IRSE
Institution of Railway Signal Engineers

Fundamental Requirements for Train Control Systems

The following fundamental requirements describe the overall purposes of a train control system. They are an extended set of the requirements that were originally set out in the Institution of Railway Signal Engineers' Signalling Philosophy Review [2001], later revised in a paper to the IRSE on Signalling Philosophy, Principles and Practice [2004]. They have subsequently been reviewed and further revised by the IRSE's Education and Professional Development Committee during 2013/14, and are now published in their final form by the IRSE.

The requirements are non-specific about the means by which they are achieved, and could include people, procedures and technology in any combination. They should, therefore, be applicable to any form of train control system no matter how elementary or sophisticated and no matter which country or network.

Reflecting the non-specific nature of the requirements, the phrase "train control system" in the document should be understood to include people, procedures and technology (and where the single word "system" is used, this means the "train control system"). Where the phrase "signalling system" is used, this is a reference specifically to that part of the train control system which is implemented by means of technology (infrastructure-based and train-borne).

These requirements are not mandated by the IRSE, and therefore the word "should", rather than "shall" is used throughout the text. Supporting guidance is shown in italics immediately after each requirement. Nevertheless, the requirements are regarded as essential for any train control system.

The requirements do not address the processes and competences for the design, build, testing and commissioning phases of a train control system.

1. Core operational requirements for train control systems

1.1 The system should facilitate the safe, efficient and effective operation/use of railway infrastructure and rolling stock.

[The system should meet the needs of operators in terms of: permitted train movements (such as normal running; joining/splitting; platform sharing, shunting etc); permitted routing of trains; capacity 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].

1.2 The intrusiveness of the system into the efficient and effective running of the railway in performing its safety function should be minimised.

[The need for safety can conflict with the need to facilitate efficient and effective operations. In seeking safety, designers of the system should consider the impact that their proposed design might have on the operability of the railway].

1.3 The reliability, availability and maintainability of the signalling system should be sufficient for it to fulfil the operational requirements for which it is provided.

[The specification and attainment of appropriate levels of reliability and availability are essential to the delivery of the timetabled train service. 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].

1.4 "Degraded mode" facilities should be provided to enable trains to move when elements of the signalling system have failed.

[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 degraded modes of operation should be handled in a way that minimises risk, and may include "graceful degradation" as a means of facilitating this. Likewise, the arrangements for transitioning back to normal operation should also facilitate safe and timely recovery].

2. Core functional safety requirements for train control systems

2.1 Before a train is given authority to move along a section of line:

a) the section of line should be proved to be secure (to prevent derailment and to avoid conflict with movement authorities given for other trains), and
b) the section of line should be proved to be clear of other traffic (to prevent collision), except in circumstances where a train is permitted to enter an occupied section of line.

[The term "secure" 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, for instance, prove that the line is clear of obstructions, or that the gauge is correct and the track is physically stable].

[The circumstances for movements onto occupied lines may include platform sharing, coupling of trains, permissive working, and shunting].

[Where the train is stationary at a station, depot or siding, duties such as train preparation, loading, unloading, closing doors etc, 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].

2.2 After authority to move along a section of the line has been given, the security of the line should be maintained for the movement until:

a) the complete train has passed clear of the section of line, or
b) the authority has been rescinded and the train has come to a stand as a consequence, or
c) the authority has been rescinded (and this information has been communicated to the train) and the train has sufficient space to come to a stand safely before the start of the section of line over which authority to move had been given.

[This requirement does not exclude the possibility of sectional route release, whereby parts of a section of line are released progressively when the train has passed clear, facilitating earlier setting of other routes].

2.3 The train driver (or automatic train operation sub-system [ATO]) should be provided / equipped with unambiguous, consistent and timely information that enables safe control of the train.

[The train may be operated by a driver, but this requirement also includes the possibility of the train being driven by an ATO sub-system, either with or without a driver present].

[This covers the requirement to give the driver (or the ATO sub-system) 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 etc].

[Data entry sub-systems on board the train which are used by the driver to set parameters relevant to the safe operation of the train control system are also within the scope of this requirement].

2.4 Sufficient space should be provided between following trains to allow each train to brake to a stand safely.

[The space between following trains is usually calculated on the assumption that the train ahead is stationary].

2.5 Controls should be in place to prevent and/or mitigate the consequences of:

a) trains passing the end point of their movement authority; and

b) trains exceeding the maximum permitted speed and;

c) trains (and individual vehicles) moving without authorisation.

