NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
62278

Première édition
First edition
2002-09

Applications ferroviaires –
Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)

Railway applications –
Specification and demonstration of reliability, availability, maintainability and safety (RAMS)

Numéro de référence
Reference number
CEI/IEC 62278:2002

Numérotation des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000. Ainsi, la CEI 34-1 devient la CEI 60034-1.

Editions consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

Informations supplémentaires sur les publications de la CEI

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique. Des renseignements relatifs à cette publication, y compris sa validité, sont disponibles dans le Catalogue des publications de la CEI (voir ci-dessous) en plus des nouvelles éditions, amendements et corrigenda. Des informations sur les sujets à l'étude et l'avancement des travaux entrepris par le comité d'études qui a élaboré cette publication, ainsi que la liste des publications parues, sont également disponibles par l'intermédiaire de:

- **Site web de la CEI (www.iec.ch)**
- **Catalogue des publications de la CEI**

  Le catalogue en ligne sur le site web de la CEI (http://www.iec.ch/searchpub/cur_fut.htm) vous permet de faire des recherches en utilisant de nombreux critères, comprenant des recherches textuelles, par comité d'études ou date de publication. Des informations en ligne sont également disponibles sur les nouvelles publications, les publications remplacées ou retirées, ainsi que sur les corrigenda.
- **IEC Just Published**

  Ce résumé des dernières publications parues (http://www.iec.ch/online_news/justpub/jp_entry.htm) est aussi disponible par courrier électronique. Veuillez prendre contact avec le Service client (voir ci-dessous) pour plus d'informations.
- **Service clients**

  Si vous avez des questions au sujet de cette publication ou avez besoin de renseignements supplémentaires, prenez contact avec le Service clients:

  Email: custserv@iec.ch
  Tél: +41 22 919 02 11
  Fax: +41 22 919 03 00

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site (www.iec.ch)**
- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (http://www.iec.ch/searchpub/cur_fut.htm) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.
- **IEC Just Published**

  This summary of recently issued publications (http://www.iec.ch/online_news/justpub/jp_entry.htm) is also available by email. Please contact the Customer Service Centre (see below) for further information.
- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

  Email: custserv@iec.ch
  Tel: +41 22 919 02 11
  Fax: +41 22 919 03 00

.

NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
62278

Première édition
First edition
2002-09

Applications ferroviaires – Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)

Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE XC

Pour prix, voir catalogue en vigueur
For price, see current catalogue

SOMMAIRE

CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

APPLICATIONS FERROVIAIRES – SPÉCIFICATION ET DÉMONSTRATION DE LA FIABILITÉ, DE LA DISPONIBILITÉ, DE LA MAINTENABILITÉ ET DE LA SÉCURITÉ (FDMS)

AVANT-PROPOS

1) La CEI (Commission Électrotechnique Internationale) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI 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, la CEI, entre autres activités, publie des Normes internationales. 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 la CEI, participent également aux travaux. La CEI 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 la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux intéressés sont représentés dans chaque comité d'études.
3) Les documents produits se présentent sous la forme de recommandations internationales. Ils sont publiés comme normes, spécifications techniques, rapports techniques ou guides et agréés comme tels par les Comités nationaux.
4) Dans le but d'encourager l'unification internationale, les Comités nationaux de la CEI s'engagent à appliquer de façon transparente, dans toute la mesure possible, les Normes internationales de la CEI dans leurs normes nationales et régionales. Toute divergence entre la norme de la CEI et la norme nationale ou régionale correspondante doit être indiquée en termes clairs dans cette dernière.
5) La CEI n'a fixé aucune procédure concernant le marquage comme indication d'approbation et sa responsabilité n'est pas engagée quand un matériel est déclaré conforme à l'une de ses normes.
6) L'attention est attirée sur le fait que certains des éléments de cette norme internationale peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 62278 a été établie par le comité d'études 9 de la CEI: Matériel électrique ferroviaire.

