IEC 62279

Edition 2.0 2015-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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 ferroviaire

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 45.060

ISBN 978-2-8322-2741-1

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

RAILWAY APPLICATIONS – COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS – SOFTWARE FOR RAILWAY CONTROL AND PROTECTION SYSTEMS

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62279 has been prepared by IEC technical committee 9: Electrical equipment and systems for railways.

This standard is based on EN 50128:2011.

This second edition cancels and replaces the first edition, issued in 2002. It constitutes a technical revision.

The main technical changes with respect to the previous edition are as follows:

- requirements on software management and organisation, definition of roles and competencies, deployment and maintenance have been added;
- a new subclause on tools has been inserted in 6.7, based on IEC 61508-2:2010;
- tables in Annex A have been updated;
- a new Annex B on key software roles and responsibilities has been introduced;

- a new Annex C on document control summary has been introduced;
- Annex B on Bibliography of techniques has been revised and updated as new Annex D.

The main changes with respect to EN 50128:2011 are listed below:

- the subclause on tools in 6.7 has been updated;
- Annex B on key software roles and responsibilities has been modified.

The text of this standard is based on the following documents:

FDIS	Report on voting
9/2023/FDIS	9/2046/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

This Standard should be read in conjunction with IEC 62278:2002, *Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS).*

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

INTRODUCTION

This Standard is part of a group of related standards. The others are IEC 62278:2002, *Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)* and IEC 62425:2007, *Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*.

IEC 62278:2002 addresses system issues on the widest scale, while IEC 62425:2007 addresses the approval process for individual systems which can 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 provides a set of requirements with which the development, deployment and maintenance of any safety-related software intended for railway control and protection applications should comply. It defines requirements concerning organisational structure, the relationship between organisations and division of responsibility involved in the development, deployment and maintenance activities. Criteria for the qualification and expertise of personnel are also provided in this Standard.

The key concept of this Standard is that of levels of software integrity. This Standard addresses five software safety integrity levels where SIL 0 is the lowest and SIL 4 the highest safety related integrity levels. The higher the risk resulting from software failure, the higher the software safety integrity level will be.

This Standard has identified techniques and measures for the five levels of software integrity. The required techniques and measures for software Safety Integrity Levels 0 to 4 are shown in the normative tables of Annex A. In this standard, 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 Standard does not give guidance on which level of software integrity is appropriate for a given risk. This decision will depend upon 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 within the scope of IEC 62278 and IEC 62425 to define the process of specifying the safety functions allocated to software.

This Standard specifies those measures necessary to achieve these requirements.

IEC 62278 and IEC 62425 require that a systematic approach be taken to:

a) identify hazards, assessing risks and arriving 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 Safety Requirements Specification into a Safety-Related System of a validated 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 and fault detecting measures) nor the application of

software fault tolerant approaches can guarantee the absolute safety of the software. 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 components and component libraries,
– clear documentation and traceability,
– auditable documents,
– validation,
– assessment,
– configuration management and change control, and
– appropriate consideration of organisation and personnel competency issues.

The System Safety Requirements Specification identifies all safety functions allocated to software and determines their safety integrity level. The successive functional steps in the application of this Standard are shown in Figure 1 and are as follows:

a) define the Software Requirements Specification and in parallel consider the software architecture. The software architecture is where the safety strategy is developed for the software and the software safety integrity level (7.2 and 7.3);
b) design, develop and test the software according to the Software Quality Assurance Plan, software safety integrity level and the software lifecycle (7.4 and 7.5);
c) carry out software/software and software/hardware integration on the target hardware and verify functionality (7.6);
d) accept and deploy the software (7.7 and 9.1);
e) if software maintenance is required during operational life then re-activate this Standard as appropriate (9.2).

A number of activities run across the software development. These include testing (6.1), verification (6.2), validation (6.3), assessment (6.4), quality assurance (6.5) and modification and change control (6.6).

Requirements are given for support tools (6.7) and for systems which are configured by application data or algorithms (Clause 8).