[Technical solutions may include overlaps, train protection/warning systems, flank protection, approach control/release of signals, etc. It also includes other measures, e.g. train driving and stabling procedures, driver competence, provision of information to drivers, prevention of unauthorised access to driving cabs, etc.]

2.6 Protection should be provided for the public and trains at level crossings.

[Not all level crossings are necessarily protected by the signalling system itself; in simple cases an independent means of protection may be provided].

2.7 The means should be provided for protecting trains, worksites and workers during engineering work.

[All types of engineering work are included within this requirement, whether or not they affect the train control system itself].

[This should 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 (engineering vehicles etc) 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; and warning trackside workers of the approach of trains].

2.8 The signaller should be provided with unambiguous, consistent and timely information, and suitable control facilities, to enable the safe authorisation of train movements.

[This includes the information required under failure and degraded mode conditions, so far as possible, as well as normal operations. The requirement also includes ancillary information systems such as train describers, critical fault alarms and data entry systems, upon which the signaller depends. The term signaller also includes other personnel who may have responsibility for authorising train movements].

[This requirement is not intended to preclude the possibility of automation of some of the functions traditionally performed by a signaller, e.g. with automatic route setting and conflict resolution].

2.9 The system should have facilities for communication between signallers and others.

[This includes not only driver-signaller communication, but also communication, for example, between signallers in neighbouring control centres, and between signallers and emergency services. The nature of the communications systems should be appropriate for the purposes to which they are to be put, for both normal operations and failure/degraded mode situations].

2.10 The means should be provided for preventing trains from being routed onto a line with which they are not compatible.

[Situations where this requirement applies includes incompatibilities of gauge between track and train, incompatible traction supply systems for the train, and incompatible train-borne train control sub-systems. It may also include restrictions on access to tunnels for certain types of trains, or restrictions on specific train types being permitted on sections of line at the same time, such as hazardous freight and passenger trains].

2.11 Facilities should be provided to instruct a train to stop in an emergency.

[This requirement could be met by facilities 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. Account should also be taken of the risks of stopping trains in unsuitable locations].

3. Essential supporting safety requirements for train control systems

3.1 The level of safety performance of the system should meet specified targets.

[Targets should be commensurate with, or better than, levels of safety performance of comparable systems already in service, meet the reasonable expectations of users, and comply with legal requirements].

3.2 The signalling system and the associated operating rules should be compatible with each other.

[The signalling system, the associated operating rules and the users/operators together constitute the wider train control system, as defined in the introduction to this document. The compatibility and completeness of these elements of the train control system is essential for the safe operation of the railway under normal, degraded and emergency conditions].

3.3 The human factors associated with the safe use/operation of the system should be taken into account in the specification and design of the system.

[Even though the system may be highly automated, there 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].

3.4 In the event of a failure of the signalling system, it should remain in, or revert to, a state which preserves the safety of trains.

[Modern signalling systems usually revert to a safe state, such as signals automatically restoring to danger, although this may not always be necessary or desirable, and indeed mechanical signalling systems do not generally do this].

[In addition, failures and faults in the signalling system should so far as possible be self-revealing to operators and maintainers, both to aid prompt and safe rectification, and to avoid situations where a fault is latent (hidden) and does not reveal itself until some other event occurs].

3.5 The signalling system should not be subject to, nor be the cause of, unsafe interactions with other railway systems and equipment.

[This includes both interactions where there is an intentional interface with other systems and equipment, and interaction where there is no interface, such as electromagnetic interference. The "other systems and equipment" refers to other railway infrastructure and trains].

3.6 The system should be resilient to unwanted external influences that could adversely affect the safety and availability of the system.

[This includes addressing environmental/climatic effects, cyber-attacks on software-based sub-systems, vandalism, unwanted electrical/radio interactions with non-railway systems].

3.7 The arrangements for the maintenance and modification of the signalling system should be appropriate for ensuring its continuing safe operation.

[Systems should be designed so far as possible to prevent the possibility of inadvertent errors during maintenance and repair work. Systems should include the provision of diagnostic systems for monitoring the health of the equipment].

[It should be possible for the maintenance and modification activities to be performed on equipment without undue risk to either the operational railway or the personnel carrying out the work. This may have implications for the design of equipment and its physical location].

3.8 Personnel who use, operate and maintain the signalling system, or in any other way form part of the train control system, should be demonstrably competent to perform their tasks and duties.

[This includes the competence of drivers, signallers, maintainers and others whose activities contribute to the overall safe working of the system, and should include selection, training, competence assessment and periodic review of continuing competence].

END