ILNAS

Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN 50128:2001

Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems

Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Logiciels pour systèmes de commande et de protection

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Software

03/2001

National Foreword

This European Standard EN 50128:2001 was adopted as Luxembourgish Standard ILNAS-EN 50128:2001.

Every interested party, which is member of an organization based in Luxembourg, can participate for FREE in the development of Luxembourgish (ILNAS), European (CEN, CENELEC) and International (ISO, IEC) standards:

- Participate in the design of standards
- Foresee future developments
- Participate in technical committee meetings

https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html

EUROPEAN STANDARD **EN 50128**

NORME EUROPÉENNE

EUROPÄISCHE NORM March 2001

ICS 29.280; 45.060.10

English version

Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems

Applications ferroviaires -
Systèmes de signalisation, de télécommunication et de traitement -
Logiciels pour systèmes de commande et de protection ferroviaire

Bahnanwendungen -
Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme -
Software für Eisenbahnsteuerungs- und Überwachungssysteme

This European Standard was approved by CENELEC on 2000-11-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

CENELEC
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Foreword

This European Standard was prepared by SC 9XA, Communication, signalling and processing systems, of Technical Committee CENELEC TC 9X, Electrical and electronic applications for railways.

The text of the draft was submitted to the formal vote and was approved by CENELEC as EN 50128 on 2000-11-01.

The following dates were fixed:

- latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2001-11-01
- latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2003-11-01

This European Standard should be read in conjunction with EN 50126: "Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)" and EN 50129: "Railway applications - Safety related electronic systems for signalling".

Annexes designated "normative" are part of the body of the standard.
Annexes designated "informative" are given for information only.
In this standard, annex A is normative and annex B is informative.

Contents

Pages

Figures

Introduction

This Standard is part of a group of related Standards. The others are EN 50126 "Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)" and EN 50129 "Railway applications - Safety related electronic systems for signalling". EN 50126 addresses system issues on the widest scale, while EN 50129 addresses the approval process for individual systems which may exist within the overall railway control and protection system. This Standard concentrates on the methods which need to be used in order to provide software which meets the demands for safety integrity which are placed upon it by these wider considerations.

This Standard owes much of its direction to earlier work done by Working Group 9 of IEC/TC 65. The work of WG 9 resulted in a generic standard for software for safety systems which is now part of IEC 61508. A particular aspect of the work by WG 9 is its inclusion of Software Integrity Level 0, which covers non-safety software, as well as Software Integrity Levels 1 to 4, which cover safety-related and safety-critical software. This Standard also covers all five Software Integrity Levels.

Account has also been taken of the work of the Institution of Railway Signal Engineers (the IRSE), in particular its Technical Report Number 1, which addressed the same topic.

The key concept of this European Norm is that of levels of software safety integrity. The more dangerous the consequences of a software failure, the higher the software safety integrity level will be.

This European Standard has identified techniques and measures for 5 levels of software safety integrity where 0 is the minimum level and 4 the highest level. Four of these levels, 1 to 4, refer to safety-related software, whilst level 0 refers to non safety-related software. This level has been included as normative in order to allow a smooth transition between software developments for non-safety related systems and those for safety-related systems. The required techniques and measures for each software safety integrity level and for the non safety-related level are shown in the tables. In this version, the required techniques for level 1 are the same as for level 2, and the required techniques for level 3 are the same as for level 4. This European Standard does not give guidance on which level of software integrity is appropriate for a given risk. This decision will depend upon the many factors including the nature of the application, the extent to which other systems carry out safety functions and social and economic factors.

It is the function of EN 50126 and EN 50129 to specify the safety functions allocated to software.

This European Standard specifies those measures necessary to achieve these requirements. The process is illustrated in Figure 1.

