

Category 1 Standard

S1196 Signalling and Signalling Control - Concept and Requirements



Please read the Written Notices
attached to this standard

Issue No.: A4

Issue date: November 2011
Review date: November 2016

MAYOR OF LONDON

 **Documents**
Document Sharing Hub



Contents

1	Purpose	3
2	Scope	3
3	Requirements	4
3.1	System Requirements	4
3.2	Process Requirements	11
3.3	Operational Environment	16
3.4	Electromagnetic compatibility (EMC)	19
3.5	Design requirements for use in 25kV areas	21
3.6	Evidence of Compliance	23
4	Responsibilities	23
5	Supporting Information	24
5.1	Background	24
6	References	25
6.1	References	25
6.2	Abbreviations	27
6.3	Definitions	27
6.4	Technical content manager	28
6.5	Document history	29
7	Current Written Notices attached to this standard are:	29



1 Purpose

The purpose of this Standard is to provide a statement of the requirements concerning process, technical and environmental issues which shall be applied at the conceptual phase of the life cycle of signalling and signalling control systems.

2 Scope

- 2.1 The Standard covers the following systems which are used on the London Underground Railway:
 - a) Vital Signalling Systems (including interlocking sub-systems, train detection sub-systems, trackside sub-systems, trainborne sub-systems, automatic train protection sub-systems, automatic train control sub-systems);
 - b) Signalling Control and Information Systems (including local site control sub-systems, central control room sub-systems, automatic vehicle identification sub-systems).
- 2.2 This Standard focuses on requirements for the first stage of the lifecycle, Concept and Requirements. The totality of requirements contained within the complete suite of Signalling and Signalling Control Standards (see 5.1.1) shall be complied with for these systems.
- 2.3 This issue of the standard replaces 1-196 A3.



3 Requirements

3.1 System Requirements

3.1.1 System Design

- 3.1.1.1 Signalling and Signalling Control Systems shall be managed and developed in compliance with European standards, in particular BS EN 50126, BS EN 50128, BS EN 50129.
- 3.1.1.2 The initial system design process shall be based on a system lifecycle which enables the implementation of the dependability requirements stated in BS EN 50126.
- 3.1.1.3 A Design Authority shall be nominated for each system and equipment type. The Design Authority shall be a professional in the relevant signalling or control field with expert domain knowledge who is independent of the delivery team and has independent reporting lines to the project delivery team.
- 3.1.1.4 The design process shall include documented design reviews at a level, depth and frequency appropriate to the task.
- 3.1.1.5 The design for Service Control Centres shall be in accordance with the ergonomic and operability requirements of Standards 1-217, Integration of Human Factors into Systems Development and 1-218, Universal Human Computer Interface.
- 3.1.1.6 The design reviews shall include persons with a system understanding of the project requirements and expertise from all the prime facets of the implementation of that design.

Note: This should cover both technical and operational facets of the system under review.

- 3.1.1.7 A preliminary design shall be prepared at an early stage in a project.

Note: This is to be used as the basis for the preliminary hazard assessment of the system and its application.

- 3.1.1.8 The system architecture shall be determined, having due regard for:
 - a) The required functionality;
 - b) Ease of verification and validation;
 - c) Diverse protection for critical elements of the system;
 - d) The ability of the system to sustain the required functionality throughout its lifecycle;
 - e) Normal and degraded modes of operation;
 - f) Graceful degradation to ensure safe system functioning;
 - g) The effect of human error during operation and maintenance;
 - h) Ease of modification and maintenance.
- 3.1.1.9 The design of processor based systems shall facilitate the migration to later generation units which shall be downwardly compatible, as far as this is practicable.
- 3.1.1.10 The safety and reliability of the transition between duty and standby systems shall be assessed and documented.



Note: An example of a transition would be where two processors are used with a stepped changeover activated on failure of the duty processor.

- 3.1.1.11 The design shall be analysed to show that the reliability and maintainability criteria are achievable.
- 3.1.1.12 The analysis shall document all failures capable of affecting operational availability and highlight the precautions taken and the specific features designed to mitigate the effects of failures.
- 3.1.1.13 Maintenance strategies shall be developed from the analysis to ensure that the specified system recovery and availability is achieved or exceeded.
- 3.1.1.14 All components of the safety signalling system shall be supported by the organisation which designed the system or their deputies for the designed equipment life. Functionally similar spare parts shall be provided throughout the expected life of the system. However, where equipment designs have changed, the supplier shall demonstrate that they continue to meet the safety criteria.

3.1.2 Performance

- 3.1.2.1 The achievement of the train service performance requirements contained within the specifications for the new or modified signalling system shall be recorded within the System Design Documentation.

3.1.3 Safety

- 3.1.3.1 Each system shall have defined safety goals to achieve. These shall be stated in the System Requirements Specification. The achievement of these goals shall be demonstrated.

Note: This requirement is applicable to mainline signalling, signalling control systems, depot signalling and depot control systems.

The safety goals should include factors linked to the primary purpose of train separation by a safe distance as well as those required for the application of the system to the particular environment and interfaces to systems supplied by others.

