Command, controlling and signalling

1. Executive summary

Command, control and signalling systems are fundamental to the safe management of railways because they ensure that trains are spaced safely apart and that conflicting movements are avoided. Failures in these systems have the potential for catastrophic consequences.

ORR's strategy for regulating the management of train movements and signalling safety recognises both the need for the entire industry to continue to operate existing systems safely, and to increase its capability to introduce future changes safely. This includes managing long-established systems that remain in service beyond their originally anticipated life, as well as the risks that arise during transition from older to newer technologies.

Train accidents caused by faults in signalling equipment are rare but potentially catastrophic. Railway organisations must therefore remain alert to the precursors of such events. Signalling wrong-side failures must be correctly identified, categorised, reported and then be thoroughly investigated so that root causes are understood, addressed and any risks are managed effectively. The quality of dutyholder investigations is critical to preventing low-frequency, high-consequence events.

ORR monitors the rollout of the Digital Railway programme, including automated traffic management and in-cab train control systems, to ensure that transitional risks from legacy to modern systems are effectively managed. This requires effective cooperation across the industry, particularly where multiple technologies and operating models coexist over extended periods.

ORR continues to actively monitor Network Rail's move from traditional signalling locations to Railway Operating Centres (ROCs). This includes consideration of workstation ergonomics, operator workload and contingency arrangements, to avoid creating single points of failure that could affect large geographic areas of the network.

Train Protection and Warning System (TPWS) remains a key safety control on the mainline railway. Although originally envisaged as a short-term solution, TPWS is now required for many more years. ORR engages with railway organisations to ensure the continued integrity of TPWS and actively monitors exemptions to ensure they remain valid when changes are made to signalling systems, rolling stock or operating conditions.

Whether signalling systems are newly designed, renewed or enhanced, ensuring software integrity is essential. ORR undertakes this through its formal role in authorising equipment into service and, where necessary, through enforcement. ORR also expects signalling schemes to take opportunities to improve related safety risks, such as those associated with level crossings or track worker protection.

ORR's focus for command, control and signalling

- ✓ Ensure RUs are working together to address the risk of overspeeding
- ✓ Maintain safety on existing signalling and train control systems
- ✓ Identify and address precursors to catastrophic signalling failures
- ✓ Ensure safe transition from legacy to digital and automated systems
- ✓ Manage risks arising from centralisation and new operating models
- ✓ Maintain the integrity of train protection systems and signalling software
- ✓ Influence design early to embed safety and exploit improvement opportunities

- → Next 2. Our view of the risk

2. Our view of the risk

What the risk is and who it affects

Command, control and signalling systems are critical to the safe operation of the railway because they control train movements, ensure trains are safely spaced apart and prevent conflicting movements. Failures in these systems can result in unsafe conditions and have the potential for catastrophic consequences, including multi-train accidents.

Although signalling systems are designed to fail to a safe condition, fallible humans are involved in the design, installation, testing, inspection, operation, maintenance and repair of signalling systems. As a result, failures can occur that may lead to an unsafe condition. Such failures are rare but potentially catastrophic.

The most significant signalling-related risks in this area are signalling wrong-side failures and overspeeding events, which can each lead to serious or catastrophic consequences.

Signalling Wrong-Side Failure

A signalling wrong-side failure occurs when signalling equipment fails in an unsafe condition, permitting a train movement that should have been prevented. A signalling wrong-side failure gives a less restrictive indication than is safe, which should not be confused with environmental issues such as leaf mulch reducing rail conductivity or trees obscuring signal aspects. These environmentally driven effects may disrupt operations, but they are not wrong-side failures, and it is important to distinguish between the two when assessing faults.

Overspeeding

Overspeeding presents a significant risk to passengers, the workforce, and the public. It may arise from a driver failing to respond to a signal or speed restriction, from degraded braking performance, or from limitations in legacy signalling systems. Duty holders must recognise their responsibilities under the Health and Safety at Work etc. Act 1974 and the Railways and Other Guided Transport Systems (Safety) Regulations 2006 (ROGS), including the requirement for effective cooperation between duty holders.

