OFFICE OF
RAIL AND ROAD

# Strategic Risk Chapters

## Command, Control and Signalling

01 July 2025

# Contents

# SRC Command, Control and 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 both the need for the entire industry to suitably uphold safety on all existing systems that are in place, and to increase its capability to embrace future changes safely.

We will keep under observation the quality of duty holder investigations involving signalling incidents. Train accidents caused by faults with signalling equipment have 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 must be thoroughly investigated so that the root causes are understood, addressed and any risks managed effectively.

We will monitor the rollout of the Digital Railway programme, automated traffic management and in-cab train control systems so that the transitional risks from older to newer systems are effectively managed. This requires effective industry co-operation.

ORR will continue active monitoring of Network Rail's move from signalling locations to the twelve railway operating centres (ROCs). Focus areas range from the ergonomic design of workstations to having contingency arrangements that avoid single points of failure affecting large geographic areas.

We will engage with railway businesses to ensure that appropriate steps are taken to ensure the continued integrity of the Train Protection and Warning System (TPWS). This technology was originally envisaged as having a short lifetime until 2009 but is now necessary for many more years. We continue to actively monitor exemptions granted against the use of this train protection to ensure that these remain valid when changes are later made to a signalling system, rolling stock, or speed restrictions.

Whether a signalling system/signalling systems assets are designed as new, or part of a renewal/enhancement it is a requirement to ensure optimal software integrity. ORR can do this through the formal role of authorising equipment into service or by using enforcement powers.

We will ensure that schemes take advantage of opportunities to improve related areas such as level crossing safety, or track worker protection from train movements.

# 1. Introduction

Signalling has evolved from lineside visual indications providing advice to drivers to modern in-cab systems.

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

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’. Such a failure is vividly illustrated by the rail accident at Clapham Junction, December 1988.

The official investigation into Clapham Junction introduced a number of reforms to the industry. The signalling discipline was in the vanguard of introducing structured, systematic competence management systems, and safety critical workers became subject to limitations on their working hours.

Clapham (and the fatal crash at Purley in March 1989) 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).

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.

Since the introduction of RSR99, Train Protection and Warning System (TPWS) has been installed across the mainline railway at all legally required locations to ensure a minimum level of train protection at higher risk signals and junctions. TPWS 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.

On some routes, TPWS has been fitted additionally at more locations than required as a minimum. This was expected to be an interim measure not exceeding 2009 but is expected to be in use for many more years to come.

The mainline railway has plans to upgrade to ATP across all routes pursuant to the long-term plan to develop a digital railway and that many non-mainline operations already have ATP in place.

# 2. The risk landscape

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

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.

Communications-based train control (CBTC) systems are in use in large areas of LUL. CBTC is a signalling system that uses telecommunication between onboard and trackside equipment for train operation and control which offers a large degree of mitigation against SPADs and overspeeding with its automatic driving control functionality, including ATP protection.

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.

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.

RSSB developed a tool to assess the risks arising from any signal overrun – the Signal Over-run Risk Assessment Tool (SORAT), and a tool to estimate the number of times a signal is approached at red - Red Aspect Approaches to Signals (RAATS). Network Rail uses these tools to model the consequences of a SPAD and identify appropriate SPAD prevention.

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.

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.

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.

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.

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. These events 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 low frequency such events must be prevented *so far as is reasonably practicable*.

To understand the risks from wrong-side signalling failures better, railway businesses must investigate such occurrences thoroughly. 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.

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.

# 3. Challenges

## Train Protection Warning Systems (TPWS)

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.

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.

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.

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 time to largely implement the Digital Railway, we will press others to consider the reasonable practicability of introducing this improvement.

## Managing the transition to centralisation (Railway Operating Centres)

Control of a significant portion of the mainline railway is progressively being centralised into twelve Railway Operating Centres (ROCs) although ORR understands that Network Rail has stopped short of a complete migration to the ROCs.

Anticipated benefits are in the management of the network, improved coordination and reduced costs. However, owing to the large sections of line controlled from individual ROCs, contingency plans are required to minimise risks from cyber-attacks, fire, total power outages and system failures. Ensuring adequate redundancy and resilience to disruption remain key.