EN 50126 and EN 50129 require that a systematic approach be taken to:

i) identifying hazards, risks and risk criteria;

ii) identifying the necessary risk reduction to meet the risk criteria;

iii) defining an overall System Safety Requirements Specification for the safeguards necessary to achieve the required risk reduction;

iv) selecting a suitable system architecture;

v) planning, monitoring and controlling the technical and managerial activities necessary to translate the System Safety Requirements Specification into a Safety-Related System of a validated safety performance (or safety integrity).

As decomposition of the specification into a design comprising safety-related systems and components takes place, further allocation of safety integrity levels is performed. Ultimately this leads to the required software safety integrity levels.

The current state-of-the-art is such that neither the application of quality assurance methods (so-called fault avoiding measures) nor the application of software fault tolerant approaches can guarantee the absolute safety of the system. There is no known way to prove the absence of faults in reasonably complex safety-related software, especially the absence of specification and design faults.

The principles applied in developing high integrity software include, but are not restricted to:

- top-down design methods;
- modularity;
- verification of each phase of the development lifecycle;
- verified modules and module libraries;
- clear documentation;
- auditable documents; and
- validation testing.

These and related principles must be correctly applied. This standard specifies the level of assurance required to demonstrate this at each software safety integrity level.

After the System Safety Requirements Specification, which identifies all safety functions allocated to software and determines the system safety integrity level, has been obtained or produced, the functional steps in the application of this European Standard are shown in Figure 2 and are as follows:

i) define the Software Requirements Specification and in parallel consider the software architecture. the software architecture is where the basic safety strategy is developed for the software and the software safety integrity level (clauses 5, 8 and 9);

ii) design, develop and test the software according to the Software Quality Assurance Plan, software safety integrity level and the software lifecycle (clause 10);

iii) integrate the software on the target hardware (clause 12);

iv) validate the software (clause 13);

v) if software maintenance is required during operational life then re-activate this European Standard as appropriate (clause 16).

A number of activities run across the software development. These include verification (clause 11), assessment (clause 14) and quality assurance (clause 15).

Requirements are given for systems which are configured by application data (clause 17).

Requirements are also given for the competency of staff involved in software development (clause 6).

The standard does not mandate the use of a particular software development lifecycle. However a recommended lifecycle and documentation set are given (clause 7 and Figures 3 and 4).

Tables have been formulated ranking various techniques/measures against the 5 software safety integrity levels. The tables are in annex A. Cross-referenced to the tables is a bibliography giving a brief description of each technique/measure with references to further sources of information. The bibliography is in annex B.

1 Scope

1.1 This European Standard specifies procedures and technical requirements for the development of programmable electronic systems for use in railway control and protection applications. It is aimed at use in any area where there are safety implications. These may range from the very critical, such as safety signalling to the non-critical, such as management information systems. These systems may be implemented using dedicated microprocessors, programmable logic controllers, multiprocessor distributed systems, larger scale central processor systems or other architectures.

1.2 This European Standard is applicable exclusively to software and the interaction between software and the system of which it is part.

1.3 Software safety integrity levels above zero are for use in systems in which the consequences of failure could include loss of life. Economic or environmental considerations, however, may also justify the use of higher software safety integrity levels.

1.4 This European Standard applies to all software used in development and implementation of railway control and protection systems including:

application programming;

operating systems;

support tools;

firmware.

Application programming comprises high level programming, low level programming and special purpose programming (for example: Programmable Logic Controller ladder logic).

1.5 The use of standard, commercially available software and tools is also addressed in this European Standard.

1.6 This European Standard also addresses the requirements for systems configured by application data.

1.7 This European Standard is not intended to address commercial issues. These should be addressed as an essential part of any contractual agreement. All the clauses of this European Standard will need careful consideration in any commercial situation.

1.8 This European Standard is not intended to be retrospective. It therefore applies primarily to new developments and only applies in its entirety to existing systems if these are subjected to major modifications. For minor changes, only clause 16 applies.

2 Normative references

This European Standard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this European Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies (including amendments).

EN 50126	Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
EN 50129*	Railway applications - Safety related electronic systems for signalling

* at draft stage