

Category 2 Standard

S2500 Safety signalling philosophy

(Formerly E7001)

Issue No.: A3

Issue date: January 2012
Review date: January 2017

MAYOR OF LONDON

 **Documents**
Document Sharing Hub



Contents

1	Purpose	3
2	Scope	3
3	Requirements	3
3.1	Introduction	3
3.2	Assurance	3
3.3	Safety Considerations	4
3.4	Distance of Safety	4
3.5	Overlap	4
3.6	Diversity	5
3.7	Interlocking	5
3.8	Train detection	5
3.9	Capacity	5
3.10	London Underground's particular operational requirements	6
3.11	Data Transmission	7
3.12	Environmental Requirements	7
3.13	Systems Assurance	7
3.14	Processes and Procedures	9
3.15	Licensing	9
3.16	Reliability and Maintainability	10
3.17	Equipment Location	10
3.18	Renewal	11
3.19	System Implementation and Acceptance	11
3.20	Commissioning	13
3.21	Warranty	13
3.22	Design Changes to Signal Assets	13
3.23	Electromagnetic Compatibility	13
4	Responsibilities	13
5	Supporting information	14
6	References	14
6.1	Legislation and Standards	14
6.2	Abbreviations	15
6.3	Definitions	15
6.4	Requirement owner	17
6.5	Document history	17

1 Purpose

- 1.1 This standard is intended to define the underlying philosophy that shall be adopted in relationship to the life cycle of safety signalling systems to London Underground, and forms part of a group of corporate engineering standards. Quality assurance and design standards appropriate to safety critical control system development shall be followed in the application of this philosophy.

2 Scope

- 2.1 These safety standards apply to all stages of the specification, design, installation, commissioning and maintenance of all areas of the Underground's main line safety signalling systems.
- 2.2 It is not the purpose of this document to describe, in technology-specific terms, how the philosophy is to be met. Reference should be made to the Signalling Specifications for the works to be undertaken and to Section 6 (Legislation and Standards) for detailed requirements.
- 2.3 This standard replaces E7001 A2, which is withdrawn.

3 Requirements

3.1 Introduction

- 3.1.1 This standard sets out the London Underground minimum safety requirements for safety signalling systems; all intolerable risks shall be eliminated and all remaining risks shall be reduced to be as low as reasonably practicable. The standard embraces principles 20, 21 and 22 of the Office of the Rail Regulator "Railway Safety Principles and Guidance" documents, Part 1 and Part 2, section D. These cover:

Part 1, Principle 20: signalling - safe routing, spacing and control;
Part 1, Principle 21: signalling - degraded conditions; and
Part 1, Principle 22: control system – safe operation and control.

Part 2, section D gives guidance on the above principles.

- 3.1.2 The reliability of the Underground Signalling System shall be high since it is designed for high service intensity and passengers react more immediately to being held underground in the event of a failure.

3.2 Assurance

- 3.2.1 In order to meet these high standards the initial system design process shall be based on a system lifecycle which enables the implementation of the dependability requirements stated in BS EN 50126-1, these are: reliability, availability, maintainability and safety (RAMS). Guidance for BS EN 50126-1 is given in PD CLC/TR 50126-2; Railway Applications – the Specification and the Demonstration of Reliability, Availability, Maintainability and Safety (RAMS): Guide to the application of EN 50126-1 for Safety. At all stages of the design process, the consequences of component or equipment failures shall be allowed for (refer to BS EN 50128 for software and BS EN 50129 for hardware requirements), as shall the possibility of human errors in operation. The safety of the railway depends on all the component parts and hence the safety system design shall embrace the train braking and control systems, the signalling control system, the railway reference manual, the railway infrastructure and the environment as well as the signalling system itself. Account shall be taken of EMI external to the London Underground

railway, for example interference from adjacent running lines operated by other infrastructure controllers.

3.3 Safety Considerations

3.3.1 The signalling system comprises a subset of the overall transport system and shall have defined safety goals; these are defined in terms of safety functions and required levels of integrity to achieve the safe routing, spacing and control of trains. The achievement of these goals shall be demonstrated.

3.3.2 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.

3.3.3 The production of vital software shall be to BS EN 50128 and at least to Safety Integrity Level 4 defined in BS EN 50129.

3.3.4 Both the overall architecture and the individual elements of the signalling system shall, so far as practicable, be designed to minimise any feasible threat to its intended performance resulting from human error in implementation, maintenance or operation. This shall include a requirement to prevent, by design, the substitution of a physically interchangeable but functionally incorrect component.

3.3.5 Information relating to safety critical, or potential safety critical failures, shall be disseminated to other rail users and also to the original equipment manufacturer.

3.4 Distance of Safety

3.4.1 The primary requirements of the safety signalling system is to maintain a safe distance between trains such that collisions cannot occur and to minimise the risk of train derailment. In modern signalling systems the speed of the train shall be continuously monitored and speed limits vitally enforced to aid the achievement of these requirements.

