Strategy for regulation of health and safety risks – chapter 11: Management of train movements & signalling

Signalling, command and train control systems are fundamental to the safe management of railways because they ensure that trains are spaced safely apart and conflicting moves are avoided.

ORR's strategy for regulating the management of train movements and signalling safety recognises the need for the entire industry to increase its capability in order to secure the greatest benefit from future changes; its focus is to influence industry planning to embrace this challenge.

Our aims are:

For all railway duty holders we will monitor the quality of their investigations of signalling incidents. Train accidents caused by signalling equipment failure fall into the category of low frequency events with the potential for catastrophic consequences. It is therefore essential that railway businesses are alert to the precursors to such catastrophic events. A wrong-side signalling failure – one where the asset does not fail to a safe condition – must be thoroughly investigated so that the root causes are understood and addressed. ORR is mindful of the small but concerning number of wrong-side failures and we will commit proportionate resource to encourage duty holders to manage this risk effectively.

For the mainline railway, we will:

- Monitor and influence the introduction of the Digital Railway – the move to automated traffic management and in-cab train control systems – so that the greatest benefits are realised. This requires improved industry leadership, co-operation and governance as well as engagement with stakeholders in the Department for Transport and European Union.
- Influence the Digital Railway programme so that its rollout manages the risks of transition from old to new systems effectively. This requires effective industry co-operation.
- Continue our active monitoring of Network Rail's move away from individual signalling locations to a small number of railway operating centres (ROCs). We will ensure that Network Rail understands the full implications of this change and addresses them appropriately. Our concerns range from the ergonomic design of workstations to having contingency arrangements that avoid single points of failure affecting large geographic areas.
- Engage with railway businesses to ensure that appropriate steps are taken to ensure the continued integrity of the Train Protection and Warning System

(TPWS) technology that was originally envisaged as having a short lifetime but is set to be in use for many more years. For instance, we are actively encouraging train operators to conduct suitable and sufficient assessments of the risks arising from a lack of TPWS in-service monitoring functionality and whether there is a case for fitment on trains that do not yet have this facility.

For new signalling (renewals, upgrades or enhancements) we will:

- require optimal software integrity. We can do this through our formal role of authorising equipment into service or by using our enforcement powers.
- ensure that schemes take advantage of opportunities to improve related areas such as: level crossing safety, or the ease of track workers protecting themselves from train movements.

Index of issues discussed

Introduction

1. Signalling systems fulfil a fundamental function of safe rail travel by keeping trains a safe distance apart and avoiding conflicting movements. Signalling has evolved from rudimentary lineside visual indications providing advice to drivers to modern in-cab systems that do not require a driver (as in the case of the Docklands Light Railway) as they constantly monitor and supervise a train's safe operation.

2. Because signalling and train control systems are critical, their development has often led innovation in safety engineering. From Victorian mechanical interlocking to modern solid-state equivalents and software-based systems, signalling engineers have sought to eliminate or mitigate human error by operators. Signalling has also enshrined the principle of failing to a safe condition.

3. Despite this focus, fallible humans are involved in the design, installation, testing, inspection, operation, maintenance and repair of signalling systems. As a result, failures could occur that may lead to an unsafe condition, known as 'wrong side failure'

4. Signalling systems are very reliable. However, if they fail there is the potential for a catastrophic event, especially if it is a wrong side failure. This was vividly illustrated by the last such rail accident – Clapham Junction, December 1988. A wrong side failure meant that a train was erroneously signalled into an already occupied section, resulting in it running into the rear of a stationary train. The force of that collision caused the first train to be deflected into the path of a third, oncoming, train. 35 people were killed, nearly 500 injured, 69 of them seriously.

5. The cause of the Clapham crash was incorrect wiring work undertaken as part of the Waterloo Area Resignalling Scheme. An overworked signal technician had left a redundant wire in such a condition that it was able to make a connection with an electrical relay, causing a signal to display a green aspect regardless of the occupancy of the related track circuit.