Learning from Clapham Junction

The rail accident at Clapham Junction in December 1988 resulted in 35 fatalities and was caused by a signalling wrong-side failure introduced during maintenance.

The accident demonstrated that, despite signalling systems being designed to fail safe, human involvement across the signalling lifecycle can introduce defects with catastrophic consequences. In 2022 an incident at South Wingfield shared two dangerous common features with Clapham:

1. A loss of signalling integrity that permitted two trains to occupy the same section
2. Human and organisational factors contributing to the risk.

Though mechanisms differed (Clapham: wiring error; South Wingfield: testing/competence-process shortcomings), the consequence was functionally identical: a wrong-side failure that removed protection.

These incidents are defining examples of the need for robust competence, assurance and investigation to prevent low-frequency, high-consequence failures.

The risk landscape

Historically, a significant proportion of train accident risk arose from Signals Passed at Danger (SPADs). The introduction of the Train Protection and Warning System (TPWS) on the mainline railway has substantially reduced this risk, with estimates indicating that around 85% of mainline SPAD risk was removed following its introduction. There has been no mainline fatality due to a SPAD since the Railway Safety Regulations 1999 came into force.

Risk profiles differ across the rail sector:

RSSB tools such as the Signal Over-run Risk Assessment Tool (SORAT) and Red Aspect Approaches to Signals (RAATS) are used to understand SPAD risk and inform appropriate prevention measures.

Residual and emerging signalling risks

Now that many SPAD-related risks have been eliminated or mitigated, the most significant signalling-related risks arise from signalling wrong-side failures and overspeeding. These failures are low frequency but high consequence, as they can permit trains to continue towards danger. Despite their rarity, they must be prevented so far as is reasonably practicable.

Effective management of this risk depends on high-quality investigation and reporting of signalling wrong-side failures and overspeeding, which are important precursors to catastrophic events. Although robust systems exist for recording and investigating such failures, there is a possibility that some events may go unnoticed, particularly where detection relies on human observation. This may lead to incomplete or skewed data, reducing the industry's ability to understand underlying risk trends. Modern signalling systems increasingly provide automated alerts, which should reduce this risk over time.

System dependencies and degraded operation

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.

Recent incidents have highlighted that newer rolling stock, operating at higher performance levels, can expose limitations in legacy signalling and protection systems where overspeed risk is not adequately mitigated.

Spital Junction

Overspeed events at Spital Junction involved trains approaching junction signals at speeds that exceeded the limits assumed within the signalling and protection arrangements. The incidents highlighted the interaction between braking performance, signal approach control and the configuration of protection systems. They reinforced the need to ensure that braking assumptions, rolling stock characteristics and signalling protection parameters are aligned, particularly where newer rolling stock with improved performance operates over legacy infrastructure.

Grantham South

Events at Grantham South similarly involved trains approaching restrictive signals at higher-than-anticipated speeds. These occurrences drew attention to the importance of ensuring that signal approach controls, braking curves and protection system settings reflect actual rolling stock performance. They also underlined the need for robust assurance when introducing changes to rolling stock or signalling arrangements, so that overspeed risk is not inadvertently increased.

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 organisations introduce 'degraded' working – i.e. procedures to get train services moving again, when equipment has failed. By their nature, these processes are vulnerable, and there are few engineering controls to rely on. They depend on adherence to process and excellent 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, the ORR is 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.

Why risk must be actively understood

The command, control and signalling risk landscape is shaped by a combination of legacy systems, human performance, system dependencies and emerging technologies. While many historic risks have been substantially reduced, residual and emerging risks remain, particularly those associated with signalling wrong-side failures and system transitions.