- 3.1.3.2 The safety goals shall address the safety requirements defined in Standards S1195 Signalling - Functional Requirements, and S1194, Signalling Control - Functional Requirements.
- 3.1.3.3 The system development shall include an analysis of all factors which affect the system safety, including maintenance, reliability, availability and operational issues, which can lead to potentially unsafe conditions in both normal and failure modes of the system. The analysis shall be used to ensure the occurrences of hazardous events are minimised through the system design.
- 3.1.3.4 During consideration of potential system hazards, account shall be taken of human limitations, in accordance with Standard 1-217, Integration of Human Factors into Systems Development.
- 3.1.3.5 An analysis of the signalling and signalling control systems shall be carried out during the system design phase to determine their safety integrity levels as defined in BS EN 50126.
- 3.1.3.6 Signalling interlocking system for main line applications shall be considered to be a system of Safety Integrity Level 4 as defined in BS EN 50126.



Note: It is recognised that there may be sub-systems or components of a lower Safety Integrity Level within the total system.

3.1.3.7 Application design and configuration safety issues shall be described in project-particular specifications or other associated procurement documents.

3.1.3.8 A formal process for the validation and verification of system design and safety of the signalling and signalling control system shall be implemented.

3.1.4 Health and Safety

3.1.4.1 All potential hazards to all persons on the railway shall be identified and a preliminary hazard analysis shall be performed in accordance with BS EN 50126.

Note: Items that should be addressed in the analysis include:

- a) electric shock;
- b) moving trains;
- c) hazardous substances;
- d) pressurised systems;
- e) component and equipment failures;
- f) human error in operation and maintenance operations;
- g) maintenance and repair issues.

3.1.4.2 The requirements for staff protection shall be agreed with LU Operations and the Maintainer. The agreement shall cover the location, type of mechanism to be provided and the security arrangements.

3.1.4.3 All equipment shall conform to BS 7671.

3.1.4.4 All materials used in the construction of equipment to be installed in underground or enclosed environments shall comply with Standard 1-085, Fire Safety Performance of Materials.

3.1.5 Impact on railway operations

3.1.5.1 All works associated with the introduction of a signalling or signalling control system shall be carried out in accordance with the relevant requirements of Standards S1198, Signalling and Signalling Control - Installation, Testing, Commissioning and Handover, and S1199, Signalling and Signalling Control - Operation and Maintenance.

3.1.5.2 The impact on the operation of the railway of any proposed design change to the signalling or signalling control system shall be determined by review of the LU Rule Book and its associated appendices.

3.1.5.3 The concepts and methods to be employed in any staged introduction of signalling systems shall be fully developed as part of the overall system design, and before detailed application design is commenced.

Note: During a major project it may be necessary to introduce the systems in a number of stages. These 'stageworks' should be kept to a minimum, subject to meeting LU's requirements for service continuity. The proposed stageworks should be defined in the System Requirements Specification.



- 3.1.5.4 To ensure correct application design, operation and maintenance of the system, a method of configuration control shall be devised. This shall address such issues as inter-changeability and compatibility of modular components considering the version or model number and the as built status.
- 3.1.5.5 Systems shall be designed to minimise the possibility of any incorrect connection of the system or its sub-systems.
- 3.1.5.6 The design shall ensure that interchangeable components cannot incorrectly become operational in the system.

Note: Clause 3.1.5.6 is written in the above manner to recognise that it may not in some circumstances be possible to prevent the actual fitting of an incorrect component, e.g. an Erasable Programmable Read Only Memory (EPROM) chip. In the case of an EPROM, a software solution could be used to prevent the wrongly inserted component from becoming operational. In the majority of cases it is expected that simple mechanical keying would enable the requirement to be met.

3.1.6 Signalling Systems

3.1.6.1 Functional requirements

- 3.1.6.1.1 A signalling system shall provide the appropriate functionality as defined in Standard S1195, Signalling - Functional Requirements.

3.1.6.2 Operation with Infrastructure

- 3.1.6.2.1 A signalling system shall be capable of operating in all configurations of infrastructure to which it is exposed on the Underground. The Supplier shall define and declare the limiting parameters of the design.

Note: Current infrastructure includes:

- a) Tunnel sections within cast iron or concrete lined tunnels and with suicide pits in station areas;
- b) Sub-surface sections within concrete or brick lined tunnels;
- c) Open sections on viaducts, embankments and in cuttings;
- d) A fourth rail conductor system supplying 630 Volts DC (nominally);
- e) Sections using a third rail 750 Volts DC (nominally) conductor system, as used by Network Rail on sections of the Underground where joint running with other operating authorities occurs; and
- f) Sections of lines paralleled by routes with 25 kV 50Hz AC overhead electrification or adjacent to 400kV overhead pylons are also encountered.

The design parameters of any new configuration introduced by the Supplier will be expected to be covered by clause 3.1.6.2.1

- 3.1.6.2.2 Where there is a requirement to signal trains in both directions over a length of track the system used shall be designed to the same safety integrity level for both directions of travel regardless of the technology used for the signalling system.

3.1.6.3 Table Of Controls

- 3.1.6.3.1 A Table of Controls shall be developed and maintained for each interlocking system, which fully defines the interlocking logic to be applied.