6. Because of this incident, and the subsequent official investigation (by Anthony Hidden), the industry introduced a number of reforms. The signalling discipline was in the vanguard of introducing structured, systematic competence management systems, and for the first time all safety critical workers became subject to limitations on their working hours.

7. Clapham (and the fatal crash at Purley in March 1989) also played a part in prompting the industry and government to consider protecting trains against the risks of Signals Passed at Danger (SPADs) by some form of automatic train protection (ATP) – despite Clapham not being an ATP-preventable crash. Network-wide ATP was ultimately rejected on grounds of affordability, but the work informed the joint inquiry into train protection systems by Lord Cullen and Professor Uff, who had conducted the public inquiries arising from the SPAD-caused train collisions at Ladbroke Grove and Southall (1999 and 1997).

8. The Uff-Cullen inquiry envisaged the imminent introduction of ATP as part of the European Rail Traffic Management System (ERTMS). In the interim, it recommended, for mainline operations, a short-term solution (for no longer than 10 years) that would introduce immediate benefits for a fraction of the cost of full ATP. This approach was mandated by the Railway Safety Regulations 1999. The mainline railway adopted the Train Protection and Warning System (TPWS). This is a system overlaid onto existing signalling to prevent or mitigate SPAD risk at key locations and manage the risks of over-speeding at the most critical permanent speed restrictions and on the approach to buffer stops.

The risk landscape

9. It has been estimated about 85% of mainline SPAD risk was removed by the introduction of TPWS (there has not been a mainline fatality or injury due to a SPAD since the 1999 Regulations came into force).

10. For other railway networks, the risk was quite different. London Underground (LUL) had comprehensively mitigated the risk from SPADs by using train-stops at signals, which activated train brakes by striking a tripcock. LUL was also the pioneer of automatic train operation (ATO). When the Victoria line opened in 1968, it was the world's first fully automatically operated railway. This system was further developed on the Central line.

11. The Victoria line has since been upgraded to the latest communications-based train control (CBTC) systems. It provides automatic driving control functionality, including ATP protection for over-speeding and the enforcement of driving and movement limits. Like the system in use on the Docklands Light Railway, this means that there is a very high degree of control of risk from a SPAD, or its modern in-cab equivalent.

12. On metro and light rail systems, the risks from SPADs have largely been controlled, either by modern signalling systems, incorporating ATP, or due to the ease of braking lighter vehicles and/or use of track brakes by some operators.

13. On the mainline railway SPAD risk remains from signals which are not protected by TPWS and from the potential for train drivers to dilute the protection TPWS affords by 'reset and go' – i.e. inappropriately resetting the equipment and continuing without the signaller's authority. The latest TPWS equipment mitigates the risks from this behaviour.

14. The Wootton Bassett SPAD (March 2015) was one of the most serious on the mainline since the introduction of TPWS and illustrates the potential harm from overriding train protection equipment. A steam hauled charter train passed a signal at danger at a junction, less than a minute after another service had passed. The cause was the driver wrongly isolating the Automatic Warning System (AWS) and TPWS equipment following an earlier intervention, meaning these systems were unable to operate to mitigate his error when he passed the junction signal.

15. RSSB has developed a tool to assess the risks arising from any signal overrun – the Signal Over-run Risk Assessment Tool (SORAT). Network Rail uses this to model the consequences of a SPAD and identify appropriate SPAD prevention tools.

16. There are risks that are inherent in TPWS continuing beyond its anticipated life – these are considered later when we discuss the challenges facing the industry.

17. All train protection systems are dependent on reliable brakes that can stop trains in a safe and repeatable manner. Braking systems vary in effectiveness depending on the type of rolling stock. Weather and railhead contamination affect adhesion causing significant differences in braking distances. This is critical in the management of wheel and rail interfaces with respect to train protection systems' performance.