3.4.2 The minimum safe distance permissible is that which will allow a train at any instant to brake and come to rest before the position at that instant of another train or other obstruction ahead. Determination of this safe braking distance requires knowledge of the track geometry/gradient, the environment and the rolling stock performance. It shall make allowance for worst case conditions, such as system response times, wheel/rail adhesion and train brake degradation.

3.4.3 The obstruction ahead shall be assumed to be stationary when calculating the safe braking distance, unless the train movements are opposing, when the speed of the approaching train shall also be included.

3.4.4 For signal overlap design, reference shall be made to engineering standard S1197, Signalling and Signalling Control – Design and Implementation.

3.5 Overlap

3.5.1 In order to maintain a safe distance between trains for fixed block signalling systems, a track section beyond the block boundary shall be calculated, known as

the 'overlap'. If a train passes the STOP command point, the overlap shall provide full protection to any other train in the area of control. The method of activating the emergency brakes under these circumstances may vary but the system shall be designed to safety principles.

- 3.5.2 The overlap will be used within the overall system design to ensure that collisions will not occur. If a single signal enforcement equipment failure occurs there shall continue to be at least one enforced signal overlap/safe braking distance between trains.
- 3.5.3 For signal overlap design, reference shall be made to engineering standard S1197, Signalling and Signalling Control – Design and Implementation.

3.6 Diversity

- 3.6.1 The signalling system shall make use of diverse means of ensuring safe operation of sub-systems in critical areas where analysis has demonstrated a high potential risk or other known areas of concern such as the primary train detection system and the 'authority to proceed' instruction.
- 3.6.2 When elements of the signalling system cannot meet the safety criteria or are considered critical to the system operation they may be subject to 'proving'. This diverse process shall monitor in a vital manner the return of an element to its safe state prior to its next use.
- 3.6.3 Diverse techniques shall, as far as reasonably practicable, be designed to reduce the risks of common mode failure and to avoid unrevealed failure modes.
- 3.6.4 The safety analysis of signalling sub-systems which use diversity shall consider the level of integrity of each system path, including the operating procedures to be used in the event of failure, to ensure acceptable levels of overall system safety.

3.7 Interlocking

- 3.7.1 London Underground's interlocking requirements may be met by processor-based or relay interlocking systems which shall conform to the latest legislation on railway related safety critical systems, and meet the LU specified safety criteria in standards S1195, Signalling – Functional Requirements and E7054, Signalling interlocking systems.

Note: LU still has a significant population of mechanical interlockings that may require modification to meet business or operational needs pending their replacement.

3.8 Train detection

- 3.8.1 The safety signalling system shall be equipped with continuous train detection as defined in standards S1195, Signalling – Functional Requirements and E7055, Train detection systems.

3.9 Capacity

- 3.9.1 The Underground system requires a high capacity service in the central area. This high capacity is defined in signalling terms by the headway requirement for these areas.
- 3.9.2 The system design shall assume station dwell values based upon the expected mean dwell time plus a minimum of one standard deviation as defined in the Specification of Works.

3.9.3 The signalling system shall be capable of returning to its required capacity in the shortest practicable time after a train service perturbation. A recovery margin shall be included in the designed service interval which equates to the ability of the design to achieve this aim.

3.9.4 During periods of service perturbation it is expected that trains will be permitted to 'close-up' on each other. This shortening of the distance between trains is permitted by the application of an enforced speed reduction, hence reducing the necessary safe braking distance. This closing-up factor is used to shorten the time taken for the signalling system to return the train service to its defined capacity. This feature will result in increased inter-station journey times and shall be optimised with the recovery capabilities in the signalling design.

3.10 London Underground's particular operational requirements

3.10.1 The development of LU's signalling systems has incorporated certain features which are particular to the London Underground railway. These features are either based upon the use of a four rail traction system or have arisen in response to earlier incidents when an improved level of safety was subsequently required.

3.10.2 The features described here shall be provided in any signalling system proposed for the Underground. This list of features shall not be regarded as complete as LU shall continue to seek methods of safety improvement through its signalling system.

a) Wrong Road Protection; At locations where trains can reverse or platforms where there is a forward movement to permit a 'shunt back' the signalling system shall prevent the movement of a train in the opposite direction to that required.

b) Remote Securing of Points; To enable train movements to take place at the time of certain equipment failures, in particular localised failure of the train detection system or flank point detection, a facility shall exist on certain signals in interlocking areas (As defined in the Specification of Works) to indicate to the train driver that the following is true:

- 1) The points in the route are detected in the required state for the route.
- 2) The interlocking lock functions are engaged for that route.
- 3) A request is received from the Signal Control System for activation of this feature at this interlocking or locality.

The route when so indicated shall remain in this state until a train on its approach has traversed the route and the Signal Control System has requested the facility be de-activated.

c) Terminal Station and Siding Protection;

The speed of a train approaching a terminal station or siding shall be controlled to the required value when nearing the stopping point. Where an ATP system is provided the protection shall be absolute.

Where train arresters are used the signalling system shall ensure that the train is normally brought to a halt in advance of the arrester.

d) Staff Protection Keyswitches;

Keyswitches shall be provided to protect staff when they have to enter areas where there is restricted clearance whilst a train service is in operation. Operation of a keyswitch shall cause signalling systems in the area