Understanding these risks, and how they differ across parts of the railway, is essential to managing train movement safety effectively and to supporting the safe introduction of future signalling and train control systems.

- ← Previous Command, controlling and signalling
- → Next 3. Compliance expectations

3. Compliance expectations

Why compliance matters

Command, control and signalling systems are safety-critical because they directly control train movements and prevent conflicting routes. Failures in these systems, particularly signalling wrong-side failures, can have catastrophic consequences. Although such events are rare, their potential severity means that risks must be prevented so far as is reasonably practicable.

Compliance expectations therefore focus on ensuring that railway organisations maintain the integrity of their signalling and train control systems throughout their lifecycle, and that failures, incidents and precursors are identified, investigated and addressed effectively. The quality of dutyholder investigations into signalling incidents is critical to understanding root causes and preventing low-frequency, high-consequence events.

Why compliance is critical

- ✓ Wrong-side signalling failures are low frequency events but have potential for high severity consequences
- ✓ Robust investigation of incidents and precursors is essential
- ✓ System integrity must be maintained as technology and operations change

The legal and regulatory basis

Railway organisations are required to manage the risks associated with signalling and train control systems through their own safety management systems. This includes duties under the Health and Safety at Work etc. Act 1974, The Railways and Other Guided Transport Systems (Safety) Regulations 2006 (ROGS), and The Railway Safety Regulations 1999 (RSR), including Regulation 3 relating to train protection. ORR's role is to provide assurance that these arrangements are effective and, where necessary, to promote and enforce improvements to secure safe outcomes.

ORR expects signalling systems to be designed, installed, tested, operated, maintained and renewed in a way that ensures continued system integrity. Whether a signalling system is newly designed or part of a renewal or enhancement, appropriate steps must be taken to ensure optimal safety and software integrity. ORR undertakes this through its formal role in authorising equipment into service and, where necessary, through the use of enforcement powers.

Cyber security is also a key element of system integrity. Dutyholders are expected to address cyber security risks in the specification, design, procurement and operation of command, control and signalling systems.

When compliance must be demonstrated

Compliance must be demonstrated throughout the lifecycle of signalling and train control systems and whenever changes are made that could affect safety. This includes:

- the introduction of new signalling or train control systems;
- renewals, enhancements or upgrades to existing systems;
- changes to rolling stock, operating rules or speed profiles;
- transitions from legacy to digital or automated systems; and

- organisational or operational changes, such as the move to centralised control in Railway Operating Centres
- following incidents, failures or identified precursors

Where incidents or failures occur, including signalling wrong-side failures, dutyholders must ensure that investigations are thorough and that identified risks are addressed effectively. Exemptions – defined by The Railway Safety Regulations 1999 – relating to train protection systems, such as TPWS, must be kept under review and confirmed as valid when changes are made to infrastructure or operations.

ORR's expectations of dutyholders

Dutyholders are expected to:

- ☑ maintain the integrity of signalling and train control systems in service
- ☑ ensure that signalling incidents and precursors, including wrong-side signalling failures, are identified, reported and investigated to a high standard
- ☑ manage transitional risks when moving from legacy systems to newer technologies, including through effective co-operation with other industry parties
- ☑ ensure that software, data and system interfaces are correctly specified, tested and assured throughout the system lifecycle
- ☑ manage human performance risks, including workload, competence and situational awareness, particularly where operating models or control arrangements change
- ☑ ensure that appropriate contingency, redundancy and resilience arrangements are in place to avoid single points of failure affecting large areas of the network
- ☑ take opportunities, when renewing or enhancing signalling systems, to improve related safety risks, such as those affecting level crossings or track worker protection

ORR expects to be engaged early in the development of new or significantly modified signalling schemes so that safety can be influenced at the design stage, rather than relying solely on end-of-process authorisation.