Requirements are also given for the independence of roles and the competence of staff involved in software development (5.1, 5.2 and Annex B).

This Standard does not mandate the use of a particular software development lifecycle. However, illustrative lifecycle and documentation sets are given in 5.3, Figure 3 and Figure 4 and in 7.1.

Tables have been formulated ranking various techniques/measures against the 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 of techniques is in Annex D.

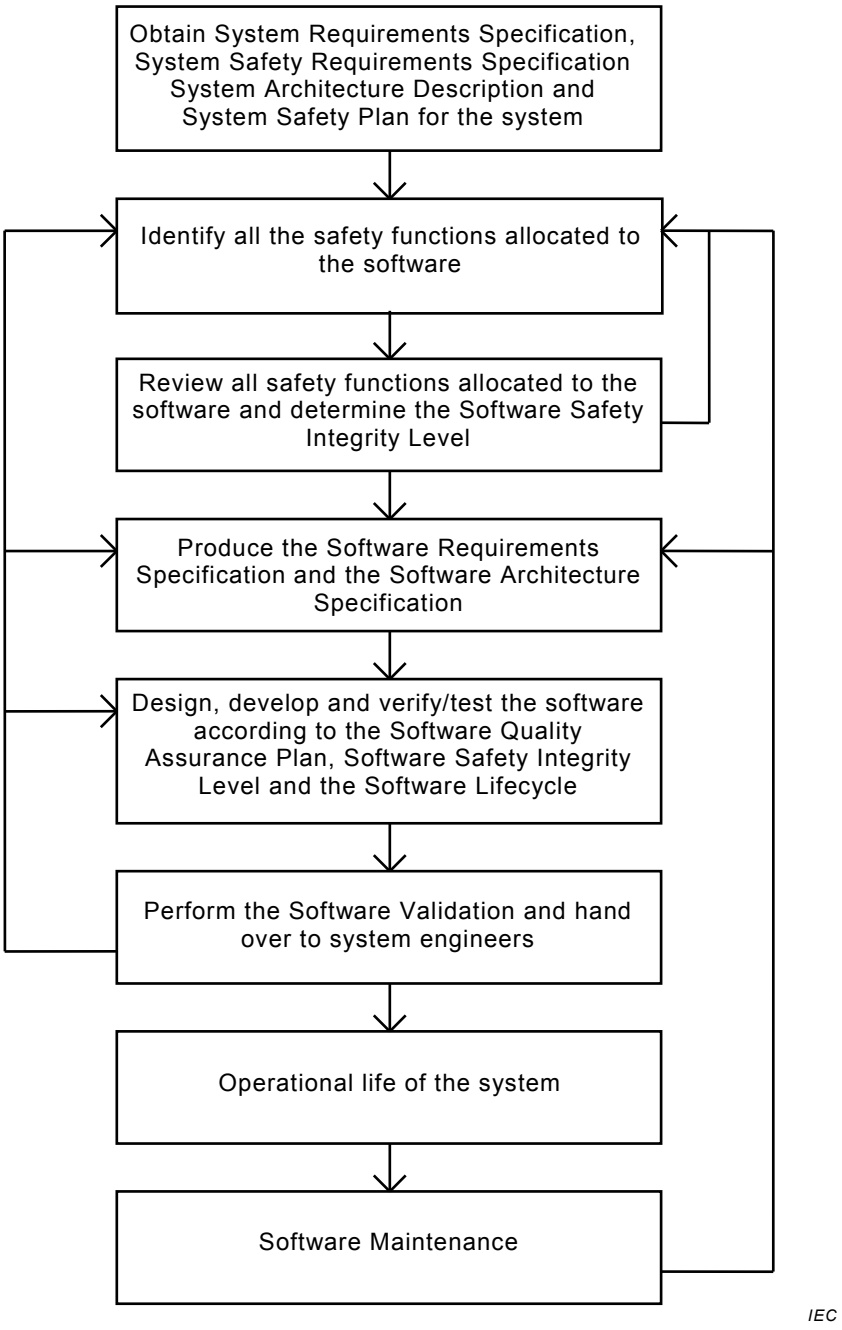


Figure 1 – Illustrative software route map

RAILWAY APPLICATIONS – COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS – SOFTWARE FOR RAILWAY CONTROL AND PROTECTION SYSTEMS

1 Scope

1.1 This International Standard specifies the process and technical requirements for the development of software for 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 systems can be implemented using dedicated microprocessors, programmable logic controllers, multiprocessor distributed systems, larger scale central processor systems or other architectures.