La présente norme, basée sur la norme européenne EN 50126 (1999), a été préparée par le Comité Technique 9X du CENELEC: Applications électriques et électroniques dans le domaine ferroviaire. Elle a été soumise aux Comités Nationaux pour vote suivant la procédure par voie express, par les documents suivants:

FDIS	Rapport de vote
9/686/FDIS	9/703/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 norme ne suit pas les règles de structure des normes internationales comme le spécifie la Partie 2 des Directives ISO/CEI.

NOTE Cette norme a été reproduite sans modifications importantes de son contenu original ou de ses règles structurelles.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant 2008. A cette date, la publication sera

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

RAILWAY APPLICATIONS – SPECIFICATION AND DEMONSTRATION OF RELIABILITY, AVAILABILITY, MAINTAINABILITY AND SAFETY (RAMS)

FOREWORD

1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.
3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62278 has been prepared by IEC technical committee 9: Electric railway equipment.

This standard based on the European Norm EN 50126 was prepared by Technical Committee CENELEC TC 9X : Electrical and electronic applications for railways. It was submitted to the National Committees for voting under the Fast Track Procedure as the following documents:

FDIS	Report on voting
9/686/FDIS	9/703/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 standard does not follow the rules for structuring International Standards as given in Part 2 of the ISO/IEC Directives.

NOTE This standard has been reproduced without significant modification to its original content or drafting.

The committee has decided that the contents of this publication will remain unchanged until 2008. At this date, the publication will be

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

INTRODUCTION

La présente Norme internationale fournit aux sociétés d'exploitation ferroviaire et aux industries ferroviaires un processus permettant de mettre en oeuvre une démarche cohérente de gestion de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité désignée par l'acronyme FDMS. Les processus de spécification et de démonstration des exigences de FDMS sont les clés de voûte de cette norme dont le but est de promouvoir une compréhension et une approche communes pour la gestion de la FDMS.

Cette norme peut être systématiquement appliquée par les sociétés d'exploitation et les industries ferroviaires tout au long des phases du cycle de vie d'une application ferroviaire afin de développer des exigences de FDMS spécifiques au domaine ferroviaire et de satisfaire à ces exigences. L'approche système définie par cette norme facilite l'évaluation des interactions relatives à la FDMS entre les éléments d'un système ferroviaire complexe.

Cette norme promeut la synergie entre les sociétés d'exploitation et les industries ferroviaires, quelles que soient la nature et l'étendue de leurs relations contractuelles, afin de parvenir au meilleur compromis entre les performances de FDMS et les coûts.

Le processus défini par cette norme suppose que les sociétés d'exploitation et les industries ferroviaires aient développé des politiques Qualité, Performance et Sécurité. L'approche définie dans cette norme est en accord avec les prescriptions de gestion de la qualité des normes internationales de la famille ISO 9000.

INTRODUCTION

This International Standard provides Railway Authorities and railway support industry with a process which will enable the implementation of a consistent approach to the management of reliability, availability, maintainability and safety, denoted by the acronym RAMS. Processes for the specification and demonstration of RAMS requirements are the cornerstones of this standard. This standard aims to promote a common understanding and approach to the management of RAMS.

This standard can be applied systematically by a Railway Authority and railway support industry, throughout all phases of the life cycle of a railway application, to develop railway specific RAMS requirements and to achieve compliance with these requirements. The systems-level approach defined by this standard facilitates assessment of the RAMS interactions between elements of complex railway applications.

This standard promotes co-operation between a Railway Authority and railway support industry, within a variety of procurement strategies, in the achievement of an optimal combination of RAMS and cost for railway applications.

The process defined by this standard assumes that Railway Authorities and railway support industry have business-level policies addressing Quality, Performance and Safety. The approach defined in this standard is consistent with the application of quality management requirements contained within the ISO 9000 family of International Standards.

