Fundamental requirements for a train control system

BACK TO BASICS

In the first of a planned series of 'back to basics' subjects on train control and communications, this article summarises the fundamental requirements for a train control system. These requirements will be familiar to experienced signalling engineers, but are recommended reading for anyone new to railway control and communications and for IRSE members preparing to take the IRSE Exam.

The requirements were originally set out in the IRSE Signalling Philosophy Review (2001) and have subsequently been reviewed and revised a number of times. They are available in full via the IRSE website at irse.info/ex3ous.

The requirements are not mandated by the IRSE, although the Institution regards them as essential for any train control system.

The word 'signalling' is defined by the IRSE as all the equipment, electrical, mechanical or otherwise, methods, regulations and principles whereby the movement of railway or other traffic is controlled. Throughout the requirements, and in this article, the phrase "train control system" includes the people, procedures and technology used to signal trains; and where the single word "system" is used it means the "train control system". Where the phrase "signalling system" is used, this means the part of the train control system which is implemented by means of technology, which could be both infrastructure-based and train-borne. The requirements are equally applicable whatever form of train control system (as defined above) is used to control train movements. Accordingly, they are written at a high level, with the intention that users interpret and apply the requirements through the specific method of train control that is proposed for a railway.

The requirements are in three sections. The first deals with operational requirements, the second with functional safety requirements, and the third addresses supporting safety requirements.

Operational requirements for train control systems

The system will need to meet the needs of operators in terms of:

- permitted train movements (such as normal running; joining/ splitting; platform sharing, shunting);
- permitted routing of trains;
- capacity provision and utilisation;
- and flexibility of operations.

The system may also contribute to efficient resource management, such as efficiency in traction energy consumption, and minimising wear and tear on the track.

If, in addressing requirements for safety, the proposed design constrains the operability of the railway, the impact of this will need to be assessed and minimised (but without compromising acceptable levels of safety, of course).

In order to deliver the timetabled train service, the specification and attainment of appropriate levels of reliability and availability are essential. Reliability and availability also contribute to overall levels of system safety. Maintainability is essential in order to ensure that the specified levels of reliability and safety continue to be met throughout the service life of the system.

To achieve required levels of overall availability, the provision of degraded modes of operation is desirable. However, human intervention as a means of safely controlling train movements under failure conditions (e.g. signallers authorising trains to pass signals at danger, manual on-site operation of points) entails significantly higher risk and is therefore not the preferred means of meeting this requirement. Transitions to and from degraded modes of operation will need to minimise risk, facilitated by "graceful degradation" as well as timely and safe mechanisms for recovery to normal operation.

Train control has a long history but is evolving rapidly as technological change offers new alternatives to manage the safe movement of trains to deliver the optimum experience for railway passengers and freight users. There is however a series of underpinning requirements for any train control system. *Photo Shutterstock/hxdyl*.

Functional safety requirements for train control systems

Before a train is given authority to move along a section of line, the section of line needs to be proved to be secure (see below) and clear of other traffic, to prevent derailments and collisions, and to avoid conflict with movement authorities given for other trains.

Exceptions to this are circumstances where a train is permitted to enter an occupied section of line, such as for platform sharing, coupling of trains, permissive working, and shunting.

Where the train is stationary at a station, depot or siding, activities such as train preparation, loading, unloading, closing doors must also be completed before the train is moved. However, these activities are not normally regarded as part of the functionality of the train control system.

The term "secure" (see above) refers to a limited set of safety requirements, primarily relating to the position and locking of points, and the routing of other trains. Signalling systems do not usually prove that the line is clear of all obstructions, or that the gauge is correct and the track is physically stable, so other control measures may need to be considered to manage these risks.

When authority to move along a section of the line has been given, the security of the line needs to be maintained for the movement until the complete train has:

- passed clear of the section of line; or
- the authority has been rescinded (withdrawn) and the train has come to a stand; or
- the authority has been rescinded (with information communicated to the train) with the train having sufficient space to come to a stand safely before the start of the section of line over which authority to move had been given.

In some signalling systems sectional route release is used, whereby parts of a section of line are released progressively when the train has passed clear, to facilitate earlier setting of other routes.

The train driver (or the automatic train operation sub-system [ATO]) will require unambiguous, consistent and timely information that enables safe control of the train. This may include:

- proceed/stop information;
- the provision of warning information regarding the approach to the end of the movement authority or a section of lower speed line, to enable the train to brake safely;
- the provision of speed, routing, gradient, braking capability information.

In addition, data entry sub-systems may be required in order to input train parameters that are relevant to the safe operation of the train control system (e.g. weight, length, braking capability).

Sufficient space will be required between following trains to allow each train to brake to a stand safely; this is usually calculated on the assumption that the train ahead is stationary.

Suitable control measures will be required in order to prevent and/or mitigate the consequences of a train:

- passing the end point of its movement authority;
- exceeding the maximum permitted speed;
- moving without authorisation.