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

1.3 This Standard is not relevant for software that has been identified as having no impact on safety, i.e. software of which failures cannot affect any identified safety functions. The concept of SIL 0 is introduced because uncertainty is present in the evaluation of the risk, and even in the identification of hazards. At least the SIL 0 requirements of this Standard are fulfilled for the software part of functions that have a safety impact below SIL 1.

1.4 This Standard applies to all safety related software used in 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 This Standard also addresses the use of pre-existing software and tools. Such software may be used, if the specific requirements in 7.3.4.7 and 6.5.4.16 on pre-existing software and for tools in 6.7 are fulfilled.

1.6 Software developed according to any version of this Standard will be considered as compliant and not subject to the requirements on pre-existing software.

1.7 This Standard considers that modern application design often makes use of generic software that is suitable as a basis for various applications. Such generic software is then configured by data, algorithms, or both, for producing the executable software for the application. The general Clauses 1 to 6 and 9 of this Standard apply to generic software as well as for application data or algorithms. The specific Clause 7 applies only for generic software while Clause 8 provides the specific requirements for application data or algorithms.

1.8 This 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 Standard will need careful consideration in any commercial situation.

1.9 This 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 9.2 applies. The assessor analyses the

evidences provided in the software documentation to confirm whether the determination of the nature and scope of software changes is adequate. However, application of this Standard during upgrades and maintenance of existing software is highly recommended.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62278:2002, *Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)*

ISO/IEC 90003:2014, *Software engineering – Guidelines for the application of ISO 9001:2008 to computer software*

ISO/IEC 25010 series, *Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models*

ISO 9000, *Quality management systems – Fundamentals and vocabulary*

ISO 9001:2008, *Quality management systems – Requirements*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

APPLICATIONS FERROVIAIRES – SYSTÈMES DE SIGNALISATION, DE TÉLÉCOMMUNICATION ET DE TRAITEMENT – LOGICIELS POUR SYSTÈMES DE COMMANDE ET DE PROTECTION FERROVIAIRE

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 62279 a été établie par le comité d'études 9 de l'IEC: Matériels et systèmes électriques ferroviaires.

La présente norme est basée sur l'EN 50128:2011.

Cette deuxième édition annule et remplace la première édition, parue en 2002, dont elle constitue une révision technique.

Les modifications techniques majeures par rapport à l'édition précédente sont les suivantes:

- des exigences relatives à la gestion et à l'organisation, à la définition des rôles et des compétences, au déploiement et à la maintenance des logiciels ont été ajoutées;

- un nouveau paragraphe concernant les outils a été ajouté en 6.7, fondé sur l'IEC 61508-2:2010;
- les tableaux en Annexe A ont été mis à jour;
- une nouvelle Annexe B concernant les principaux rôles et responsabilités relatifs au logiciel a été introduite;
- une nouvelle Annexe C concernant le résumé du contrôle des documents a été introduite;
- l'Annexe B concernant la Bibliographie des techniques a été révisée et mise à jour comme nouvelle Annexe D.

Les modifications majeures par rapport à l'EN 50128:2011 sont énumérées ci-après:

- l'article concernant les outils en 6.7 a été mis à jour;
- l'Annexe B concernant les principaux rôles et responsabilités relatifs au logiciel a été modifiée.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
9/2023/FDIS	9/2046/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Cette norme doit être utilisée conjointement avec l'IEC 62278:2002, *Applications ferroviaires – Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)*.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

INTRODUCTION

La présente Norme fait partie intégrante d'un groupe de normes connexes. Les autres sont l'IEC 62278:2002, *Applications ferroviaires – Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)* et l'IEC 62425:2007, *Applications ferroviaires – Systèmes de signalisation, de télécommunications et de traitement – Systèmes électroniques de sécurité pour la signalisation*.

