail wheels until the opposite end rail wheels were in squash or clear of the rail.

118 The tests simulated eleven on-tracking scenarios to attempt to recreate the free-wheel scenario. In none of these did the RRV get into the free-wheel state, and the interlocks were seen to operate as intended. The results showed that the rail control system software appeared to perform as designed across all eleven scenarios. On this basis, failure of the software to perform as designed was then discounted as a factor and was not the subject of further testing and analysis.

119 Some additional tests were done on the effect of losing data signals between the rail control box in the cab and the control system in the chassis. This was to simulate a scenario where the data signal, which passes through *sliprings* to the chassis, was lost, to see if it was possible to get into a free-wheel state. These showed that control functionality was lost when the data connection was lost, and movement stopped. Similarly, when the data connection was restored, the control system responded correctly, ie any interlock that had been active before the loss of signal remained active. No mechanism by which this could give rise to the free-wheel state was identified.

120 The RAIB constructed a test box that could be inserted into the electrical circuit between the potentiometers and the control system computer. This allowed simulation of faults in the wiring harness and connectors between the potentiometers and the control computer. It also allowed supply and control voltages to be measured and a selection of open circuit, short circuit and resistive faults on the potentiometer to be simulated. The test box was inserted into the front and rear potentiometer circuits, in turn.

121 With the relevant rail wheels in the free-wheel position, open circuit faults on each of the three terminals of the associated potentiometer were simulated. In addition, short circuits between the wiper and the other terminals were created. For all the faults, the computer system (paragraph 32) allowed the opposite end wheel to release, and a potentiometer fault alarm was raised[19]. The interlocks reapplied automatically on removal of the faults. The results were the same for both potentiometers.

122 A test was then carried out for each set of rail wheels, to characterise the relationship between rail chassis angle and the position input to the control system (measured in volts). The purpose of this was to inform later analysis.

123 This was followed by a check of the potentiometers' outputs over their whole range of travel. This did not reveal any sudden changes in, or loss of, the control system input voltages as the potentiometers were swept from one end to the other.

---

[19] A potentiometer fault alarm is raised by the indication of an error code displayed on the monitoring display in the cab. There is no audible alarm. The error code is visible to the operator and is recorded on the memory on the machine display unit.

Second set of test results

124 A second set of tests explored in more detail the interaction between the RRV's rail wheel control system and the potentiometers which detect the positions of the rail chassis. This included the simulation of faults to discover how the system reacted.

125 Tests were undertaken to identify the routeing and integrity of the wiring carrying the potentiometer signals to the control system computer. This identified the connectors that the signals passed through, and the majority of these were checked to see if any disturbance to these altered the voltage received at the control system computer. There was no indication of any loss of signal during these tests.

126 The test box was used to assist measurement of the precise voltages at which interlocks and alarms were operated and freed as each set of rail wheels were moved. This allowed the control system actions to be characterised more closely than in the first set of tests.

127 Another series of tests were carried out to show the effect of a resistive potentiometer wiper on the interlocks. With a range of resistances in series with the potentiometer wiper, the computer system released despite the rail wheels being in a free-wheel condition. The release was instantaneous on application of the fault, and the interlock was restored instantly on removal of the fault.

128 The effects of a resistive fault were simulated for the potentiometer wipers and both power supply connections to the potentiometers. The effects on the control system input voltage and the interlock and fault alarms were recorded for differing resistances on both potentiometers (paragraphs 142 to 145). This showed that it was possible for a resistive potentiometer wiper, or for a high resistance in the associated circuit, to release the opposite end interlock, without initiating a potentiometer fault alarm.

Testing and examination of potentiometers

129 The testing and examination was carried out in a laboratory, and focused on potentiometers of the type used on the incident RRV.

130 Four potentiometers were available for this testing:

1. One removed from an identical machine from Hydrex's Bristol depot, which had operated for 236 hours, fewer hours than the incident machine;
2. The front end potentiometer from the incident machine (which had operated for 1331 hours);
3. The rear end potentiometer from the incident machine (1331 hours); and
4. One removed from an identical machine from Hydrex's Salsburgh (Scotland) depot, which had operated for 1311 hours.

131 All of the four potentiometers removed were of the same sealed unit type. Each potentiometer contains two wipers that 'sweep' over separate semi-circular tracks to vary the resistance in the electrical circuit. Each wiper (which is 0.7 mm wide) is made up of 10 separate contact fingers which may individually move as the wiper moves around the track (figure 10).

132 The first three potentiometers were swept over their working range to check if any disturbances in the resistance could be detected. No anomalies in the resistances measured were found.

133 This was not done for the fourth potentiometer, so that there was an example that had not been swept (during the tests), for comparison during the internal inspection.

134 All four potentiometers were opened up and examined for signs of any damage or debris. Detailed photographs of this process were taken.

135 The swept areas of all the potentiometers were clearly defined, and marks could be seen where the potentiometer wipers had rested. All the potentiometer tracks showed two marks close to one end of the travel, and one mark at the other end. It was concluded that these corresponded to the full and automatic squash positions at one end, and the fully raised position at the other end (figure 10).

136 In the third potentiometer (which was from the rear end of the incident machine), a loose fibre was observed on the swept area of the potentiometer track (figure 10).

137 A dark fibre was also observed on the fourth potentiometer, but this was clear of the swept area, and did not appear to be loose.

138 The fibre found in the rear (third) potentiometer was 0.01 mm in diameter and 2.28 mm long (figure 10). It is possible that a fibre of this size could have been trapped under one (or part of one) of the wipers and created a resistive fault in the electrical circuit.

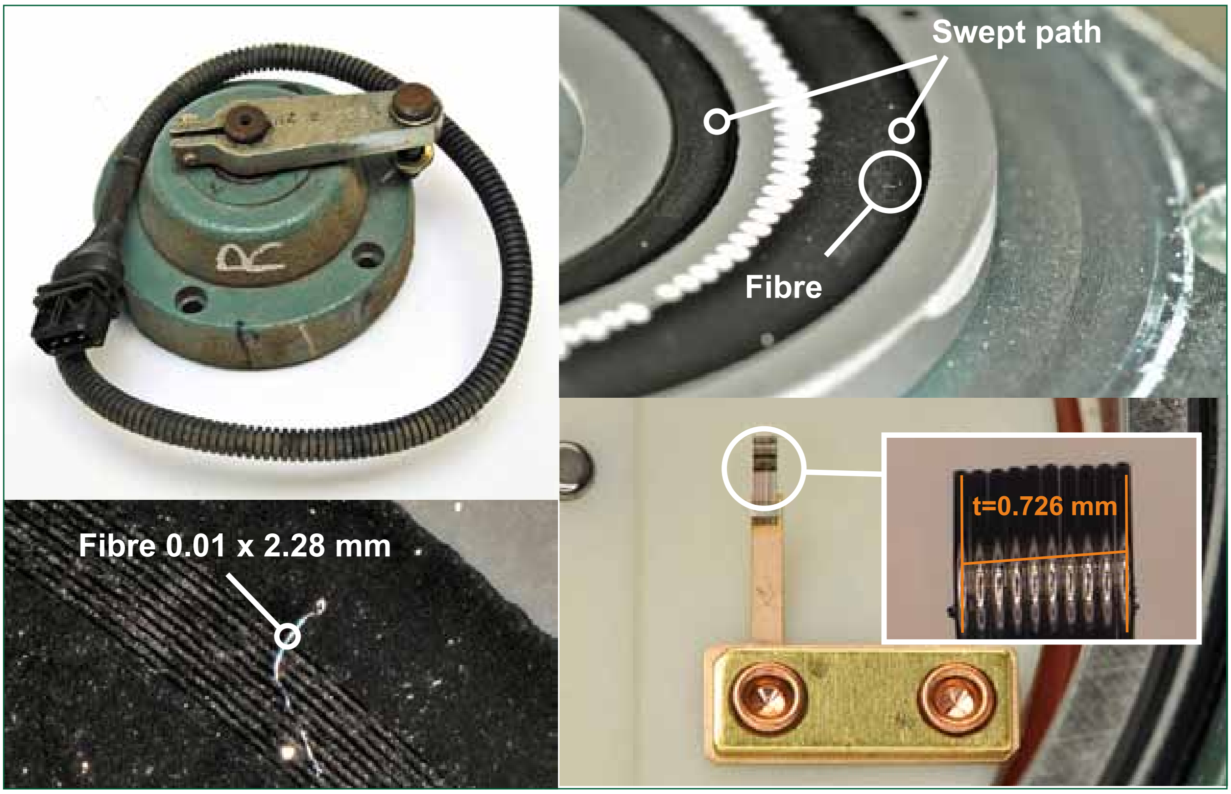


Figure 10: Photographs (clockwise from top left) of the 'third' potentiometer, swept path, wiper arrangement and track and fibre (with dimensions in millimetres)

139 The RAIB undertook testing with the third potentiometer using various fibres of a similar size to the one that was found in it. The RAIB found that it was possible to change the resistive output of the potentiometer (and on occasions obtain an open circuit) by the introduction of different fibres across the swept path, under the wiper. The RAIB did not carry out tests with the fibre that was found in potentiometer number three, because its small size meant that it was impractical to place the fibre in position under the wiper. Although a fibre of the dimensions of that found is unlikely to have interfered with the operation of the potentiometer, testing with other fibres has shown the potential for contaminants in the potentiometer to give rise to a single point failure of the control system.