18. Signalling equipment is designed to fail to a safe condition – meaning that the immediate risk is controlled by preventing train movements. Whilst this is safe in the short term, it causes delay and inconvenience. To avoid this most railway businesses introduce ‘degraded’ working – i.e. procedures to get train services moving again, when equipment has failed. By their nature, these processes are vulnerable; there are few engineering controls to rely on; they rely on adherence to process and good communication.

19. As degraded working is inherently less reliable in controlling risks, it is desirable to avoid it so far as possible. Remote Condition Monitoring (RCM) of signalling equipment can be used to predict failure – so it can be safely remediated before it fails. This brings a safety benefit as well as a clear performance benefit. Similarly, we are encouraged to see the development of certain systems that might bring a degree of technological assistance to degraded working if the main signalling system fails. Such innovation adds to the resilience of the entire railway system.

20. The main signalling-related risks, now that those associated with SPADs are effectively eliminated or mitigated, relate to hazards associated with a wrong side signalling failure. Although these events are rare, they are potentially catastrophic, as they can fail in such a way that multiple trains could be permitted to continue travelling towards danger. This characteristic means that despite their very low frequency such events must be prevented *so far as is reasonably practicable*.

21. To understand the risks from wrong-side signalling failures better, railway businesses must investigate such occurrences thoroughly – even where the harm has not been realised. These are significant precursors to catastrophic risk and the industry needs the highest quality intelligence about them. The potential for multi-fatality outcomes necessitates that the industry maintains its focus and effort on ensuring the integrity of its signal assets.

22. From our inspection activities, it is not clear that the industry has a complete picture of the precursors to risk in its signalling assets, particularly for the introduction of new technologies and ways of working. Although there are robust systems for the recording and investigation of wrong-side signalling failures, there is a possibility that some events may go unnoticed. At many signal boxes, for example, observing that a track circuit has failed to detect the presence of a train may depend upon a signaller happening to see the right part of a display panel at the right time. It is therefore possible that there is under-reporting of such events. Modern signalling systems are capable of generating alerts when track circuits operate in an unexpected sequence, so the significance of this weakness should reduce as systems are upgraded.

What Challenges Remain?

Train Protection Warning Systems (TPWS)

23. TPWS has already been in place on Network Rail's controlled infrastructure for much longer than was anticipated when it was introduced under the 1999 Regulations. This brings a range of challenges: the existing equipment may be nearing the end of its design life; its maintenance regime needs to be closely monitored and reviewed to ensure its continued integrity; and enhancements should be considered in cases where the introduction of ERTMS or other ATP solutions is not envisaged for a considerable time.

24. More modern forms of TPWS have an in-service monitoring function and a visible and audible SPAD alert, which provides an additional indication to the driver. In-service monitoring will indicate that the on-board equipment is failing to detect a signal from the line side equipment; typically, this happens when an antenna or electrical circuit on the train becomes damaged.

25. Rolling stock without this function has no in-service indication - there is no detection, so the driver is not alerted to the TPWS being inactive and there is therefore no TPWS mitigation to reduce SPAD risks if the driver fails to respond to a signal at danger. An example of the possible consequences of this occurred at Greenford in March 2014 when a train passed two signals at danger. TPWS was fitted to the train and to both signals, but it did not intervene to apply the brakes of the train, as intended. This was because the on-train TPWS equipment had self-isolated when the driver had prepared the train for departure from Paddington station.

26. Some Train Operating Companies (TOCs) and Freight Operating Companies (FOCs) have introduced more modern forms of TPWS. Given the extended timescales for retaining TPWS, and uncertainty over the implementation of the Digital Railway, we will press others to consider the reasonable practicability of introducing this improvement.

Software integrity

27. Since 2005, there have been a number of incidents that show the potential for human error to undermine the integrity of the signalling system. These errors can compromise the safe spacing of train movements. At Peterborough, Shenfield, Rugby, Milton Keynes, Tonbridge and Glasgow Central, errors in the data programming of solid state interlocking (SSI) controls led to situations where trains were able to enter sections that were already occupied. Although none of these occurrences resulted in collisions, the outcome of any of them could have been a multi-fatality train accident. Further software errors have passed through the testing and commissioning phase unnoticed at Reading, Southampton, Stockley and

Streatham re-signalling schemes, indicating that these systems could have been better designed and tested.