L'IEC 62278:2002 traite des systèmes au niveau le plus général, tandis que l'IEC 62425:2007 traite des processus d'approbation des systèmes individuels qui peuvent exister dans le cadre du système ferroviaire global de contrôle-commande et de protection. La présente Norme traite en particulier des méthodes à utiliser pour fournir des logiciels répondant aux exigences d'intégrité de la sécurité imposées par ces considérations plus larges.

La présente Norme fournit un ensemble d'exigences qu'il convient qu'il soit respecté par le développement, le déploiement et la maintenance de tout logiciel de sécurité destiné aux applications ferroviaires de contrôle-commande et de protection. Elle définit les exigences concernant la structure organisationnelle, la relation entre organisations et la répartition des responsabilités impliquées dans les activités de développement, de déploiement et de maintenance. Des critères de qualification et d'expertise du personnel sont également fournis dans la présente Norme.

Le concept-clé de la présente Norme est celui des niveaux d'intégrité de logiciel. La présente Norme traite de cinq niveaux d'intégrité de la sécurité logicielle dans lesquels SIL 0 correspond au niveau d'intégrité de sécurité le plus bas et SIL 4 au niveau le plus élevé. Plus le risque résultant d'une défaillance logicielle est élevé, plus le niveau d'intégrité de la sécurité logicielle est élevé.

La présente Norme a identifié des techniques et mesures applicables aux cinq niveaux d'intégrité de la sécurité logicielle. Les techniques et mesures requises pour les Niveaux d'intégrité de la sécurité logicielle 0 à 4 sont indiquées dans les tableaux normatifs de l'Annexe A. Dans la présente norme, les techniques requises pour le niveau 1 sont identiques à celles du niveau 2, et les techniques requises pour le niveau 3 sont identiques à celles du niveau 4. La présente Norme ne fournit aucune ligne directrice sur le niveau d'intégrité logicielle approprié pour un risque donné. Cette décision sera tributaire de nombreux facteurs, notamment de la nature de l'application, de la limite dans laquelle les autres systèmes assurent des fonctions de sécurité ainsi que de facteurs socio-économiques.

Le processus de spécification des fonctions de sécurité allouées au logiciel est défini dans le domaine d'application des normes IEC 62278 et IEC 62425.

La présente Norme spécifie les mesures nécessaires au respect de ces exigences.

L'IEC 62278 et l'IEC 62425 exigent qu'une approche systématique soit adoptée pour ce qui concerne:

a) l'identification des dangers, l'évaluation des risques et la prise de décisions en fonction de critères de risque,

b) l'identification de la réduction des risques nécessaire au respect des critères d'acceptation de risque;

c) la définition d'une Spécification des Exigences de Sécurité du Système, globale, qui décrit les protections indispensables en vue d'atteindre la réduction des risques requise,

d) le choix d'une architecture système adaptée,

e) la planification, le contrôle et la maîtrise des activités techniques et de management nécessaires pour transformer la Spécification des exigences de sécurité en un Système de sécurité dont l'intégrité de la sécurité est validée.

Au fur et à mesure que la spécification se décompose en une conception comprenant des composants et des systèmes relatifs à la sécurité, l'affectation des niveaux d'intégrité de la sécurité est effectuée. Finalement, cela conduit aux niveaux d'intégrité de la sécurité logicielle requis.

L'état actuel de la technique est tel que ni l'application des méthodes d'assurance qualité (mesures d'évitement des défauts et mesures de détection des défauts), ni l'application d'approches logicielles à tolérance aux pannes ne peuvent garantir la sécurité absolue du logiciel. Il n'existe aucun moyen connu de prouver l'absence de défauts dans un logiciel relatif à la sécurité raisonnablement complexe, en particulier l'absence de défauts de spécification et de conception.