Overview of test and examination findings

140 None of the tests carried out by the RAIB showed the presence of an electrical fault, suggesting that, if any such fault existed during the on-tracking before the accident, it was transitory.

141 The RAIB has concluded that a single electrical component fault could bypass the control system interlock function, allowing one set of rail wheels to be raised or lowered even if the other end was neither fully raised nor fully lowered. This could allow the RRV to become unbraked.

142 This failure scenario could arise because of a fault on a potentiometer, such as a high resistance spot on the wiper (eg as a result of contamination, or corrosion) or because of a loose or contaminated connection in a connector. Such a fault can cause a change in the output voltage, which is ‘read’ by the control system computer, leading the system to behave as if the wheels are in a different position from where they really are. For example, if the wheels at one end are partly lowered, the computer may detect them as being fully lowered. This means that the interlock would no longer prevent movement of the other rail wheels, allowing the machine to enter a free-wheel state. It is also possible for such a fault to release the opposite end interlock function, without initiating a potentiometer fault alarm.

143 Figure 11 shows the relationship between the input voltage (as seen by the control system) and the road/rail wheel air gap, for the rear wheels of the accident RRV.

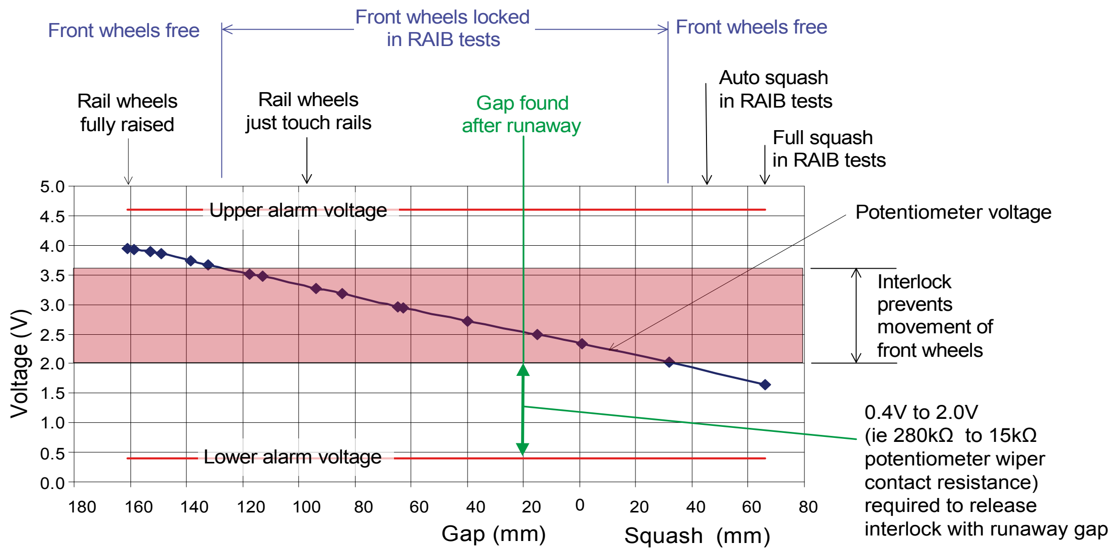


Figure 11: Graph showing relationship between voltage and road/rail wheel air gap

144 The green arrow represents the range of voltage values (0.4 to 2.0V) at the input to the control system that will cause a release of the interlock function (allowing the raising or lowering of the other end rail wheels), despite the existence of a 20 mm air gap. Additionally, no fault alarm will be generated by the control system. A range of wiper resistance values (between 280 kΩ and 15 kΩ) will cause this control voltage to move from the red shaded 'interlock area' (figure 11) to within the green arrow area (non-interlock area – rail wheels free to move).

145 The evidence suggests that the RRV control system did not prevent the machine getting into an unbraked condition. This is likely to have been as a result of a single point failure. This most probably occurred in the form of a change in the electrical resistance, possibly in the rear potentiometer or in the circuit associated with the rear potentiometer and control system (paragraph 139). The design of the RRV control system was therefore a causal factor in the accident.

The layout of the cab controls

146 **The labelling of the selection buttons on the rail (ZW) control panel had the potential to confuse the machine operator. This was a possible causal factor.**

147 The probable actions of the machine operator during the on-tracking of the RRV on 20 July are described in paragraph 163 and figure 13.

148 The damage to the RRAP (figure 12) indicates that it is likely that the operator made several mistakes in incorrectly selecting the front or rear chassis before operating the controls to raise or lower them. On the rail (ZW) control panel, the front chassis lock button is labelled 'VA' and the rear chassis lock button is labelled 'HA' (figure 13). These labels are abbreviations of the German translation of front and rear.

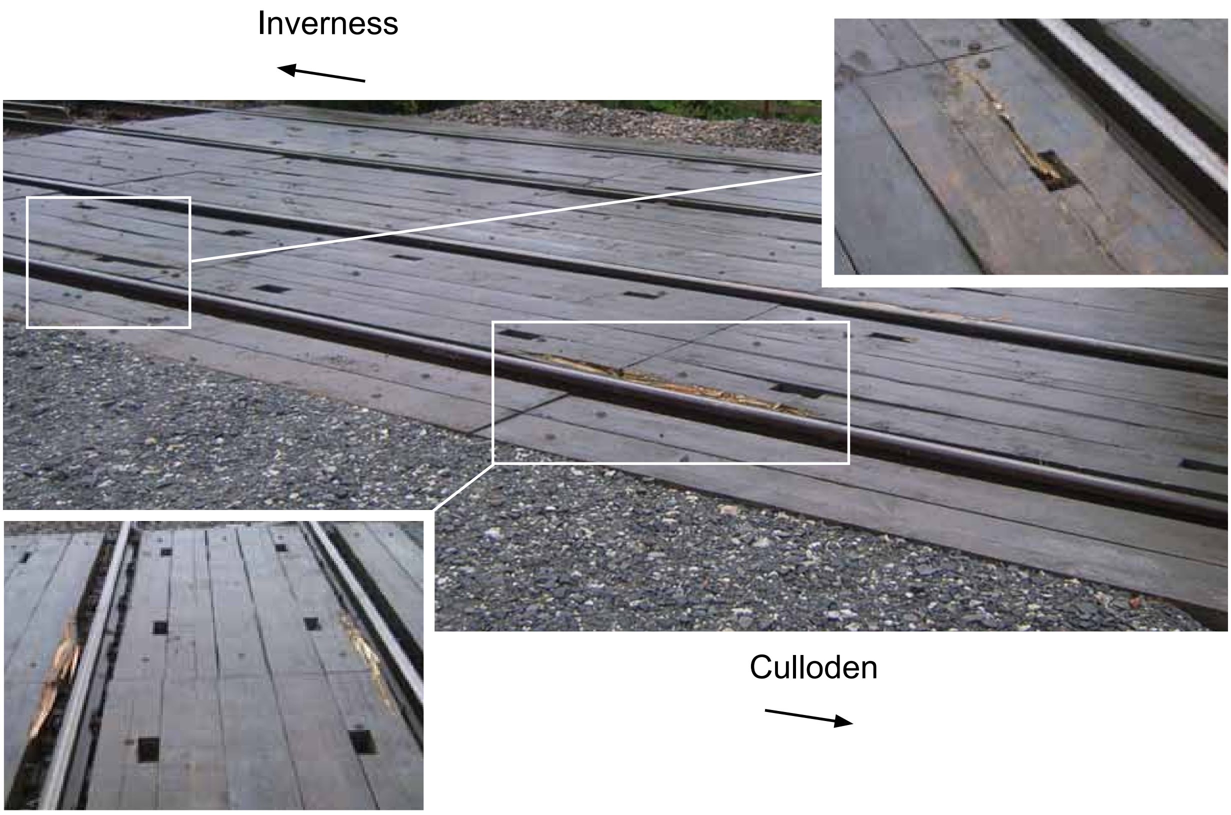


Figure 12: Detailed pictures of damage to Drumrosach RRAP

149 If the VA (front) button is depressed, this action locks the front rail chassis and allows the rear rail wheels to be raised or lowered as required (if the interlock function permits this). In addition, an indicator light on the VA button illuminates. In order to unlock the front rail chassis, the same button is pressed again and the indicator light extinguishes. The HA (rear) button operates in the same fashion, but locks and unlocks the rear rail chassis.