The move to the ROCs raised concerns that unsustainable workloads may be placed on signallers which can be detrimental to their performance, for example in decision-making and communications, which can result in errors in train regulation or providing permission for users 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. NR has a standard to manage the risk of operator error due to workload arising from changes in operation demand. This is known as the National Operating Procedure (NOP) Operational Workload Assessment, 3.37.

However, there have been examples where the combining of workstations in a ROC has resulted in unmanageable workload for a signaller. Network Rail had to introduce temporary measures to manage the workload as a result before a permanent solution could be implemented. This was considered to have arisen as a result of the lack of visibility of signaller cognitive workload. The difficulties of measuring cognitive workload i.e. the mental effort required for tasks such as decision-making are apparent and RAIB's Class Investigation into factors affecting safety-critical human performance in signalling operations on the national network (2020) recognised this issue and recommended that Network Rail should 'develop improved techniques for measuring and predicting cognitive aspects of signaller workload, building on the existing research it has conducted in this area, and integrate the use of such techniques in its management of signaller workload'. Whilst Network Rail has made laudable attempts to address this recommendation, the final objective has yet to be achieved. ORR will continue to manage this RAIB recommendation to its completion.

Other risks can be introduced when integrating workstations into the ROCs, including, the loss of a signaller's geographical knowledge of level crossings under their control or design changes which fail to meet the information needs of the user, for example, the insufficient overview of the signalling area arising from the implementation of four rather than the recommended six workstations contributed to a shift supervisor failing to observe an approaching train and giving permission to a tractor with trailer to cross which resulted in a collision at Hockham Road in 2016. Excellence in Human Factors Integration combined with Network Rail's robust implementation of their assurance processes remain essential for enabling the safe operation of new and upgraded signalling systems in the ROCs.

## Software integrity

Incidents have been highlighted where software errors have passed through the testing and commissioning phase unnoticed. Errors have occurred in data programming, and where there is not a clear communication of assurance responsibilities.

Appropriate steps must be taken by duty holders to ensure the continued integrity of the software used in the different types of signalling applications.

## Cyber security

We will expect duty holders to have addressed cyber security issues in the specification, design and purchasing and operation of Command, Control and Signalling equipment and systems.

## Digital Railway

The term ‘Digital Railway’ is used to describe Network Rail’s programme to roll out ERTMS.

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 Railways Interoperability) (Amendment)(EU Exit) Regulations 2019.

Whilst rail data transmission has been via GSM-R, this system has now met obsolescence and it is understood this is to be replaced by The Future Railway Mobile Communication System (FRMCS).

The implementation plan for ERTMS within Great Britain will take many years, targeting equipment that is life expired.

The railway industry is actively engaged in progressing ERTMS projects in line with the implementation plan. Network Rail has the role of coordinating the whole industry towards achieving the plan.

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. These are the features that can deliver the most significant improvements in safety and capacity.

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 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.

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.

Digital Railways rely 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.

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.

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.

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.

In 2018 Automatic Train Operation (ATO) was introduced to the mainline on the central London section of Thameslink. This development allowed for 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.

## Exploiting opportunities

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.

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.

# 4. ORR Activity

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.

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.

We have regular meetings with 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.

We target our limited resources at trying to achieve improvement in risk management, especially managing the changes arising from adopting a Digital Railway. We 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.

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.

# Appendix: Glossary of terms

| Acronym | Definition |
|---|---|
| ATO | Automatic Train Operation |
| ATP | Automatic Train Protection |
| AWS | Automatic Warning System |
| CBTC | Communications-Based Train Control |
| CSM | Common Safety Method |
| ERTMS | European Rail Traffic Management System |
| ETCS | European Train Control System |
| FOC | Freight Operating Company |
| FRMCS | Future Railway Mobile Communication System |
| GSM-R | Global System for Mobile Communications - Railway |
| ORR | Office of Rail & Road |
| RAATS | Red Aspect Approaches to Signals |
| RCM | Remote Condition Monitoring |
| ROC | Railway Operating Centres |
| ROSCO | Rolling Stock Operating Company |
| RSSB | Rail Safety and Standards Board |
| 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/contact-us