Les principes appliqués dans le développement de logiciels à haute intégrité incluent, sans s'y limiter:

– des méthodes de conception descendante,
– la modularité,
– la vérification de chaque phase du cycle de vie du développement,
– des composants vérifiés et des bibliothèques de composants,
– une documentation claire et la traçabilité,
– des documents aptes à être audités,
– la validation,
– l'évaluation,
– la gestion de configuration et le contrôle des modifications, et
– l'étude appropriée des questions de compétence de l'organisation et du personnel.

La Spécification des exigences de sécurité du système identifie toutes les fonctions de sécurité allouées au logiciel et détermine leur niveau d'intégrité de la sécurité. Les étapes fonctionnelles successives de l'application de la présente Norme sont montrées à la Figure 1 et consistent à:

a) définir la Spécification des Exigences du Logiciel et, en parallèle, considérer l'architecture du logiciel. La stratégie de sécurité pour le logiciel et le niveau d'intégrité de la sécurité logicielle (7.2 et 7.3) sont développés dans l'architecture du logiciel;
b) concevoir, développer et soumettre à essai le logiciel selon le Plan d'Assurance Qualité du Logiciel, le niveau d'intégrité de la sécurité logicielle et le cycle de vie du logiciel (7.4 et 7.5);
c) mener à bien l'intégration logiciel/logiciel et l'intégration logiciel/matériel sur le matériel cible et vérifier la fonctionnalité (7.6);
d) accepter et déployer le logiciel (7.7 et 9.1);
e) si la maintenance du logiciel est requise pendant la vie opérationnelle, réactiver, le cas échéant, la présente Norme (9.2).

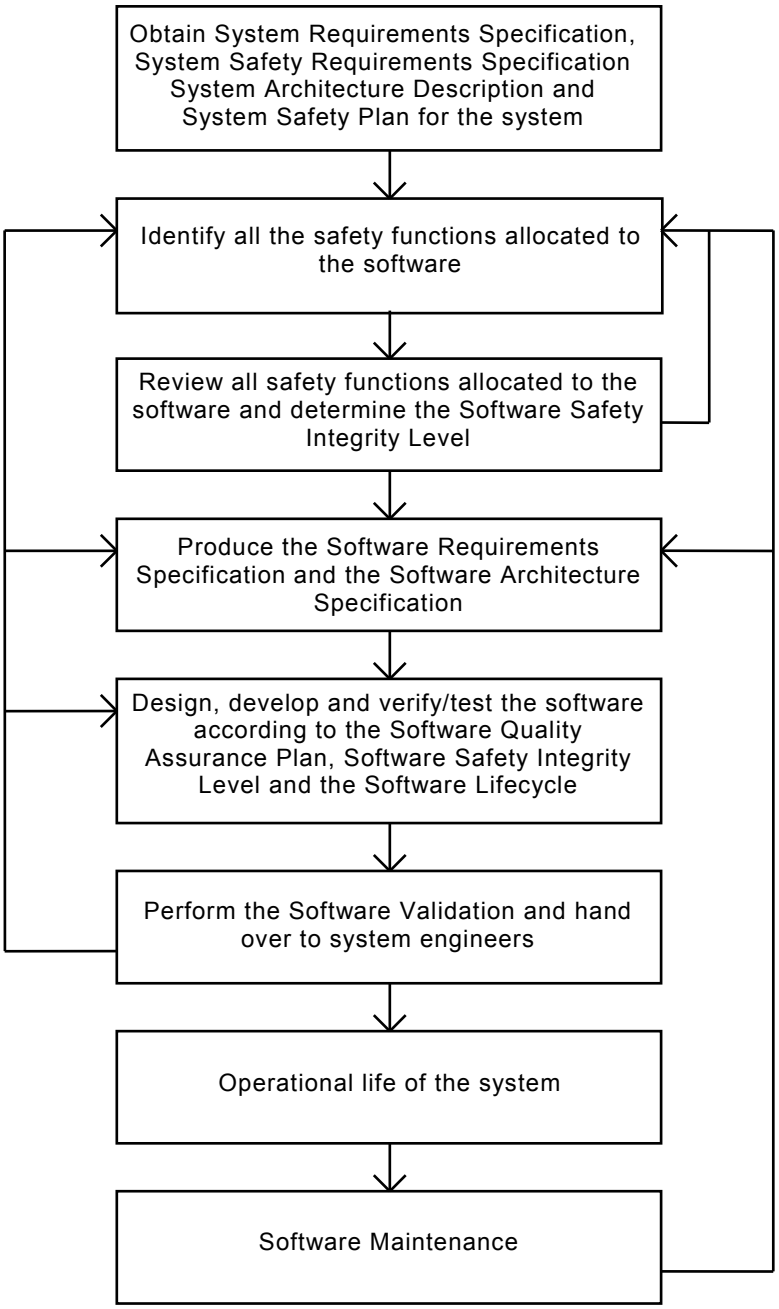
Un certain nombre d'activités se déroulent au cours du développement du logiciel, parmi lesquelles les essais (6.1), la vérification 6.2), la validation (6.3), l'évaluation (6.4), l'assurance qualité (6.5) et le contrôle des modifications et des évolutions (6.6).