150 Once the operator has locked a front or rear chassis and the respective lock button is illuminated (only one end can be selected at a time), the next step is to press either the 'raise' or 'lower' buttons to command the other rail chassis to move (figure 13). The design of the controls therefore requires the operator to depress the front (VA) button, if he wishes to move the rear rail wheels, and vice versa with the rear (HA) button and the front wheels. The operation of selecting one end in order to move the other end is potentially confusing. This adds to the complication of the buttons being labelled with the letters 'VA' or 'HA' for front and rear. Furthermore, the cab and boom arm are able to rotate through 360°, also making it possible that the operator may become confused between the front and rear of the machine.

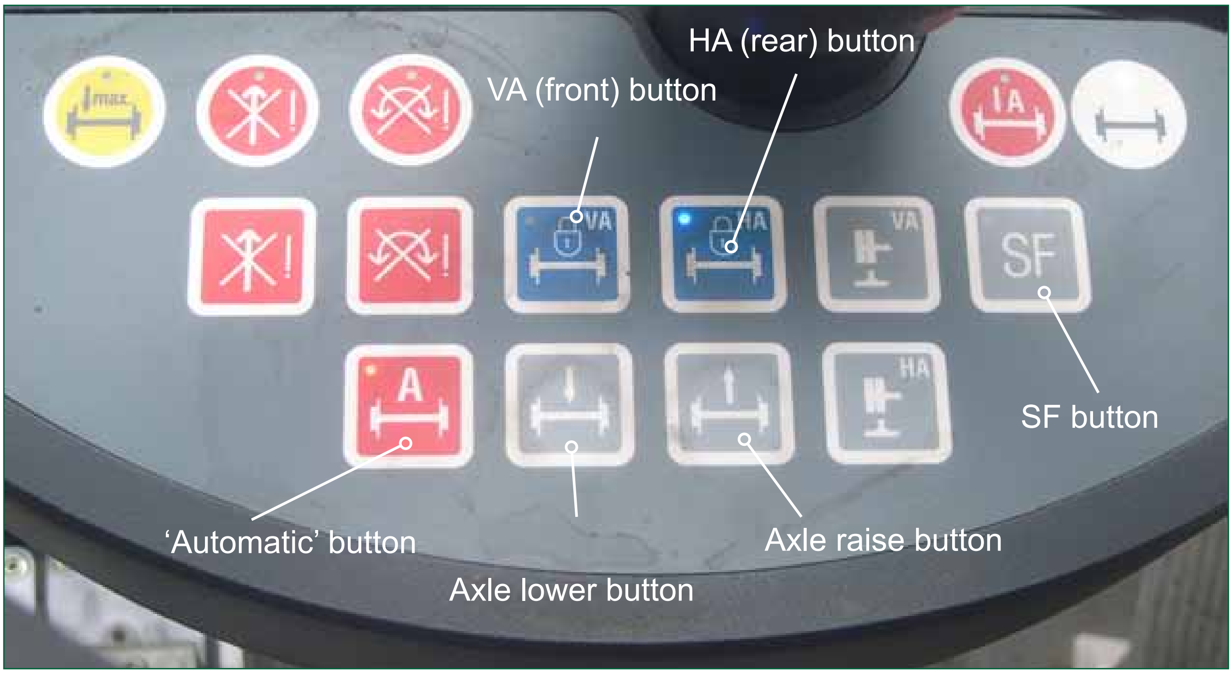


Fig 13: Rail (ZW) control panel indicating axle operation buttons

151 Had the lock buttons been correctly selected, and then operated by the machine operator in the correct sequence, he might have realised that there was a problem with the machine before deploying his front end rail wheels (figure 14 [step k]). The design of the human-machine interface may have confused the operator, and was therefore a possible causal factor in the accident.

Locked rail controls

152 The machine operator was unable to raise the rail wheels at either end of the RRV to lower the machine down onto its road wheels, or lower the rail wheels to engage with the road wheels (to slow, derail or stop it). This was a causal factor.

153 The testing undertaken by the RAIB (paragraphs 116 to 128) showed that the RRV control system computer continuously monitors the position of the rail chassis, and indicates whether each rail wheel axle is in an unbraked condition. Consequently, it can detect when both rail wheels are simultaneously in an unbraked condition. However, the control system is designed such that the control logic is the same whether one or both sets of wheels are unbraked. This means that when the control system detects that both wheel sets are unbraked, the interlock prevents either wheelset from being raised or lowered. This means that the machine operator is then unable to raise the rail wheels (to bring the road wheels into contact with the ground) or lower the rail wheels (to bring them into contact with the road wheels). The operator is therefore unable to recover from a potentially dangerous situation.

154 The RRV was originally designed to be equipped with a Special Function (SF) button that, when operated, would override the interlock function and allow the operator to raise or lower both front and rear rail wheels as required. This button had been disabled in the control system software, version 4.3, installed on the RRV involved in the accident.

155 Had the SF button been enabled in the RRV involved in the accident, it could have been used to override the interlock function.

156 All type 1033 RRVs (as used by the three UK companies that own them) had version 4.3 software installed at the time of the accident. When the machines were first sold by Liebherr in May 2009, 10 machines (from a total of 41) had been operating with the SF button enabled. By November 2009, the 10 original machines had been changed to version 4.3, and the SF button had been disabled.

157 Hydrex had requested that Liebherr disable the SF button during Hydrex's customer acceptance of the machines in 2009. Hydrex was concerned that the button could be deliberately or inadvertently used by operators to create an unsafe free-wheel state. Liebherr undertook the change to the software (to disable the function of the SF button) and produced version 4.3.

158 No formal risk assessment of the removal of the function was undertaken and Liebherr did not give any formal technical, operational or safety risk advice to Hydrex on the subject.

159 The RRVs computer control system can be accessed with a special electronic device known as an 'engineer's key'. When inserted into the machine's operating panel, this allows the user to modify software values, change certain operational parameters and also to override the interlock function.

160 Engineer's keys are only issued to Liebherr engineering staff, and not to machine operators or controllers. Hydrex (Scotland depot) had requested that Liebherr provide an engineer's key for the use of its maintenance staff, but Liebherr had not agreed to this.

161 Both the witness and technical evidence strongly suggests that the machine operator involved in the accident did not have access to an engineer's key. If an engineer's key had been used to override the interlock, the machine operator could, when the machine began to run away, have raised the rail wheels to lower the machine onto its road wheels, or moved the rail wheels to bring them into contact with the road wheels (paragraph 58).

162 The machine's rail controls were locked, although the control system could sense that both axles were in an unbraked condition. The fact that the operator was unable to raise or lower the rail wheels in these circumstances to stop the machine was a causal factor.

The road-rail vehicle – summary of findings

163 The following conclusions are derived from the evidence presented at paragraphs 105 to 162:

1. The runaway was not caused by a mechanical failure, low adhesion or incorrect tyres.
2. There is no evidence of a software error.
3. The interlock function did not operate as designed and this permitted the machine to be inadvertently placed in a free-wheel condition by the machine operator.
4. Although no electrical fault was identified during testing, it is likely that a transitory high resistance possibly due to the fibre within the potentiometer or the associated electrical circuit (paragraph 129) allowed a set of rail wheels to be lowered when the opposite set was unbraked.
5. It is likely that the disappearance of the high resistance condition caused the interlock function to prevent the machine operator moving either wheel set into a braked condition.

