

Guidance document

G2549 Signalling and train control systems maintenance

(Formerly
M7051)

Issue No.: A4

Issue date: March 2012
Review date: March 2017

MAYOR OF LONDON

 **Documents**
Document Sharing Hub



Contents

1	Purpose	3
2	Scope	3
3	Requirements	3
3.1	Safety considerations	3
3.2	Authorisation and training requirements	3
3.3	Determining the required maintenance regime	4
3.4	Incident management	9
3.5	Asset information	12
3.6	Maintenance resources and support	14
4	Responsibilities	14
5	Supporting information	14
6	References	15
6.1	References	15
6.2	Abbreviations	15
6.3	Definitions	16
6.4	Technical content manager	16
6.5	Document history	16



1 Purpose

- 1.1 This Guidance document describes a philosophy which can form a basis for the establishment of maintenance procedures and processes, for use on London Underground signalling and train control systems, which will be acceptable to the Professional Head of Signalling. Mandatory requirements for a maintenance strategy are defined within engineering standard E7501.

2 Scope

- 2.1 The principles defined within this Guidance document, if adopted for the planning and execution of preventive maintenance, incident management and fault rectification for signalling and train control systems on LU, would satisfy the current requirements of engineering standard E7051. The principles should be applied to new signalling and control systems at all stages of their lifecycle, and to existing systems where applicable.

3 Requirements

3.1 Safety considerations

- 3.1.1 Due to the safety critical nature of signalling assets safe systems of work should be devised. The systems of work should be based on appropriate risk assessment techniques to identify the particular hazards (such as electric shock, moving trains and hazardous substances) and to assess the effectiveness of the proposed safeguards.
- 3.1.2 Everyone concerned in specifying, carrying out or monitoring maintenance activities should be regularly reminded of the vital nature of their role, and that inadequate or improper maintenance activities may lead directly or indirectly to collision or derailment, or to serious loss of process.
- 3.1.3 Due consideration should be given to customer safety when conducting maintenance activities in or near public areas.

3.2 Authorisation and training requirements

3.2.1 Licensing

- 3.2.1.1 All staff are presently assessed to be competent to work on signalling assets this is achieved by the requirements defined in engineering standard S1203.

3.2.2 Task authorisation and certification

- 3.2.2.1 Engineering standard E7500 defines the mechanism by which disturbance to the function of an asset is sanctioned in advance through the issue of an Authority to Work Certificate.

3.2.3 Training

- 3.2.3.1 Training should be supplemented by field experience and workplace assessment before licences are issued.
- 3.2.3.2 Where a novel system is being introduced and there is no opportunity for field experience in the LU environment, then simulation, related operational experience, involvement with the pre-commissioned system, and other similar methods should be employed to bridge the gap as far as possible.
- 3.2.3.3 Whenever new systems are introduced appropriate training facilities and materials should be provided, and the necessary training carried out before the systems are

brought into use. It is important that the training addresses not only the technical issues but also the procedures needed for working in the railway environment. This should not be overlooked in cases where systems are initially maintained by a supplier during a warranty period.

3.3 Determining the required maintenance regime

3.3.1 Fundamental requirements

3.3.1.1 The overall system requirements, safety and availability performance, are the starting point in determining the maintenance regime. The factors in sections 3.3.2 and 3.3.3 should be fully considered in the process.

3.3.1.2 Safety and availability performance requirements will normally be specified as MTBF, MTTR. Alternatively MTBM and MDT are used, if planned maintenance downtime is included as well as corrective maintenance and MTBWSF figures. The Project Requirements Definition, or in particular system or application standards or specifications should define the minimum requirements.

3.3.1.3 The maintenance regime should be subject to review and under the control of a suitable management system, itself subject to programmed review and audit (See section 3.3.7).

The maintenance regime should be reviewed:

- a) routinely at intervals to re-validate the basic assumptions and the suitability of the regime;
- b) in advance of significant planned changes to the system;
- c) following incidents or other evident shortcomings.

Processes should be established to enable maintainers to report potential deficiencies in the regime and for these to be considered.

3.3.2 Safety criteria

3.3.2.1 The safety aspects of maintenance should not be considered in isolation, but should be seen in relation to the whole of the safety lifecycle, embodying and sustaining the system safety requirements and integrity levels which the designer sought to achieve. Guidance on the safety lifecycle may be found in BS EN 61508-1.