APPLICATIONS FERROVIAIRES – SPÉCIFICATION ET DÉMONSTRATION DE LA FIABILITÉ, DE LA DISPONIBILITÉ, DE LA MAINTENABILITÉ ET DE LA SÉCURITÉ (FDMS)

1 Domaine d'application

1.1 La présente Norme internationale

– définit la FDMS en termes de fiabilité, de disponibilité, de maintenabilité et de sécurité et leurs interactions;

– définit un mode de management de la FDMS fondé sur le cycle de vie du système;

– permet de contrôler et de maîtriser les conflits entre les composantes de la FDMS;

– définit un processus systématique pour spécifier les exigences de FDMS et pour démontrer que ces exigences sont satisfaites;

– met en évidence les spécificités du domaine ferroviaire;

– ne définit pas d'objectifs quantifiés de FDMS, ni d'exigences pour une application ferroviaire spécifique;

– ne prescrit pas d'exigences destinées à maîtriser la vulnérabilité du système;

– ne définit pas les règles ou les processus de certification des produits ferroviaires vis-à-vis des prescriptions de cette norme;

– ne définit pas un processus d'approbation par les autorités responsables de la réglementation de sécurité.

1.2 La présente Norme internationale est applicable

– à la spécification et à la démonstration des exigences de FDMS pour toute application ferroviaire et à tout niveau d'une telle application, d'une ligne complète aux grands systèmes de cette ligne jusqu'aux sous-systèmes et aux équipements y compris ceux qui comportent des logiciels. Elle est notamment applicable

  - aux nouveaux systèmes,
  - aux nouveaux systèmes intégrés dans un système existant en service avant la parution de cette norme, bien qu'elle ne soit pas applicable a priori aux autres parties de ce système existant,
  - aux modifications de systèmes existants en service avant la parution de cette norme, bien qu'elle ne soit pas applicable a priori aux autres aspects de ces systèmes existants;

– à toutes les phases concernées du cycle de vie d'une application donnée;

– par les sociétés d'exploitation et les industries ferroviaires.

NOTE Cette norme fournit des informations complémentaires sur ses modalités d'application.

RAILWAY APPLICATIONS – SPECIFICATION AND DEMONSTRATION OF RELIABILITY, AVAILABILITY, MAINTAINABILITY AND SAFETY (RAMS)

1 Scope

1.1 This International Standard

- defines RAMS in terms of reliability, availability, maintainability and safety and their interaction;
- defines a process, based on the system life cycle and tasks within it, for managing RAMS;
- enables conflicts between RAMS elements to be controlled and managed effectively;
- defines a systematic process for specifying requirements for RAMS and demonstrating that these requirements are achieved;
- addresses railway specifics;
- does not define RAMS targets, quantities, requirements or solutions for specific railway applications;
- does not specify requirements for ensuring system security;
- does not define rules or processes pertaining to the certification of railway products against the requirements of this standard;
- does not define an approval process by the safety regulatory authority.

1.2 This International Standard is applicable

- to the specification and demonstration of RAMS for all railway applications and at all levels of such an application, as appropriate, from complete railway routes to major systems within a railway route, and to individual and combined sub-systems and components within these major systems, including those containing software; in particular
  - to new systems,
  - to new systems integrated into existing systems in operation prior to the creation of this standard, although it is not generally applicable to other aspects of the existing system,
  - to modifications of existing systems in operation prior to the creation of this standard; although it is not generally applicable to other aspects of the existing system;
- at all relevant phases of the life cycle of an application;
- for use by Railway Authorities and railway support industry.

NOTE Guidance on the applicability is given in the requirements of this standard.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. 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).

CEI 60050(191):1990, *Vocabulaire Electrotechnique International (VEI) – Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité*

CEI 62279, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Logiciels pour systèmes de commande et de protection ferroviaire* [1]

ISO 9001:2000, *Systèmes de management de la qualité – Exigences*

ENV 50129:1998, *Applications ferroviaires – Systèmes électroniques de sécurité pour la signalisation*

3 Définitions

Pour les besoins de la présente norme, les définitions suivantes s'appliquent.