Given the above, it has been possible to identify a single sequence of events that most closely matches the evidence available and results in a runaway of this type[20]. This sequence is shown in figure 14.

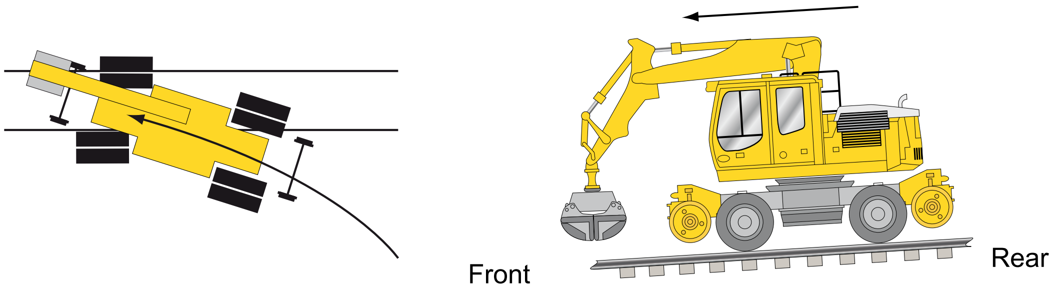


Figure 14 a/b - Rail mode is selected on the ZW box. The RRV is driven onto the RRAP front end first. The machine controller is not present. The RRAP is on a 1 in 50 max gradient

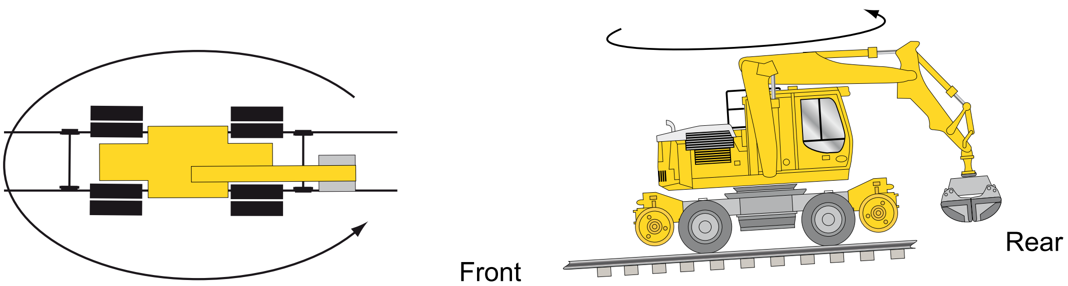


Figure 14 c/d - The cab is swung to the rear of the RRV. The machine operator believes that the rear rail wheels are in line with the track: they are not.

[20] The RRV was on-tracked with all road and rail controls correctly set in line with the on-tracking machine instructions and procedures.

Figure 14e - The machine operator lowers the front rail wheels by mistake. He stops lowering when he feels the front end lift up. Damage is caused to the RRAP (figure 12).

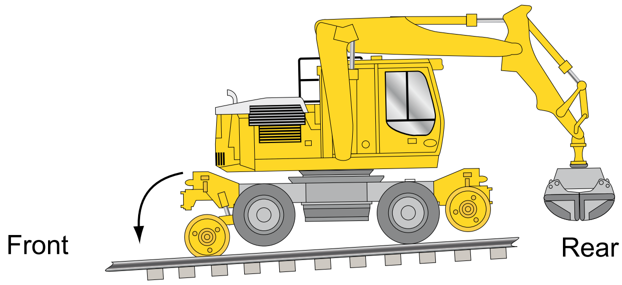


Figure 14 f - The machine operator raises the front rail wheels fully up and manoeuvres the RRV forward and backwards to re-align the rear rail wheels.

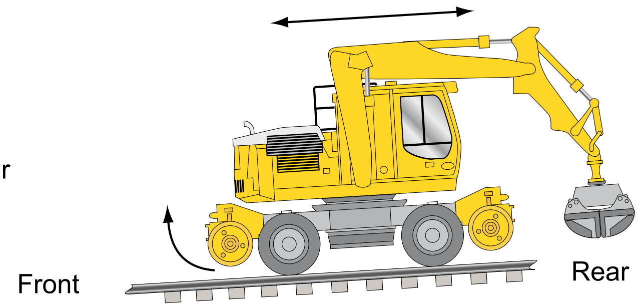
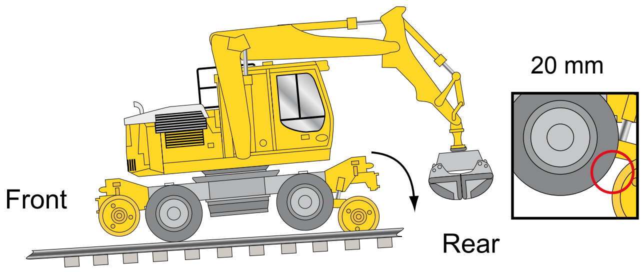


Figure 14 g - The machine operator believes that the rear rail wheels are now in line with the track. They are still not. The machine operator lowers the rear rail wheels onto the RRAP surface causing damage (figure 12). A gap of about 20 mm (inset) (paragraph 106) is left by the machine operator between the rear road and rail wheels (in accordance with the normal process during on-tracking).



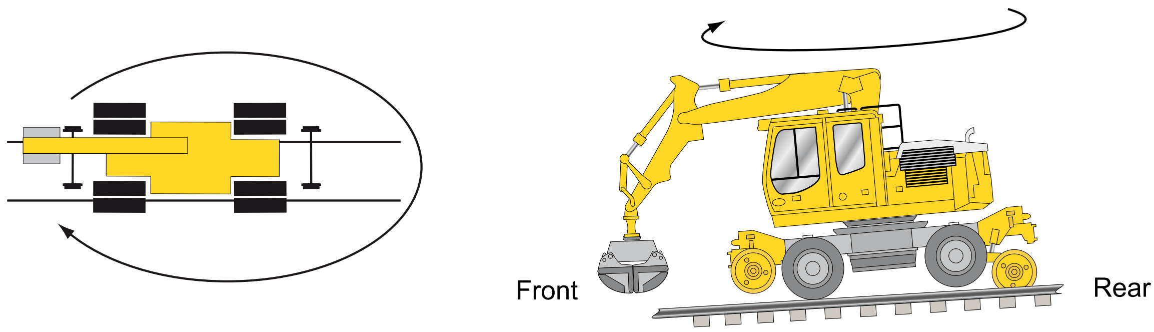


Figure 14 h - i - The machine operator swings the cab to the front of the RRV

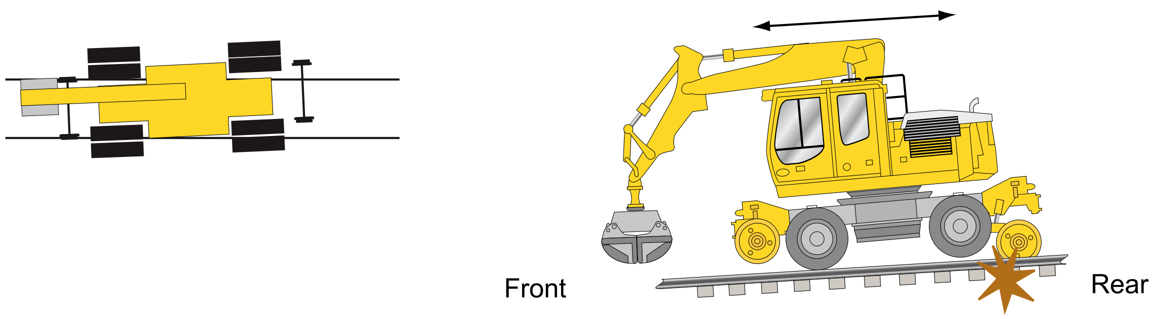


Figure 14 j - k - The machine operator manoeuvres the RRV forwards and backwards to line up the front rail wheels. This causes further damage to the RRAP at the uphill end. A resistance fault occurs to the rear potentiometer or circuit. The new voltage allows the computer system to release the front rail wheels despite the existence of the 20 mm air gap between the rear road and rail wheels. The machine operator does not complete the lowering of the rear rail wheels at this time because he selects the front chassis by mistake and the front wheels move.