Des exigences sont données en ce qui concerne les outils (6.7) et les systèmes qui sont configurés par des données d'application ou par des algorithmes d'application (Article 8).

Des exigences sont également fournies en ce qui concerne l'indépendance des rôles et la compétence du personnel impliqué dans le développement du logiciel (5.1, 5.2 et Annexe B).

La présente Norme n'impose pas l'utilisation d'un cycle de vie spécifique de développement du logiciel. Cependant des ensembles illustratifs de cycle de vie et de documentation sont fournis en 5.3 (Figure 3 et Figure 4) et en 7.1.

Des tableaux ont été établis pour classer diverses techniques/mesures par rapport aux niveaux d'intégrité de la sécurité logicielle. Les tableaux sont donnés en Annexe A. En référence croisée avec les tableaux, la bibliographie fournit une brève description de chaque technique/mesure avec des références à des sources complémentaires d'informations. La Bibliographie de techniques est donnée en Annexe D.



Anglais	Français
Obtain System Requirements Specification, System Safety Requirements Specification, System Architecture Description and System Safety Plan for the system	Obtenir pour le système la Spécification des Exigences du Système, la Spécification des Exigences de Sécurité du Système, la Description de l'Architecture du Système et le Plan de Sécurité du Système
Identify all the safety functions allocated to the software	Identifier toutes les fonctions de sécurité allouées au

Anglais	Français
	logiciel
Review all safety functions allocated to the software and determine the Software Safety Integrity Level	Examiner toutes les fonctions de sécurité allouées au logiciel et déterminer le niveau d'intégrité de la sécurité logicielle
Produce the Software Requirements Specification and the Software Architecture Specification	Produire la Spécification des Exigences du Logiciel et la Spécification de l'Architecture du Logiciel
Design, develop and verify/test the software according to the Software Quality Assurance Plan, Software Safety Integrity Level and the Software Lifecycle	Concevoir, développer et vérifier/soumettre à essai le logiciel conformément au Plan d'Assurance Qualité du Logiciel, au niveau d'intégrité de la sécurité logicielle et au cycle de vie du logiciel
Perform the Software Validation and hand over to system engineers	Effectuer la validation du logiciel et la transmettre aux ingénieurs système
Operational life of the system	Période de fonctionnement opérationnel du système
Software Maintenance	Maintenance du logiciel

Figure 1 – Démarche illustrative relative au logiciel

APPLICATIONS FERROVIAIRES – SYSTÈMES DE SIGNALISATION, DE TÉLÉCOMMUNICATION ET DE TRAITEMENT – LOGICIELS POUR SYSTÈMES DE COMMANDE ET DE PROTECTION FERROVIAIRE

1 Domaine d'application

1.1 La présente Norme internationale spécifie les exigences relatives aux processus et aux techniques applicables au développement de logiciel pour des systèmes électroniques programmables utilisés dans les applications ferroviaires de contrôle-commande et de protection. Elle est destinée à être utilisée dans tout domaine comportant des implications de sécurité. Ces systèmes peuvent être mis en œuvre à l'aide de microprocesseurs dédiés, de contrôleurs à logique programmable (automates programmables), de systèmes multiprocesseurs distribués, de grands systèmes dotés d'un calculateur central ou à l'aide d'autres architectures.