3.1.6.3.2 The table of controls shall form the core of the safety signalling design from which the circuit or logic diagrams are derived.

3.1.6.3.3 The table of controls shall present the design specification for individual signals or routes, to enable a complete understanding of when the signal can be set and cleared or points moved.

Note: These clauses are written as it applies to a fixed block signalling system. Future systems will need an equivalent document to define the signalling logic applicable to the site.

3.1.6.4 Avoidance of single point failure

3.1.6.4.1 Where a system, or sub-system implementation uses programmable devices for the achievement of highly critical safety functions, then the design shall comply with BS EN 50128 and BS EN 61508 with regard to software and hardware diversity. In all other cases, including interfaces to the above, no reliance shall be placed on a single device for achieving safety for such highly critical safety functions..

Note: Examples used to meet this requirement are:

- a) A single track circuit relay is not relied upon for the detection of trains at signal berth positions. The series TR-GR circuit is used on signalling systems which use dual element vane relays. To cater for the possibility of a track relay failing to 'drop', with a train standing on the corresponding track circuit, the 'GR' winding of a signal relay is connected in series with the 'TR' winding of the approach track of the signal ahead. This ensures that the signal behind the train is kept at danger in the event of the critical track relay malfunction.
- b) The technique of track sequencing is used to detect and to protect against mechanically jammed relays and failures of trains to shunt track circuits.
- c) The track redundancy technique is used involving two track relays with contacts of both relays in the selection of the signal, such that mechanical failure does not result in an unsafe condition.
- d) Safe operation of the signalling does not rely upon correct operation of a single interfacing relay.
- e) A dual relay which conforms to BR 930 or BR 960 is used for the interface between the AC circuitry and a safety-critical DC input or output.

3.1.6.5 Serial interfaces

Note: A processor-based interlocking system may use safety-critical serial links to other processor-based safety-critical signalling equipment, and safety-related serial links to processor-based safety-related signalling equipment and control system equipment, as required.

3.1.6.5.1 All serial links to external systems shall conform to International Telecommunication Union (ITU) standards.

3.1.6.5.2 The recommendations of BS EN 50159, and BS EN 60870-5 shall be used as guidance in the development of data transmission systems.

3.1.6.5.3 Vital serial links shall be of a highly secure nature. No error correction nor an intermediate 'store and transmit' facility is permitted in the passing of safety signalling data without a detailed safety justification being prepared to indicate that the system as a whole is designed to cover all potential failure modes.



- 3.1.6.5.4 The operation of a serial link shall be unaffected by the presence of interference from repetitive pulsed traction control systems. (Refer to section 3.4 for other general Electromagnetic Compatibility (EMC) requirements.)
- 3.1.6.5.5 The minimum data bandwidth required on the safety-related serial links shall be detailed in the System Requirements Specification. The system response time(s) where the data bandwidth is exceeded shall also be stated.
- 3.1.6.5.6 The safety-related serial link shall cause no loss or change of data if the link bandwidth is exceeded. The data in the period when the bandwidth is exceeded shall be preserved.
- 3.1.6.5.7 The error rates for these serial links shall be addressed in the system reliability assessment.

3.1.6.6 Equipment in Rooms

- 3.1.6.6.1 The signalling system shall be designed to minimise equipment that is not contained in a signalling equipment room, wherever practical.

Note: This is to allow for safe and rapid access to equipment for maintenance purposes and to provide a secure and controlled environment for the equipment.

3.1.6.7 Equipment Trackside

- 3.1.6.7.1 The design shall minimise the amount of equipment required in trackside locations.
- 3.1.6.7.2 Equipment shall be designed so that it can be installed, used and maintained without the equipment or persons using or working on it accidentally touching the traction rails.
- 3.1.6.7.3 Signalling equipment shall not obstruct depot or main line walkways.
- 3.1.6.7.4 No trackside equipment shall be mounted in such a way that it prevents a suicide pit from being used as a place of refuge in emergency situations.
- 3.1.6.7.5 All trackside equipment shall be installed so that it does not foul the railway structure gauge, such that the requirements of Standard 1-156, Gauging & Clearances, are complied with and the requirements of the LU Rule Book are met.
- 3.1.6.7.6 In so far as it is reasonably practicable equipment shall be housed such that its security is ensured.
- 3.1.6.7.7 All components of the signalling system which may be required to be disconnected as a result of a railway signalling or permanent way maintenance activity, such as cables which traverse the track and trackside signalling units, shall be fitted with a plug and socket arrangement to minimise unit replacement time and avoid the making of incorrect connections.
- 3.1.6.7.8 Trackside signalling equipment shall be adequately labelled and identified as described in Standard S1197, Signalling and Signalling Control - Design and Implementation.

3.1.6.8 Equipment on Rolling Stock

- 3.1.6.8.1 Failure of any automatic train operation function shall not have any adverse effect on any of the automatic train protection functions.
- 3.1.6.8.2 When driven from the rear cab controls, the position of the front cab operator vigilance device shall be monitored by the automatic train protection system and emergency braking commanded if the device is released.