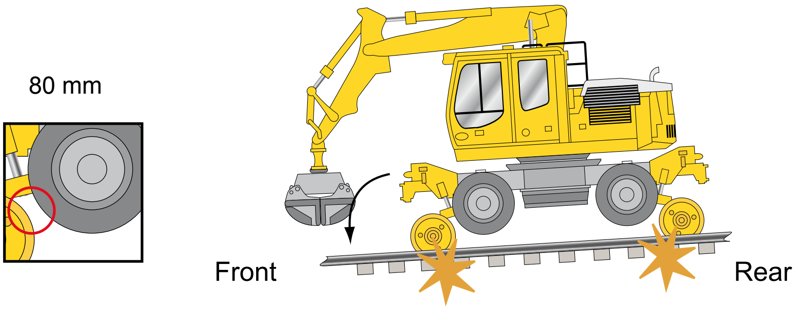


Figure 14 l - The machine operator begins to lower the front rail wheels (they move because of the presence of the electrical fault). However, the disturbance to the rear chassis caused by this movement results in the electrical fault disappearing and the interlock is automatically reinstated (paragraph 128). Consequently the front rail wheels now stop moving with approx 80 mm gap (inset) (paragraph 106) and the machine operator thinks that the rail wheels are fully down. The RRV's rail controls are now locked and the machine is in a free-wheel state.

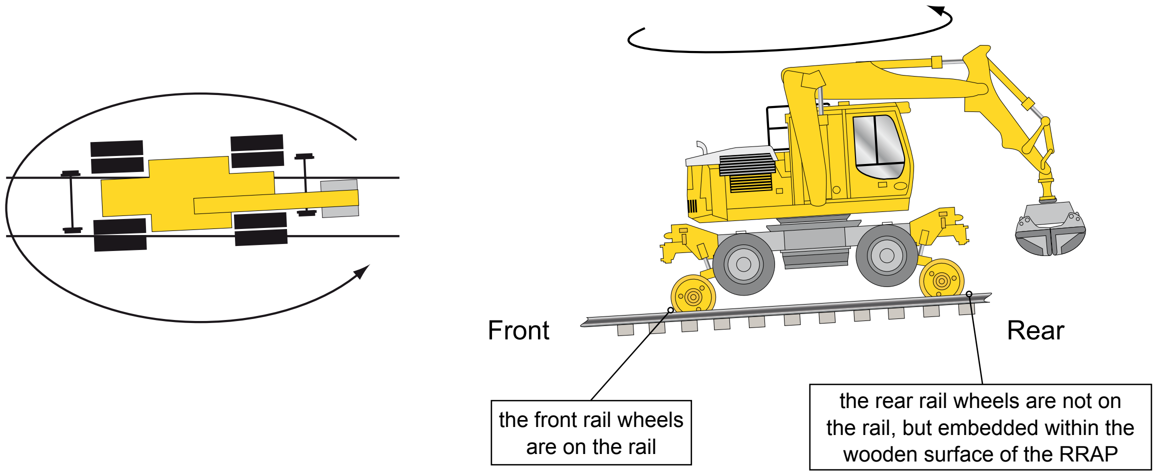


Figure 14 m - n - The machine controller arrives at the RRAP and tells the machine operator that the RRV rear axle wheels are not on the track, but in the wooden surface. The machine operator swings the cab to the rear of the RRV.

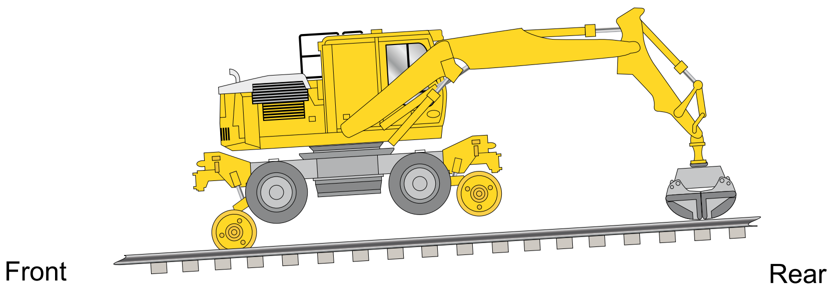


Figure 14 o - The machine operator lowers his boom arm and clam bucket onto the sleepers in the area between the running rails of the down line (at the rear end of the RRV). This lifts the RRV up and the rear rail wheels are then placed onto the track.

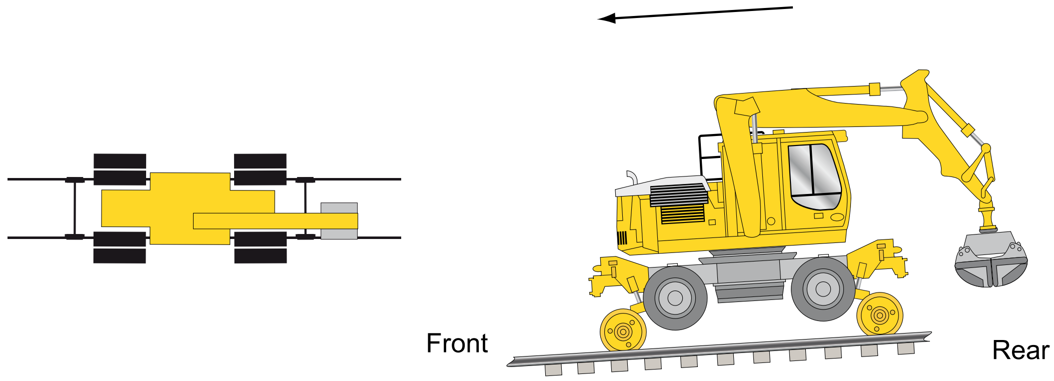


Figure 14 p - q - The RRV begins to run away as it is in a free-wheeled state and on the track.

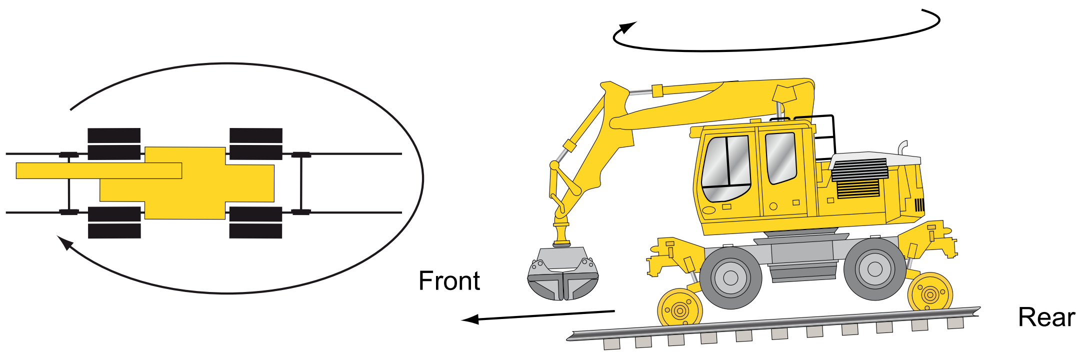


Figure 14 r - s - The machine operator quickly swings the cab to the front of the RRV (in the direction of travel).

Fig 14 a - s: High-ride RRV - the on-tracking sequence of events at Drumrosach on 20 July 2010

On-tracking of the RRV – actions of the staff involved

The machine operator carried out a sequence of actions that resulted in the RRV being in a free-wheel condition during on-tracking.

164 **If the machine operator had checked for squash during each stage of the on-tracking process, he is likely to have noticed that one set of rail wheels was not in squash against its respective road wheels (and un-braked), before trying to deploy the other set of rail wheels. This was a causal factor.**

165 The machine operator did not check for squash during the on-tracking process by slewing his machine across the tracks (as recommended by Liebherr in their operating manual). Slewing of a machine during on-tracking is not considered as good industry practice, because of the potential instability of the machine. It is not possible for him to obtain a clear view of the road and rail wheel interface from the operator's cab. He was trained not to leave his cab at this time, because of the risk of injury from falling out of the machine when it was not horizontal.

166 The machine operator made a sequence of errors during the on-tracking sequence at the RRAP, and the machine allowed the movements to occur. The operator then violated the machine's operating procedures by using the boom arm to finally position the machine onto the rails. In addition, the operation and sequence of the axle lock, raise and lower buttons were also factors. This is discussed in paragraphs 146 to 151.

167 The operator believed that the machine's interlock function was infallible (as did his employer, Hydrex) and this had been trained to all operators. This perception may have been at least partly based on the fact that Liebherr's operating manual can be interpreted as stating that both sets of rail wheels cannot be deployed simultaneously. The manual also did not specifically require the operator to visually check for squash during on-tracking.