- ← Previous 2. Our view of the risk
- → Next 4. Continuous improvement

4. Continuous improvement

How command, control and signalling risk is reduced over time

Continuous improvement in command, control and signalling is essential to maintaining safe train operations as systems age, operating models change and new technologies are introduced. Risk reduction depends on maintaining the integrity of existing systems, strengthening controls through renewal and enhancement, and managing the transition to digital and more automated technologies in a controlled way.

Taken together, these activities form a continuous improvement cycle, moving from the management of existing assets through renewal and transition, and ultimately delivering improved resilience and safety.

Managing long-term reliance on Train Protection and Warning System (TPWS)

TPWS has been in service on Network Rail's infrastructure for significantly longer than was anticipated when it was introduced under the Railway Safety Regulations 1999. This extended use presents ongoing challenges, including equipment approaching the end of its design life, the need for continued scrutiny of maintenance regimes, and consideration of enhancements where the introduction of ERTMS or other ATP solutions is not yet envisaged.

Given the extended timescales for retaining TPWS and uncertainty over the pace of Digital Railway implementation, dutyholders are expected to consider the reasonable practicability of introducing improvements to strengthen risk control.

Strengthening resilience during centralisation into Railway Operating Centres

The progressive centralisation of signalling control into twelve Railway Operating Centres (ROCs) is changing the signalling risk profile on the mainline railway. While centralisation offers benefits in network management, coordination and cost efficiency, it also concentrates control of large sections of the railway, increasing the potential impact of failures.

Continuous improvement during this transition depends on ensuring adequate contingency arrangements to manage risks arising from cyber-attack, fire, power loss and system failures, and on avoiding single points of failure that could affect large geographic areas. Ensuring sufficient redundancy and resilience to disruption remains a key requirement as control arrangements are reconfigured.

Human performance is a critical factor in the safe operation of ROCs. The move to centralised control has raised concerns that unsustainable workloads may be placed on signallers, with potential impacts on decision-making, communication and overall performance. Robust prospective workload assessments are therefore essential, and conclusions must be acted upon as systems and operating demands change. Network Rail has established standards to manage the risk of operator error arising from workload changes, including the National Operating Procedure (NOP) Operational Workload Assessment (3.37).

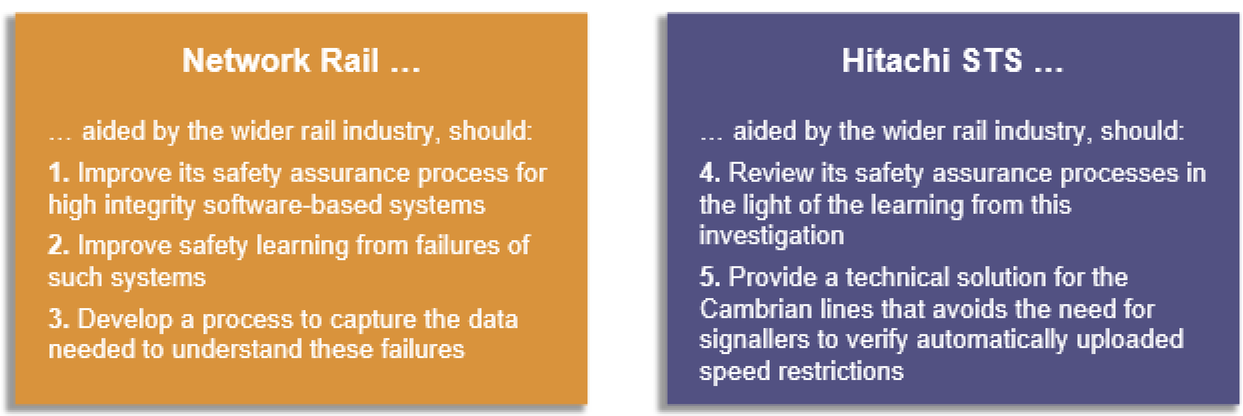
Experience has shown that combining workstations can, in some cases, result in unmanageable workload where cognitive demands are not well understood or visible. Temporary mitigations have been required in some instances before permanent solutions could be implemented. Measuring and predicting cognitive workload remains challenging, and RAIB's 2020 Class Investigation into safety-critical human performance highlighted the need for improved techniques to assess and manage these risks. Progress has been made, but further work is required, and ORR continues to oversee completion of this recommendation.