3.3.2.2 The implications of the following factors should be addressed when determining the maintenance regime:

- a) System safety functions
 - i) the allocation of safety functions between mechanical, electrical, electronic, programmable, and procedural sub-systems;
 - ii) the modes of degradation that can affect each sub-system;
 - iii) the extent of diverse or redundant protection against unsafe conditions.
- b) Required safety integrity levels
 - i) the integrity levels that should be achieved by each of the sub-systems involved (including the human factors aspects of any procedural functions) in order to meet the required overall system integrity level;
 - ii) the effect on the safety integrity levels of the various modes and degrees of degradation that can affect each sub-system, both singly and in

credible combination, including consideration of the maximum period for which degradation of one channel of a diverse protection arrangement may be permitted to remain undetected (and uncorrected) without unacceptable loss of total system integrity;

- iii) the rate at which the degradation is likely to occur, and its predictability;
- iv) the point at which the degradation becomes detectable (by visual observation, instrumented tests, remote monitoring),
- v) self-indicating loss of function, or other means), and the margin of safety that remains at that point;
- vi) the effect on the total system safety integrity levels of placing the affected sub-system into a non-operational 'safe' state pending restoration;
- vii) the scope for acceptably safe operation of the railway under alternative protective arrangements (backup systems, emergency rules, procedures, etc), pending restoration;
- viii) the feasibility of on-site restoration.

3.3.3 Availability criteria

3.3.3.1 The availability required by the operator to meet the service needs may be specified in a number of different ways, such as:

a) Operational Availability (OA)

This can be defined as the probability that the system, at any given instant of time over a given time interval, is in a state to perform the required function, under stated conditions, either disregarding or taking account of planned downtime for preventive maintenance.

- i) The ratio of Actual Operating Time (AOT), which excludes actual down time (DT), to the scheduled Operating Time (SOT), thus $OA = AOT/SOT = (SOT-DT)/SOT$

- ii) Inherent Availability (Ia), or Achieved Availability (Aa)

Inherent Availability (Ia), or Achieved Availability (Aa) can be calculated using the following: $Ia = MTBF / (MTBF + MTTR)$ or $Aa = MTBM / (MTBM + MDT)$

b) Schedule Adherence (SA)

- i) Is the probability that any given trip ends at the intended destination within a stated time allowance of the schedule:
- ii) $SA = \text{Number of successful trips} / \text{Number of scheduled trips}$

3.3.3.2 The precise definition of availability terms may vary from contract to contract. For example, a system is sometimes regarded as 'available' if it does not cause delay to the service pattern which the operator chooses to employ, and 'unavailability' may, or may not, include time for which a facility which is not presently required is not working. Similarly, a temporary repair which provided the necessary functionality would generally be regarded as restoring availability, even though the system is not yet fully returned to its 'as designed' state. In some cases, unavailability may be defined in such a way that it excludes the time for which the operator chooses not to allow the repairer access to the equipment (to avoid greater disruption).

3.3.3.3 Other parameters may be specified, e.g.

- a) the maximum permitted response time to provide technician attendance at the site of a service failure;
- b) the maximum allowable duration of any one period of service down time (before service can be resumed, possibly in a limited or degraded mode).

3.3.3.4 Satisfying the availability criteria will generally require a maintenance regime that is more intensive in at least some respects than that determined by the safety criteria alone. The following factors will typically need to be considered in determining the maintenance regime:

- a) the degree of fault tolerance in the system design;
- b) the location and accessibility of the system components;
- c) the range, predictability and probability of failure modes;
- d) the extent of built in test facilities or remote monitoring of asset condition;
- e) the typical and likely maximum times to diagnose and remedy particular failure modes;
- f) the degree of likely service disruption, and hence the impact, of particular sub - system failures.
- g) availability of technicians/supervisors:
 - i) numbers
 - ii) locations
 - iii) shift patterns
- h) availability of technician resources:
 - i) transport facilities
 - ii) communications facilities
 - iii) site specific drawings, manuals, etc
 - iv) specialist tools, test equipment, etc
- i) availability of spares:
 - i) stock holding
 - ii) locations
 - iii) transport arrangements
- j) availability of technical back-up:
 - i) ease of contact with back-up staff
 - ii) degree of expertise available extent of information and facilities available to them.