The machine controller was not present when the RRV began on-tracking.

168 **If the machine controller had been at the RRAP when the RRV began to on-track, he might have noticed that one end of the RRV was not in squash (before the operator started to lower the rail wheels at the other end). This was a possible causal factor.**

169 The Network Rail on-tracking standard, NR/L2/RMVP/0206 issue 1 section 6.4.2, states that the machine controller (and operator) shall be present at the RRAP during the on-tracking process.

170 Network Rail's RRV training module 2 (session 5) for machine controllers includes training in the on-tracking process, particularly 'instructions for raising, lowering and alignment of rail wheels'. The training encompasses both theory and a practical demonstration of undertaking the on- (and off-) tracking process.

171 The machine controller involved in the on-tracking of the RRV at Raigmore had undergone this training (paragraph 97) and was aware of his responsibility to assist the operator in lining up the rail wheels of the RRV with the running rails. He did not regard it as part of his duties to check the road and rail wheels for the correct engagement, or amount of squash, and this was not included in the training module.

172 The machine controller and the operator had worked together on a number of occasions before the day of the accident and the controller had witnessed the operator on-tracking successfully at these times. The controller stated he had no cause to doubt the operator's skill and ability to on-track the machine in his absence.

173 The RRV had been a late addition to the work. When the work had been planned for 20 July, there had been no RRV booked and the machine controller was only to have acted as PICOP, ES and COSS for the shift. When the RRV became available, his competencies allowed him to work as machine controller with the RRV, in addition to his other roles. Consequently no additional Network Rail employee was booked to undertake the RRV machine controller role.

174 On 20 July, the machine controller gave the operator permission to begin on-tracking the RRV in his absence. While the RRV drove towards the RRAP, the machine controller completed his PICOP, ES and COSS paperwork, intending to join the operator at the RRAP as soon as possible to assist in the on-tracking process. The controller arrived at the RRAP, two minutes after the RRV had started on-tracking.

175 When the machine controller arrived at the RRAP, the machine was in a free-wheel state at both ends, but he was unaware of this, although he could see that the rear end rail wheels were sitting on the wooden surface of the RRAP. At this end of the machine, the air gap between the road and rail wheels was 20 mm. Since the machine controller was not seeking to check for squash, it is very unlikely that he would have noticed this gap, especially since the crossing was dark and there was no artificial lighting present other than the lights on the RRV.

176 It is possible that had the machine controller been at the RRAP, when the RRV began on-tracking, he might have noticed that one end was not in squash when the wheels at the other end were moved by the operator. He might then have stopped the movement of the RRV and thus prevented the run away from occurring. However, observation of squash was not part of the machine controller's duties, and the lack of lighting at the RRAP made observation of the road/rail wheel interface very difficult.

The inability to stop the runaway by using the attached bucket

177 **The machine operator was unsuccessful in using the clam shell bucket (attached to the RRV boom and dipper arm) to slow, derail or stop the RRV. This was a causal factor.**

178 The RRV involved in the accident had a small clam shell bucket connected to the dipper arm through a flexible connection (paragraph 36).

179 Hydrex machine operators receive emergency training for RRV runaway situations, and the operator involved in this accident had received training in the theory of using the boom arm to stop a runaway machine. However, the training did not include any practical experience. The operator had over sixteen years experience in operating RRVs, but he had not previously been involved in a runaway of an RRV.

180 As the RRV began to move, the operator swung the cab (and boom arm) to face ahead of the machine, ie in the direction of travel. It is believed that the machine travelled with the boom arm ahead of it until just before the collision.

181 If the machine operator had moved the boom arm down towards the ground in a forceful manner while the RRV was still moving slowly, he might have caused greater damage to the infrastructure, but would have prevented the subsequent collision. As the RRV continued to free-wheel downhill on the 1 in 60 gradient, its speed increased and the effect of forcing the bucket on the ground would have decreased.

182 The fact that the machine operator was unsuccessful in using the clam shell bucket to slow, derail or stop the RRV was a causal factor in the accident, but the possible adverse consequences of using the boom arm in this way (which includes derailment and overturning of the machine) mean that the RAIB makes no recommendations in this area.

Identification of underlying factors[21]

183 The RAIB identified one underlying factor. This was:

184 **The design process and approvals process of the RRV did not deal with the potential for the single point failure mode or the potential for both sets of RRV rail wheels to become 'locked' in the free-wheel state.**

[21] Any factors associated with the overall management systems, organisational arrangements or the regulatory structure.

185 Liebherr has also been unable to produce any evidence of system risk assessment or detailed design validation for the RRV interlock function or the removal of the SF button. It has also been unable to produce evidence of a software functional specification for the design of the software of the RRV rail control system.

186 However, Liebherr has produced a *Failure Modes and Effects Analysis* (FMEA) document for the design of the software in the RRV (version 4.3, which was installed on the machine involved in the accident). This was produced post accident and dated October 2010. This document lists two failure modes (during on-tracking on a gradient) for the potentiometer and a likelihood of occurrence:

- 'when RRV in upper or lower position (machine correctly on rail or with rubber tyre on ground) – no danger'; and
- 'during raising/lowering of rail gear onto rail – failure of potentiometer possible, but occurrence low'.

187 The 'preventions' of the risk identified in the second of these bullet points were listed in the documents as:

- 'guiding by second operator;
- rotating of upper carriage – the rail gear can be seen;
- movement of rail gear to end lock position; and
- lowering of boom arm and stick (attachment) to the ground.'

188 All of the above 'preventions' are based on the assumption that the operator will continue to operate the rail chassis he was originally moving when the failure occurred. Rotating the upper part of the machine to give the operator a view of the squash is not feasible because of the instability of the machine while one end is raised and the other lowered (and is not considered good industry practice), and 'movement of rail gear to end lock position' (implying that the rail chassis moves through its full travel) may not occur if an electrical failure occurs during the movement.

189 The FMEA document does not list any failure mode(s) in connection with the lock up of the rail controls when both sets of rail wheels become unbraked (paragraph 153). No other documents were produced by Liebherr to show evidence of consideration of this failure mode.

190 The VAB (paragraph 19) did not validate, analyse, check or test the type 1033 RRV to uncover any possible 'hidden' failures. The VAB tests are functional checks of the RRV against the standard RIS 1530-PLT issue 1. The VAB made the assumption that all software validation and testing had been independently assessed by the manufacturer's 'assessor' in Germany.

191 The VAB was aware that the SF button had been disabled on the machine and did not re-test the machine after the software change had been made.

192 Network Rail believed that the VAB undertakes some validation of design documentation including FMEAs and *Hazard and Operability Studies* (HAZOPs) in connection with software design. It also believed that the VAB tests the machine's software. As stated in paragraph 190, the VAB tests are in fact purely functional type tests against the RIS 1530-PLT standard.

193 The design of the machine's control system by Liebherr was not to a 'safety integrity level' (SIL) as defined in the international standard BS EN 61508, 'Functional safety of electrical/electronic/programmable electronic safety-related systems'. Within the safety standard, four SILs are defined, with SIL 4 being the highest integrity and SIL 1 being the lowest. However, no SIL was specified by the relevant Network Rail standards when the machine was procured.

194 Given the fact that the process as applied did not detect the potential weakness of aspects of the design, there is a need for Liebherr and Network Rail to review the adequacy of the design (in terms of SIL) and approval processes for on-track plant such as RRVs. Such a review should assess the degree to which the existing processes are capable of checking that adequate engineering safety management systems and techniques have been applied to the specification, design and testing for new equipment[22].

195 The lack of consideration of credible faults in the design, safety validation and approval process for the RRV was an underlying factor in the accident.

Previous occurrences of a similar character

196 There have been a number of RRV runaways on Network Rail infrastructure in the last five years, but none have involved machines with a software-based control system.

197 The RAIB has investigated the majority of these RRV runaways, and has made recommendations. Those recommendations relevant to this investigation are summarised below. Full details of each recommendation and the actions reported to have been taken are shown in appendix C.

198 The RAIB undertook a class investigation on the subject of RRV runaways. The report, 'Investigation into runaways of road-rail vehicles and their trailers on Network Rail' (report 27/2009) was issued in October 2009. Recommendation 1 was that Network Rail should manage the specification, design, operation and maintenance of RRVs using a systems engineering process, incorporating formal safety analysis methods. Recommendation 2 addressed the assessment of the safety of operation of RRVs with the objective of reducing risk of runaways and collisions. The text of this recommendation and the actions that the RAIB has been advised have been taken in response to it can be found in appendix C.