1.2 La présente Norme est exclusivement applicable au logiciel et à l'interaction entre le logiciel et le système auquel il appartient.

1.3 La présente Norme n'est pas pertinente pour les logiciels qui ont été identifiés comme n'ayant aucun impact sur la sécurité, c'est-à-dire pour les logiciels dont les défaillances ne peuvent pas affecter des fonctions de sécurité identifiées. Le concept de SIL 0 est introduit en raison de la présence d'une incertitude dans l'évaluation du risque, voire dans l'identification des dangers. Au moins les exigences associées au SIL 0 de la présente Norme sont satisfaites pour la partie logicielle des fonctions qui ont un impact sur la sécurité en dessous de SIL 1.

1.4 La présente Norme s'applique à tous les logiciels de sécurité utilisés dans des systèmes ferroviaires de contrôle-commande et de protection, y compris:

– la programmation d'applications,
– les systèmes d'exploitation,
– les outils,
– les microprogrammes.

La programmation d'applications inclut la programmation de haut niveau, la programmation de bas niveau et la programmation spécifique personnalisée (par exemple: la logique à contacts d'un contrôleur logique programmable).

1.5 La présente Norme traite également de l'utilisation de logiciels et d'outils préexistants. Ces logiciels peuvent être utilisés si les exigences spécifiques en 7.3.4.7 et 6.5.4.16 relatives aux logiciels préexistants et aux outils en 6.7 sont satisfaites.

1.6 Un logiciel développé selon une version quelconque de la présente Norme sera considéré comme étant conforme et non soumis aux exigences relatives aux logiciels préexistants.

1.7 La présente Norme considère que la conception moderne d'applications utilise fréquemment des logiciels génériques qui sont adaptés à servir de base pour diverses applications. Ces logiciels génériques sont ensuite configurés par des données et/ou des algorithmes, afin de produire le logiciel exécutable pour l'application. Les Articles généraux 1 à 6 et 9 de la présente Norme s'appliquent aux logiciels génériques ainsi qu'aux données d'application et algorithmes d'application. L'Article spécifique 7 s'applique uniquement pour

les logiciels génériques alors que l'Article 8 fournit les exigences spécifiques pour les données d'application et algorithmes d'application.

1.8 La présente Norme ne vise pas à traiter des problèmes commerciaux. Il convient de traiter ceux-ci comme une partie essentielle de tout accord contractuel. Tous les articles de la présente Norme nécessitent une étude soignée dans toute situation commerciale.

1.9 La présente Norme n'est pas destinée à être rétroactive. Elle s'applique donc principalement aux nouveaux développements et n'est applicable intégralement aux systèmes existants que s'ils font l'objet de modifications importantes. Pour les modifications mineures, seul 9.2 s'applique. Le chargé d'évaluation analyse les preuves fournies dans la documentation du logiciel pour confirmer si, oui ou non, la détermination de la nature et de l'étendue des modifications du logiciel est adéquate. Cependant, il est hautement recommandé d'appliquer la présente Norme pendant les mises à niveau et la maintenance des logiciels existants.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 62278:2002, *Applications ferroviaires – Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)*

ISO/IEC 90003:2014, *Ingénierie du logiciel – Lignes directrices pour l'application de l'ISO 9001:2008 aux logiciels informatiques*

ISO/IEC 25010 (série), *Ingénierie des systèmes et du logiciel – Exigences de qualité et évaluation des systèmes et du logiciel (SQuaRE) – Modèles de qualité du système et du logiciel*

ISO 9000, *Systèmes de management de la qualité – Principes essentiels et vocabulaire*

ISO 9001:2008, *Systèmes de management de la qualité – Exigences*