Examples of technical solutions for these include overlaps, train protection/warning systems, flank protection, approach control/release of signals, provision of trap points and speed signs. It may also include other measures, e.g. driver competence, provision of information to drivers and operating rules.

Protection will be required for the public and trains at level crossings, although not all level crossings are necessarily protected by the signalling system itself (in simple cases an independent means of protection may be adequate based on risk). The operation of a level crossing will need to minimise the road closure time, otherwise this could lead to crossing misuse by pedestrians and road vehicle drivers.

Trains, worksites and workers will need to be protected during engineering work. This could include:

- facilities for controlling the access of trains to sections of line where work is taking place or where safety has been reduced as a result of engineering work;
- ensuring that the section of line is clear of obstructions (e.g. engineering vehicles) when work is complete and before trains are allowed to run over it;
- restricting the speed of trains to help protect track workers or because of the condition of the track;
- warning trackside workers of the approach of trains.

In order to provide a safe and efficient railway the signaller will require unambiguous, consistent and timely information, and suitable control facilities, to enable the safe authorisation of train movements (the term signaller also include other personnel who may have responsibility for authorising train movements). This includes the provision of information required under failure and degraded mode conditions, as well as for normal operations. Ancillary information systems such as train describers, critical fault alarms and data entry systems may also be required. When designing the signaller interface systems, human factors assessments will contribute to safety and efficiency.

Facilities for communication between signallers and others will be required, for both normal operation and degraded/ emergency working. This includes communication with:

- train drivers;
- signallers in neighbouring control centres;
- train operators and route controllers;
- level crossing users;
- emergency services.

The nature of the communications systems will need to be appropriate for the purposes required, for both normal operations and failure/degraded mode situations.

A means will be required for preventing trains from being routed onto a section of line with which they are not compatible. Situations where this requirement could apply include:

- incompatibilities of gauge between track and train;
- incompatible traction supply systems for the train;
- incompatible train-borne train control sub-systems;
- restrictions on access to tunnels for certain types of trains;
- restrictions on specific train types being permitted on routes, adjacent lines etc, at the same time, such as hazardous freight and passenger trains.

In order to instruct a train to stop in an emergency, appropriate facilities will be required. This could be met by functionality within the signalling system itself to enable a movement authority to be withdrawn, or by the use of an alternative/ independent means such as radio communication with the driver. The speed and reliability with which a message can be given to a train to stop needs to be commensurate with the risks associated with the emergency. The risk of stopping trains in unsuitable locations also needs to be taken into account.

Essential supporting safety requirements for train control systems

The assignment of safety targets for a train control system will need to:

- be commensurate with, or better than, the levels of safety performance of comparable systems already in service;
- meet the reasonable expectations of users;
- comply with legal requirements.

The compatibility of the operating rules with the rest of the train control system (and their completeness) is essential for the safe operation of the railway under normal, degraded and emergency conditions.

Even though the system may be highly automated, there will always be a measure of dependence on human interaction, for instance during degraded mode operation or during maintenance. Appropriate allocation of functions between the signalling system and operators, and designing the overall train control system to make it easy for operators and maintainers to perform their actions safely, is vital. The human factors will need to be addressed to help provide a safe and easy system to operate, both for operators and maintainers.

Modern signalling systems usually revert to a safe state, such as signals automatically restoring to “stop”, although this may not always be necessary or desirable (and indeed mechanical signalling systems do not generally do this). Designing the system so that failures and faults are self-revealing to operators and maintainers will aid prompt and safe rectification, and will help to avoid situations where a fault is latent (hidden) and does not reveal itself until some other event occurs.

Unsafe interactions of the system with other railway systems and equipment need to be avoided. This includes both interactions where there is an intentional interface with other systems and equipment, such as other railway infrastructure and trains; and interaction where there is no interface, such as electromagnetic interference. Unwanted external influences that could adversely affect the safety and availability of the system include:

- environmental/ climatic effects;
- cyber-attacks on software-based subsystems;
- vandalism;
- unwanted electrical/radio interactions with non-railway systems.

Problems can occur when introducing new rolling stock on routes with older signalling systems, which may not be immune to interference generated by new trains. Introducing new rolling stock in a controlled manner will facilitate early identification and rectification of problems not addressed at the design stage.

Systems that are designed so far as possible to prevent the possibility of inadvertent errors during maintenance and repair work, and which incorporate diagnostic systems for monitoring the health of the equipment, will contribute to its continuing safe operation and minimise the risk of introducing undue risk to either the operational railway or the personnel carrying out the work. These considerations may have implications for e.g. the design of equipment and its physical location.

Personnel who design, build, test, commission, operate and maintain the signalling system, or in any other way form part of the train control system, will need to be competent in order to perform their tasks and duties safely and efficiently. This includes the competence of designers, testers, drivers, signallers, maintainers and others whose activities contribute to the overall safe working of the system. The application of suitable procedures for personnel selection, training, assessment and periodic review will contribute to continuing competence.

What do you think?

What other ‘back to basics’ articles would you like to see in IRSE News? Why not share your experiences with other engineers? Email **editor@irsenews.co.uk**.