Other risks associated with ROC integration include loss of signallers' local geographical knowledge, particularly of level crossings, and design configurations that do not adequately meet users' information needs. Learning from incidents, such as the collision at Hockham Road in 2016, reinforces the importance of strong human factors integration alongside robust assurance processes to support the safe operation of new and upgraded signalling systems in ROCs.

Improving assurance of software, data and system integrity

Software and data integrity are increasingly important as signalling systems become more complex and interconnected. Incidents have shown that errors can pass through testing and commissioning where assurance responsibilities are unclear or fragmented.

Loss of safety critical signalling data on the Cambrian Coast line, 20 October 2017 highlights how software systems need to be assured. The investigation makes five recommendations:



Dutyholders are expected to strengthen assurance arrangements to ensure the continued integrity of signalling software, data and interfaces throughout the system lifecycle. This includes learning from incidents, improving communication of assurance responsibilities and maintaining clear accountability as systems evolve.

Cyber security also forms part of this assurance landscape. As systems become more connected and digitally enabled, continuous improvement requires cyber risks to be addressed alongside traditional safety risks.

Managing the transition to the 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.

Whilst rail data transmission has been via GSM-R, this system has now become obsolete 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 and represents a long-term transition rather than a single change. The rollout of ERTMS, automated train protection, traffic management systems and increasingly automated train operation will involve periods where multiple signalling and train control technologies coexist.

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.

Continuous improvement in this context depends on:

- managing transitional risks as legacy and new systems operate side by side
- ensuring data integrity, particularly for train braking performance and system interfaces
- coordinating activity across multiple system owners and duty holders
- learning from early implementations to inform later deployments

While digital systems offer significant opportunities to improve safety, capacity and performance, their integration is inherently complex and requires sustained focus to ensure risks are reduced rather than displaced.

More information on ERTMS is provided in the Appendix.

Exploiting opportunities through renewal and enhancement

Whenever signalling systems are renewed or enhanced, opportunities arise to strengthen risk controls. Resignalling schemes can address risks that were not previously considered in design, such as interactions between signals and level crossings. New schemes also provide opportunities to design signalling systems that better support track worker protection and safer systems of work.

Exploiting these opportunities is a key element of long-term risk reduction, enabling safety improvements to be embedded through design rather than relying on procedural controls alone.

Design-led improvement

Renewal and enhancement provide opportunities to embed stronger risk controls and reduce reliance on degraded working and human intervention.

Embedding improvement as normal practice

Sustained improvement in command, control and signalling depends on embedding these approaches into routine planning, operation, renewal and change management. Maintaining system integrity, strengthening assurance, learning from incidents and managing transitions safely are ongoing requirements as the railway continues to evolve.

Continuous improvement therefore supports both the safe operation of existing signalling systems and the safe introduction of future technologies.

- ← Previous 3. Compliance expectations
- → Next 5. Appendix

5. Appendix

Signalling system evolution and historical context

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 'signalling 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 many non-mainline operations already have ATP in place.

Digital Railway and system integration

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 automated control of train operations ranging from driver assistance to fully driverless operation. These are the features that can deliver significant improvements in safety.

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. The ORR is 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;
- 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.

Glossary of terms

Acronym or abbreviation	Full name
ATO	Automatic Train Operation
ATP	Automatic Train Protection
CBTC	Communications-Based Train Control
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
FOC	Freight Operating Company
FRMCS	Future Railway Mobile Communication System

Acronym or abbreviation	Full name
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

- ← Previous 4. Continuous improvement
- → Next 2. Our view of the risk