28. Some improvements to procedures for solid state interlocking (SSI) data programming, testing and validating have been introduced since 2010. We recognise that SSI is being overtaken by newer technologies, but it will still be on our railways for many years and the same potential for human error underpins Computer-Based Interlocking (CBI) – so the industry must be vigilant in ensuring the integrity of these systems.

Managing the transition to centralisation – Network Rail

29. Control of the mainline railway is being progressively centralised into a small number of Railway Operating Centres (ROCs). This rationalisation programme is having a significant impact on how the railway is operated and on the individuals who are currently part of the distributed system of signal boxes.

30. The anticipated benefits are in the management of the network, improved coordination and reduced costs. ORR has already intervened where there has been inadequate and inconsistent consideration of ergonomic considerations in the design of the working environment within ROCs. As a result, Network Rail has reviewed and revised its standard for the specification of ROCs.

31. Owing to the large sections of line controlled from individual ROCs, a contingency plan is required to minimise risks from cyber-attacks, fire, total power outages and system failures. Ensuring adequate redundancy and resilience to disruption will be key.

32. There is a risk affecting communication to the signaller where geographical knowledge is an issue, particularly from the usage of telephones at level crossings. Certain level crossings with telephones require the user to always telephone the signaller for permission to cross. At other level crossings, telephone calls must be made to the signaller to provide signal protection for long, slow or low vehicles or for livestock traverses. Failing to obtain the signaller's permission before crossing risks being struck by a train.

33. There is concern that the move to ROCs may place unsustainable workloads on signallers; this may distract them from their train regulation duties or lead to errors in giving permission to cross the railway. It is critical that robust prospective workload assessments are made for ROC personnel in this respect and that the conclusions are acted upon.

34. We have required Network Rail to revisit its assessment of the risks of this change in the nature of its operations and to improve its selection of options to mitigate these. The response has been positive and extensive – including ambitious measures to avoid single points of failure. We will continue working to ensure that appropriate steps are taken as this transformation gathers pace. We are keen to

ensure that the potential benefits of this fundamentally different way of controlling the network are realised, as safely as possible.

Digital Railway

35. The term ‘Digital Railway’ is being used to describe Network Rail’s plans to embrace new technologies that can help to meet the demand for increased capacity, reliability and performance. At first, the focus was predominantly on the introduction of ERTMS with an ambitious programme to roll this out on an accelerated timescale.

36. ERTMS refers to the standardised, interoperable European Rail Traffic Management System. It comprises GSM-R, the mobile communications system for railways, and ETCS, the European Train Control System. ETCS is the core signalling and train control system mandated for new schemes or renewals on the mainline network, under the requirements of the Interoperability Regulations.

37. The primary safety feature of ERTMS is ATP or Automatic Train Protection where, even though a driver might retain control of most functions, the system will intervene to enforce braking to keep trains safely spaced. ATO, or automatic train operation, refers to a range of increasingly automated control of train operation – culminating in the possibility of driverless trains. These are the features that can deliver the most significant improvements in safety and capacity – as envisaged by the original digital railway programme.

38. The Network Rail Digital Railway programme has been rationalised and a more cautious approach is now evident. ERTMS is just one of a number of solutions that might be appropriate at locations due for renewal – depending on the characteristics of the site. Brexit also opens up the possibility that in future there may not be a legal imperative to adopt ERTMS.

39. One element of the Digital Railway is the Traffic Management systems (TM). Traffic Management takes inputs from various systems, uses this data to identify conflict points and predict and deliver plans or options to counteract any clashes, and ensures all users are informed of changes as the systems make adjustments. TM systems are linked to the move to ROCs but have not yet been introduced, as the system is still being refined. The trial sites are Cardiff and Romford.