3.1
allocation d'objectifs spécifiques
processus par lequel les objectifs de FDMS d'un système sont subdivisés entre les différents éléments de ce système pour fournir des objectifs individuels spécifiques

3.2
évaluation
réalisation d'une expertise afin de parvenir à un jugement, fondé sur des preuves, quant à l'adéquation d'un produit

3.3
audit
examen méthodique et indépendant destiné à déterminer si les procédures spécifiques aux exigences d'un produit sont conformes aux dispositions préétablies et si ces dispositions sont efficacement mises en oeuvre et aptes à atteindre les objectifs spécifiés

3.4
disponibilité
aptitude d'un produit à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens nécessaires est assurée

3.5
mise en état de fonctionnement
terme qui regroupe toutes les activités mises en oeuvre pour mettre au point un système ou un produit avant de démontrer qu'il satisfait aux exigences prescrites

---

[1] A publier.

2 Normative references

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

IEC 60050(191):1990, *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 62279, *Railway applications – Communications, signalling and processing systems – Software for railway control and protection systems*[1]

ISO 9001:2000, *Quality Management Systems – Requirements*

ENV 50129:1998, *Railway applications – Safety related electronic systems for signalling*

3 Definitions

For the purposes of this standard, the following definitions apply.

3.1
apportionment
process whereby the RAMS elements for a system are sub-divided between the various items which comprise the system to provide individual targets

3.2
assessment
undertaking of an investigation in order to arrive at a judgement, based on evidence, of the suitability of a product

3.3
audit
systematic and independent examination to determine whether the procedures specific to the requirements of a product comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives

3.4
availability
ability of a product to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval assuming that the required external resources are provided

3.5
commissioning
collective term for the activities undertaken to prepare a system or product prior to demonstrating that it meets its specified requirements

[1] To be published.

3.6
défaillance de mode commun
défaillance résultant d'un ou de plusieurs événements qui entraînent la défaillance simultanée de deux ou plusieurs composants, donnant lieu à une incapacité du système défini à accomplir sa fonction requise

3.7
conformité
démonstration assurant qu'un caractère ou une propriété d'un produit satisfait aux prescriptions fixées

3.8
gestion de configuration
discipline qui applique une orientation et une surveillance techniques et administratives pour identifier et documenter les caractéristiques fonctionnelles et physiques d'un élément de configuration, pour maîtriser les modifications apportées à ces caractéristiques, pour enregistrer et rendre compte du traitement et de l'état de mise en œuvre des modifications et pour vérifier la conformité aux prescriptions spécifiées

3.9
maintenance corrective
maintenance effectuée à la suite d'une détection de panne et destinée à remettre un produit dans un état lui permettant d'accomplir une fonction requise

3.10
défaillance consécutive à des événements dépendants
défaillance résultant d'un ensemble d'événements dont la probabilité ne peut pas être exprimée comme le simple produit des probabilités propres de chaque événement élémentaire

3.11
temps d'indisponibilité
intervalle de temps pendant lequel un produit est en état d'indisponibilité

[CEI 60050(191), modifié]

3.12
cause de défaillance
ensemble des circonstances associées à la conception, la fabrication ou l'emploi qui ont entraîné une défaillance

[CEI 60050(191)]

3.13
mode de défaillance
conséquences prévues ou observées d'une cause de défaillance sur une entité donnée, relatives aux conditions d'exploitation à l'instant de la défaillance

3.14
taux de défaillance
limite, si elle existe, du quotient de la probabilité conditionnelle pour que l'instant T d'une défaillance d'un produit soit compris dans un intervalle de temps donné (t, t + Δt) par la durée Δt de l'intervalle de temps lorsque Δt tend vers zéro, en supposant que l'entité soit disponible au début de l'intervalle de temps

NOTE Pour les applications où la distance parcourue ou le nombre de cycles d'exploitation est mieux adaptée que le temps, l'unité de temps peut être remplacée par l'unité de distance ou le nombre de cycles, suivant le cas.

