

Command, controlling and signalling

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