

Category 1 Standard

S1210

Safety-Related Software

Issue No.: A2

Issue date: March 2014

Review date: March 2019

Contents

1	Purpose	3
2	Scope	3
3	Requirements	4
3.1	System Safety	4
3.2	Safety Software	4
3.3	Safety Software Security	6
4	Responsibilities	6
4.1	Procurement Agent (PE/SE)	6
4.2	Project or Programme Manager	6
4.3	System Engineer Manager	7
5	Supporting information	7
5.1	System Safety considerations	7
5.2	Software development and SIL analysis	7
5.3	Software security considerations	8
5.4	Environmental considerations	8
6	References	8
6.1	References	8
6.2	Abbreviations	9
6.3	Definitions	10
6.4	Person accountable for the document	11
6.5	Document history	11

1 Purpose

The purpose of this standard is to define the requirements for the development and modification of all software that supports railway safety-related functions.

2 Scope

- 2.1.1 This standard applies to the development, modification or bringing in to use of safety-related software on the railway.
- 2.1.2 It applies to the tools or methods used for the derivation, preparation or verification of software code, data, and supporting information (e.g. configuration).
- 2.1.3 Additionally, this standard applies to the tools that are used to develop or control deployment of safety-related software (e.g. software updates).
- 2.1.4 The scope also includes the interface with operational and maintenance systems, including the interface to people who may use the software as part of a safety function.
- 2.1.5 This standard applies equally to both external suppliers and LU internal teams.
- 2.1.6 The requirements of this standard form part of the assurance of railway safety, and the standard supports the railway safety assurance processes and LU category 1 standard S1538.
- 2.1.7 The requirements of this standard are not applied retrospectively to projects that are underway at the time of issue, or have been assured through prior software safety standards. The standard shall typically apply to subsequent changes (but see note 5 below).

Note 1: The scope of this standard is limited to software that supports safety functions in the context of an operational railway. This excludes non-safety related information management and support functions that are regarded as business systems, back-office, and non-operational IT information systems.

Note 2: Depots and maintenance areas are included in the scope.

Note 3: Applicability is typically determined through an impact assessment of the changes proposed to the current system, specifically in relation to the safety functions that the current and modified systems support.

Note 4: This standard applies to all safety related software used in railway control and protection systems, including

- application programming,
- operating systems,
- support tools,
- firmware.

Note 5: Changes to software (systems) that have been developed and assured to a prior software safety standard (including BS EN 50128) require careful consideration as to which standard applies. A risk-based approach should be taken to determine the potential safety impacts of not applying the new standards, versus the practicalities of introducing new process controls (including the cost and impact on the development team). The safety case for the proposed changes should present a rationale and justification for the selected approach, including an evaluation of the risks and the mitigations that reduce those risks. By default, the new standards apply.

3 Requirements

3.1 System Safety

- 3.1.1 This standard mandates the use of BS EN 50129 for the overall approach to the management of system safety, of which the software forms a part.
- 3.1.2 This standard mandates the use of BS EN 50126-1 for the identification and assessment of hazards and allocation of SILs including the software SIL apportionment.
- 3.1.3 All railway application software within the scope of this standard shall be considered as needing to meet Safety Integrity Level SIL-0 requirements as a minimum, unless it can be demonstrated that the specific application (including interfaces) has no safety impact (non-SIL) and does not interface to other systems that have safety functions.

Note 6: BS EN 50126 and BS EN 50129 require a systematic approach be taken to

- a) identify hazards, assess risks and arrive at decisions based on risk criteria;
- b) identify the necessary risk reduction to meet the risk acceptance criteria;
- c) define an overall System Safety Requirements Specification for the safeguards necessary to achieve the required risk reduction;
- d) select a suitable system architecture,
- e) plan, monitor and control the technical and managerial activities necessary to translate the System Safety Requirements Specification into a Safety-Related System of a validated safety integrity.

3.2 Safety Software

- 3.2.1 For Railway Applications this standard mandates the use of BS EN 50128:2011 for software quality management and control processes, and the selection and application of software engineering techniques.