199 Two RRV runaway accidents occurred at Brentwood, Essex, and at Birmingham Snow Hill on 4 November and 31 October 2007 respectively, and were the subject of RAIB report 11/2009. Recommendation 3 addressed the training of machine controllers, including control measures to prevent an unbraked condition, and their interface with machine operators during on- and off-tracking. Recommendation 4 addressed the training for machine controllers and their specific duties during on- and off-tracking.

[22] Current good industry practice is contained in Engineering Safety Management (the 'Yellow Book'), issue 4.0.

Observations[23]

The machine operator

200 The operator involved in the accident had not recorded the shifts he had worked in either of his two log books since June 2010 (paragraph 92) despite working many shifts. It is a Network Rail requirement that operators complete a log book for their competence assessments and records.

The machine controller

201 The Network Rail machine controller involved in the accident was not able to supply his current log book for examination as part of this investigation, despite working many shifts as a machine controller (paragraph 98). It is a Network Rail requirement that controllers complete and keep their log book for their competence assessments and records.

202 The machine controller had completed a Machine Site Arrival Check list (paragraph 51) as part of his pre-shift duties, and before the RRV was given permission to on-track. Although every entry in the check list had been ticked as 'yes', it would have been impossible for the operator to have undertaken certain checks, such as the brake test, and for the controller to have witnessed those before the RRV was on-tracked and ran away.

[23] An element discovered as part of the investigation that did not have a direct or indirect effect on the outcome of the accident but does deserve scrutiny.

Summary of Conclusions

Immediate cause

203 The immediate cause of the accident was that the road-rail vehicle ran away from the RRAP in an unbraked condition on a downhill gradient (**paragraph 102**).

Causal factors

204 The causal factors were:

a. the RRV was placed into an unbraked condition. This is likely to have been as a result of a combination of operator actions and a single point failure of the control system (**paragraph 105, Recommendation 1**);

b. the machine operator carried out a number of actions, following which the machine was on the track in an unbraked condition (**paragraph 164, no recommendation, paragraph 213**);

c. the machine operator was unable to raise the rail axles/wheels at either end of the RRV to lower the machine down onto its road wheels, or lower the rail axles to engage with the road wheels (to slow, derail or stop it) (**paragraph 152, Recommendation 1**); and

d. the machine operator was unsuccessful in using the clam shell bucket (attached to the RRV boom and dipper arm) to slow, derail or stop the RRV (**paragraph 177, no recommendation**).

205 It is possible that the following factors were causal:

a. the design of the human-machine interface, particularly the labelling of the axle selection buttons on the rail (ZW) control panel, had the potential to confuse the machine operator (**paragraph 146, Recommendation 2**); and

b. if the machine controller had been at the RRAP when the RRV began to on-track, he may have noticed that one end of the RRV was not in squash (before the operator was able to operate the rail axle at the other end) (**paragraph 168, Recommendation 4**).

Underlying factor

206 An underlying factor was that the design process and approvals process of the RRV did not identify the potential for the single point failure mode or the potential for the RRV rail axles to become 'locked' in the free-wheel state (**paragraph 184, Recommendation 3**).

Actions reported as already taken or in progress relevant to this report

Network Rail

207 On 21 July 2010, Network Rail suspended the use of all the type 1033 RRVs from operating on its infrastructure and issued an 'Infrastructure Safety Bulletin' to its staff and contractors detailing this action.

208 Network Rail has undertaken testing of type 1033 RRVs (which include new rail control system software installed by Liebherr – paragraph 210). Network Rail has also produced a technical paper entitled, 'Reintroduction of RRVs for consultation with the ORR'. This is a working document, and at the time of publication of this report, was still under revision.

209 Network Rail has also requested Liebherr, in co-operation with the owners of the type 1033 excavators, to install a security type tag to inhibit unauthorised access for the use of the engineer's key, and to install manufacturer specified tyres on all machines.

Liebherr

210 Liebherr has modified the rail control system software and is considering the use of a secondary rail chassis position sensor to provide dual redundancy and mitigate against the single point failure of the potentiometer.

211 The new software will, when an open (or short) circuit is detected in a potentiometer circuit, give an audible warning to the operator, raise error code alarms, flash a white light on the rail (ZW) control box and stop any rail chassis movement and any transmission drive movement. However, if a resistive type failure occurs in the potentiometer circuit or the RRV is in a 'lock up' free-wheel state, the machine will behave as version 4.3 of the software (as was installed on the machine involved in the accident). No other changes to the 'lock up' scenario/free-wheel state have been made.

212 Liebherr has also written an addendum to the type 1033 operating manual, making it a requirement that either the operator or controller should visually check that each set of rail wheels is fully deployed before the other end is operated.

213 Immediately after the accident, Hydrex quarantined its fleet of type 1033 RRV machines from use and advised Network Rail (and other owners) of this.

Hydrex

214 Hydrex has re-briefed its machine operators about the need to test for tyre squash once on-tracked, and the need to check tyre pressures. Hydrex has also written and issued a tyre policy and has continued to fit visual tyre pressure indicators on its fleet.

215 Hydrex has also re-briefed its maintenance staff to remind them to include a check for the correct squash values at the 6 monthly maintenance activity of each RRV.

Recommendations

216 The following recommendations are made[24]:

Recommendations to address causal, contributory, and underlying factors

1 *The intention of this recommendation is that RRVs of the type involved in the accident should be modified to prevent the circumstances arising in the future.*

Liebherr-Great Britain Ltd should undertake modifications to the type 1033, and similar RRVs (those RRVs with this type of interlocking design), to avoid the scenario where a machine that is in a free-wheel state is prevented from raising or lowering either rail axle. This should be achieved without the need for the machine operator to override the interlock function (paragraphs 204a, 204c).

2 *The intention of this recommendation is to improve the ergonomics and labelling of the RRV controls.*

Liebherr-Great Britain Ltd should undertake a review of the design of the human-machine interface on the type 1033, with particular reference to:

- ergonomics/labelling of buttons; and
- counter-intuitive operating procedures and specific operation of the HA and VA controls in the RRV machine cab;

and implement the findings of this review on existing machines, and amend its procedures to require an ergonomic assessment to be included in the design process (paragraph 205a).

continued

[24] Those identified in the recommendations, have a general and ongoing obligation to comply with health and safety legislation and need to take these recommendations into account in ensuring the safety of their employees and others.

Additionally, for the purposes of regulation 12(1) of the Railways (Accident Investigation and Reporting) Regulations 2005, these recommendations are addressed to the Office of Rail Regulation to enable it to carry out its duties under regulation 12(2) to:

(a) ensure that recommendations are duly considered and where appropriate acted upon; and

(b) report back to RAIB details of any implementation measures, or the reasons why no implementation measures are being taken.

Copies of both the regulations and the accompanying guidance notes (paragraphs 167 to 171) can be found on RAIB's website www.raib.gov.uk.

3 *The intention of this recommendation is that an appropriate safety integrity level (SIL) for the control systems of RRV machines should be established and implemented on future builds.*

Network Rail should undertake a review of the safety requirements that it specifies for RRVs, with the objective of determining an appropriate safety integrity level (SIL) for any safety functions that are required within the control systems of the machine, and implementing verification and approval arrangements that are appropriate for this SIL. This should, among other things, provide assurance that potential failure modes of interlocks, and similar safety systems, have been identified and suitably mitigated (with reference to actions taken following the RAIB's RRV Class Investigation recommendations 1 & 2) (paragraph 206).

4 *The intention of this recommendation is that the role of the machine controller, in respect of the deployment of the rail wheels of an RRV, should be clarified.*

Network Rail should undertake a review of the role of the machine controller for all types of RRV during on and off-tracking, with particular emphasis on whether it is necessary for the controller to advise the machine operator on whether the rail wheels of the RRV are fully deployed (with reference to the RAIB's RRV Class Investigation recommendation 2). This review should take into account the potential for operator error and/or the malfunction of the machine (paragraph 205).