40. TM has considerable scope to minimise delay and disruption, and to assist in reducing signallers’ workload. They also have the potential to be linked to the Driver Advisory System (DAS), which is present on some fleets – meaning drivers receive real time information.

41. The integration of multiple novel technologies under the Digital Railway initiative is inherently complex. The complexity of the challenge may be increased if, as anticipated, the technologies are implemented to varying degrees and at varying paces in different parts of the network. We are monitoring industry plans closely and exerting pressure to ensure that transitions are safely managed. It is preferable to

minimise the number of different signalling and train control systems a driver will encounter in the course of one train journey – but this aim for greater consistency can be difficult to achieve if there are competing demands to introduce new technology on a cost-effective basis, only once existing assets are life-expired, for instance.

42. The future of Digital Railway relies on the interface between trackside equipment and the corresponding on-board equipment. These may be under the ownership of different companies, which could lead to issues regarding the renewal of assets, maintainability and sustainability, and the progress of future enhancements where each owner has differing requirements and budgets.

Implementation of ERTMS, for instance, currently involves:

- Network Rail as infrastructure manager;
- the train operating companies (TOCs), freight operating companies (FOCs) and rolling stock leasing companies (ROSCOs) responsible for train fitment and for training their staff in the new equipment;
- RSSB as the custodian of relevant standards; and
- ORR as the National Safety Authority and DfT as funder.

43. This complexity means that it is hard to achieve the necessary co-operation and governance. A system authority role to bring improved governance is being considered by the industry – perhaps using the model of the System Interface Committee (SIC). This is an impartial body that looks at the system as a whole with a view to ensuring the most appropriate solution is sought to benefit overall performance, sustainability and future enhancements. Currently there are SICs chaired by RSSB for the vehicle/structures, vehicle/track, vehicle/train control & communication (TCC), vehicle/train energy and vehicle/vehicle interfaces. A ‘guiding mind’ for the digital programme would assist in increasing its effectiveness and would promote the duty of co-operation between railway undertakings that is described in ROGS.

44. A key component of ETCS is the automatic train protection (ATP) function. This is a fully functional train protection system capable of stopping trains within a defined safety zone and continuously supervising train speeds during the journey. In order to achieve this, the on-board system must have information about the train’s braking capability as well as other details about its weight and length.

45. If the wrong data is entered into the system, the performance of the train protection equipment is degraded. If, for example, the braking capability is underestimated the ATP system will force the train to brake early and so impact on performance and line capacity. If the braking capability is overestimated the ATP system cannot supervise train speeds and stopping points safely.

46. As the mainline railway progresses towards introducing ETCS, the industry must remain vigilant to ensure that the data entered into the ATP function of ETCS enable the safety function to operate correctly without interfering unduly with performance. Data entry is known to be a particular concern for freight and other non-fixed formation trains.

47. Industry should consider methods of monitoring actual braking performance against the assumed performance used by the ATP system so that corrections can be made to the ATP assumptions during a journey.

48. The mainline industry is now exploring the potential for introducing Automatic Train Operation (ATO) similar to that used on some LUL lines. This development would see ATO operating on trains with a functioning ETCS system to provide full ATP protection. ATO systems are typically configured to brake harder and later as to offer increased capacity on journeys with many station stops. In such circumstances, the ATO and ATP systems need to be able to modify their performance in the event of unexpected changes to brake performance caused, for example, by low rail adhesion. Industry must develop ways of ensuring that variations in rail adhesion are accommodated in the ATO system.

Cyber Security

49. All modern computer based systems are potentially vulnerable to cyber-attack. It is clear that the potential consequences of an attack on a safety system could be significant therefore; all organisations with a responsibility for computer based safety systems must have arrangements to monitor and block such attacks.

50. Whilst a cyber-attack that takes control of a safety system would represent a huge safety risk, the more likely scenario is an attack that denies access and causes disruption.

Exploiting opportunities

51. Whenever signalling systems are renewed an opportunity arises to consider what strengthened risk controls might be introduced. Traditionally, for example, the presence of a level crossing very close to a signal was not part of the design considerations. Therefore, a SPAD might result in a collision with a road vehicle. Resignalling schemes give industry a chance to avoid or mitigate this kind of risk.

52. Similarly, new schemes allow the signalling system to be designed with the needs of worker protection in mind. Such changes constitute the long-term solution to achieving safe systems of work – easy to carry out, secure, technologically enabled methods of protection.

ORR activity

53. For non-mainline duty holders we deal with signalling issues mainly on a reactive basis. We investigate significant occurrences to ensure that the railway business concerned has carried out a sufficiently thorough investigation itself, and has identified and implemented suitable measures to prevent a recurrence.

54. We make regular interventions with TOCs and FOCs to enable us to maintain scrutiny of a number of areas relating to risk in train control systems. For example, we have been persistent in pressing duty holders to fit or consider fitting the more modern models of TPWS equipment that bring greater integrity to the system.

55. We were instrumental in raising industry awareness of the implications of 'reset and go'. More recently, we encouraged the industry to develop a refreshed SPAD strategy following the gradual increase in total SPAD numbers since 2013.

56. On Network Rail infrastructure, we have (between 2002 and 2012) conducted extensive inspection programmes looking at topics such as signaller and signal technician competence management, investigation of wrong-side failures and the management of stretcher bars, etc.

57. This work generated a certain degree of confidence in the well-established framework Network Rail has to manage these sorts of issues – so we now target our limited resources at trying to achieve improvement in risk management, especially managing the changes arising from adopting Digital Railway and migrating to ROCs.

58. We have regular meetings with the engineers who constitute Network Rail's central technical authority. This allows us to raise concerns, monitor progress and influence outcomes regarding a range of issues. This can lead to more concentrated work being carried out on a particular topic. For example, regarding the development of ROCs, we have set up a separate series of meetings to pursue issues highlighted by our inspections. This will lead to further inspections to verify the assurances we have received.

59. The most significant challenge for the mainline railway is to oversee the roll-out of the Digital Railway to ensure that it realises all the benefits it has the potential to deliver. In recognition of the importance of this work, we have created a post dedicated to the scrutiny of ERTMS. We also have an internal working group to share intelligence about Digital Railway progress – and to track our concerns and evolve effective strategies to influence the industry to achieve best results.

60. We have a formal role in authorising new equipment into service. This gives us an opportunity to assess and 'approve' what is being proposed. However, we carry out this statutory function at the very last stage of any project. It is preferable for us to influence design decisions made at a much earlier stage. We try to become engaged far earlier in the process and have a workstream dedicated to safety by

design. We have seen improvements over recent years in the quality of the submissions made to us under the Interoperability Regulations. In the wider field of the initial integrity of assets, Network Rail has made considerable changes to its procedures and is now well placed to comply with its obligations under the Common Safety Method (CSM) on Risk Assessment and Evaluation.

Glossary of terms	
Acronym	**Definition**
ATO	Automatic Train Operation
ATP	Automatic Train Protection
AWS	Automatic Warning System
Brexit	British exit from the European union
CBI	Computer-Based Interlocking
CBTC	Communications-Based Train Control
CSM	Common Safety Method
Digital Railway	Network Rail's plans to embrace new technologies that can help to meet the demand for increased capacity, reliability and performance to accommodate rising passenger numbers.
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
FOC	Freight Operating Company
GSM-R	Global System for Mobile Communications - Railway
ORR	Office of Rail & Road
RCM	Remote Condition Monitoring
ROC	Railway Operating Centres
ROSCO	Rolling Stock Operating Company
RSSB	Rail Safety and Standards Board
SSI	Solid State Interlocking *(Brand name of the first generation processor-based interlocking)*
SORAT	Signal Over-run Risk Assessment Tool
SPAD	Signal Passed at Danger
TOC	Train Operating Company
TPWS	Train Protection and Warning System

This publication is available at orr.gov.uk

Any enquiries regarding this publication should be sent to us at orr.gov.uk