Appendices

Appendix A - Glossary of abbreviations and acronyms

COSS	Controller of site safety
CPCS	Construction plant competence scheme
ES	Engineering supervisor
FMEA	Failure modes and effects analysis
HAZOP	Hazard and operability study
ORR	Office of Rail Regulation
PICOP	Person in charge of possession
RAIB	Rail Accident Investigation Branch
RRAP	Road-rail access point
RRV	Road-rail vehicle
SIL	Safety integrity level
VAB	Vehicle acceptance body

Appendix B - Glossary of terms

All definitions marked with an asterisk, thus (*), have been taken from Ellis's British Railway Engineering Encyclopaedia © Iain Ellis. www.iainellis.com.

Cant	The design amount by which one rail of a track is raised above the other rail, measured over the rail centres.*
Certificate of conformance	Certificate issued by a Vehicle Acceptance Body indicating that a vehicle or item of plant conforms with relevant engineering standards.
Certificate of engineering acceptance	A certificate issued by a Vehicle Acceptance Body that certifies that the rail vehicle meets the required standards and gives any necessary operating restrictions.*
Cess	The space alongside the line or lines.*
Controller of site safety	A Safety Critical qualification demonstrating the holder's competency to arrange a Safe System of Work, ie protecting staff working on the line from approaching trains.*
Detonators	A small disc shaped explosive warning device designed to be placed on the railhead for protection and emergency purposes. It explodes when a train passes over thus alerting the driver.*
Down	The direction towards Inverness, and the name of the track normally used by trains travelling towards Inverness.
Engineering possession	A period of time during which one or more lines are blocked to trains to permit work to be safely carried out on or near the line.*
Engineering supervisor	The person nominated to manage the safe execution of works within an Engineering Worksite.*
Failure mode and effects analysis (FMEA)	A procedure for analysis of potential failure modes within a system for classification by the severity and likelihood of the failures.
Hazard and operability analysis (HAZOP)	A structured and systematic examination of a planned or existing process or operation, in order to identify and evaluate problems that may represent risks to personnel or equipment, or prevent efficient operation.
Holding end	A part of a wheeled vehicle that is braked and provides a means of preventing movement of the vehicle during on- and off-tracking.
Interlock	A mechanical, electrical or software system for preventing conflicting functions.
Machine Controller	A person trained and authorised to control and supervise an item of road rail plant or on-track machine other than a rail crane.*
Machine operator	A person trained and authorised to operate an item of on-track plant or machinery.

Mile post — A coloured (generally yellow, though other colours are used when two different routes run adjacent to one another) post placed at one mile intervals along a railway. Intervening quarter-mile intervals (quarter, half and three quarter) are also similarly marked.*

On- and off-tracking — On-tracking is the act of driving a road-rail vehicle onto the track and placing it in rail mode. The opposite action is off-tracking.*

Person in charge of possession — The competent person nominated to manage:

- the safe and correct establishment of the protection for the possession;
- access to the possession area by Engineering Supervisors (ES);
- the establishment of engineering work sites within the possession;
- the correct removal of the foregoing in reverse sequence, so that the possession is relinquished and the line handed back to the signaller at the due time.*

Possession — A period of time during which one or more lines are blocked to trains to permit work to be safely carried out on or near the line. A possession taken for an agreed period without the facility to run trains in the area during that period until such time as the holder of the possession decides to relinquish it. Currently called a T3 possession *

Possession limit boards — A miniature version of the stop sign used on the roads, denoting the end of an engineering possession.*

Potentiometer — A three-terminal electrical resistor with a sliding contact that forms an adjustable voltage divider.

Protection — The marking of the limits of a portion of line that has been blocked, by detonators on the rail and possession limit boards.

Road-rail vehicle — Any vehicle adapted to operate equally well on road and rail.*

Runner — A wagon provided to deal with a load (ie rails or pipes) or fixed equipment (ie a crane jib) that overhangs the end of another wagon.*

Sentinel scheme — Operated by the National Competency Control Agency (NCCA), Sentinel is the brandname for the competency control system based on photographic identity cards. The cards give details of medical fitness and railway related competencies.*

Sliprings — A system of sliding contacts on circular tracks, used to transfer electrical power and signals between two components that are required to rotate relative to each other.

Squash	The amount of deformation of the pneumatic tyres of the road wheels of an RRV when in contact with the machine's rail wheels.
Up	The direction away from Inverness, and the name of the track normally used by trains travelling in this direction.

Appendix C – Previous recommendations relevant to this investigation

Investigation into runaways of road-rail vehicles and their trailers on Network Rail, RAIB report published October 2009

Recommendation 1

Network Rail should implement a process that manages the specification, design, operation and maintenance of RRVs on its network throughout their system lifecycle. The process should include the following elements:

a) a high level requirements specification of the task;

b) a safety requirement specification, including the application of safety analysis techniques such as Hazops, FMEA and FTA;

c) specifications relating to the plant, the relevant personnel and the applicable procedures;

d) RRV configuration management systems;

e) verification and validation requirements;

f) site inspections and audits of the arrangements; and

g) a change control process.

Status: In progress, with all actions to be completed by 2013.

Recommendation 2

Network Rail should assess the operation of existing RRVs and trailers to satisfy itself, on the basis of a process of structured safety analysis, that there are adequate technical and operational controls to prevent RRVs running away.

The assessment should take account of the factors listed below and consider the reliability of the primary controls identified. It should identify any realistically possible failures of the primary controls, and where these are identified, what emergency control measures (which may be implemented through operator training) should be put in place.

Network Rail should amend their processes as appropriate to implement any improved controls identified.

The factors for consideration should include:

a) the use of trailers that are not fitted with service brakes;

b) for each type of RRV, a specific procedure covering the method of on- and off-tracking;

c) the operation of RRVs without braked rail wheels;

d) the operation of RRVs which rely on an interface between rubber and steel for traction and braking giving rise to extended and unknown braking distances in wet/contaminated conditions and on gradients;

e) the content of operator and machine controller training courses as they relate to:
   - driving on wet and/or contaminated railway lines;
   - the use of the emergency stop button;
   - the awareness of any gradient hazard and its effect on machine operation;
   - the recovery from runaway events; and
   - the measures required to ensure that travel movements are carried out safely;

f) the adequacy of maintenance documentation in relation to the maintenance of the rubber and steel interface, including tyre condition, tyre pressure and the correct adjustment of the rail gear;

g) whether brake lights would reduce the likelihood of collision when RRVs undertake multiple transits in a work site;

h) the location of RRAPs, the arrangements for possessions and work sites and their effect on RRV travel distances;

i) the adequacy and the practicality of the system of pre-use checks of RRVs and trailers;

j) the adequacy of planning processes which should assess the risk of RRV operation on wet and/or contaminated rails, as well as gradients, and include specifically notifying its contractors and suppliers of the possible effect on machine operation and the specific mitigation measures that may be required;

k) the briefing of machine controllers so that they can brief operators about the gradients that RRVs will be working on, the likely effect on machine operation and any required mitigation measures; and

l) the absence of signage at RRAPs and inclusion of information in the sectional appendix stating the gradient of the railway.

Status: In progress, with all actions due to be completed by 2016. Network Rail reports that it has produced a risk assessment that has been shared in draft format with the ORR.

Road-rail vehicle runaway incidents at Brentwood, Essex and at Birmingham Snow Hill, 4 November & 31 October 2007, RAIB report published May 2009

Recommendation 3

Network Rail should enhance the relevant modules of the Sentinel training so that machine controllers:

- are aware that operators need to come to an understanding with any person assisting them with on/off-tracking; and
- understand the control measures that prevent an unbraked condition occurring during on/off-tracking.

Status: In progress. Network Rail has outlined the actions to be taken in response to this recommendation and has recruited a plant process improvement specialist. It has also established a framework for managing the safety related change.

Recommendation 4

Network Rail should enhance the relevant modules of training given as part of the Sentinel machine controller competency scheme so that those persons holding this Sentinel competency are aware of the specific duties they should be competent to perform and any specific tasks, for example assisting the operator with on/off-tracking, that this competency does not cover.

Status: Completed. Network Rail has reported that it has completed a programme to implement actions in response to this recommendation. As part of this, Network Rail has recruited a plant process improvement specialist.

This report is published by the Rail Accident Investigation Branch,
Department for Transport.

Any enquiries about this publication should be sent to:

RAIB
The Wharf
Stores Road
Derby UK
DE21 4BA

Telephone: 01332 253300
Fax: 01332 253301
Email: enquiries@raib.gov.uk
Website: www.raib.gov.uk