3.6
common cause failure
failure which is the result of an event(s) which causes a coincidence of failure states of two or more components leading to a system failing to perform its required function

3.7
compliance
demonstration that a characteristic or property of a product satisfies the stated requirements.

3.8
configuration management
discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control change to those characteristics, record and report change processing and implementation status and verify compliance with specified requirements

3.9
corrective maintenance
maintenance carried out after fault recognition and intended to put a product into a state in which it can perform a required function

3.10
dependent failure
failure of a set of events, the probability of which cannot be expressed as the simple product of the unconditional probabilities of the individual events

3.11
down time
time interval during which a product is in a down state

[IEC 60050(191), modified]

3.12
failure cause
circumstances during design, manufacture or use which have led to a failure

[IEC 60050(191)]

3.13
failure mode
predicted or observed results of a failure cause on a stated item in relation to the operating conditions at the time of the failure

3.14
failure rate
limit, if this exists, of the ratio of the conditional probability that the instant of time, T, of a failure of a product falls within a given time interval (t, t+Δt) and the length of this interval, Δt, when Δt tends towards zero, given that the item is in an up state at the start of the time interval

NOTE For applications where distance travelled or number of cycles of operation is more relevant than time then the unit of time may be replaced by the unit of distance or cycles, as appropriate.

3.15
mode de panne
un des états possibles d'un produit en panne pour une fonction requise donnée

[CEI 60050(191), modifié]

3.16
analyse par arbre des causes
analyse qui détermine quels modes de panne du produit, des sous-produits, quels événements extérieurs ou quelles combinaisons de ces modes et de ces événements peuvent conduire à un mode de panne donné du produit, et dont le résultat est présenté sous forme d'un arbre

3.17
situation dangereuse
état potentiellement générateur de blessure humaine et/ou d'atteinte à l'environnement

3.18
registre des situations dangereuses
document dans lequel toutes les activités de management de la sécurité, les situations dangereuses identifiées, les décisions prises et les solutions adoptées sont enregistrées et référencées (également dénommé «Journal de Sécurité»)

[ENV 50129]

3.19
soutien logistique
ensemble des moyens qui sont prévus et organisés dans le but d'exploiter et de maintenir le système aux niveaux spécifiés de disponibilité et de coût global

3.20
maintenabilité
pour une entité donnée, utilisée dans des conditions données d'utilisation, probabilité pour qu'une opération donnée de maintenance active puisse être effectuée pendant un intervalle de temps donné, lorsque la maintenance est assurée dans des conditions données et avec l'utilisation de procédures et de moyens prescrits

[CEI 60050(191)]

3.21
maintenance
ensemble des actions techniques et organisationnelles, y compris les opérations de surveillance, destinées à maintenir ou à remettre un produit dans un état lui permettant d'accomplir une fonction requise

[CEI 60050(191), modifié]

3.22
politique de maintenance
description des relations entre les échelons de maintenance, les niveaux d'intervention et les niveaux de maintenance qui interviennent dans la maintenance d'une entité

[CEI 60050(191)]

3.23
mission
fonction principale du système

3.15
fault mode
one of the possible states of a faulty item, for a given required function

[IEC 60050(191)]

3.16
fault tree analysis
analysis to determine which fault modes of the product, sub-products or external events, or combinations thereof, may result in a stated fault mode of the product, presented in the form of a fault tree

3.17
hazard
physical situation with a potential for human injury and/or damage to environment

3.18
hazard log
document in which all safety management activities, hazards identified, decisions made and solutions adopted are recorded or referenced. Also known as a ”Safety Log”

[ENV 50129]

3.19
logistic support
overall resources which are arranged and organised in order to operate and maintain the system at the specified availability level at the required life cycle cost

3.20
maintainability
probability that a given active maintenance action, for an item under given conditions of use can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources

[IEC 60050(191)]

3.21
maintenance
the combination of all technical and administrative actions, including supervision actions, intended to retain an item in, or restore it to, a state in which it can perform a required function

[IEC 60050(191)]

3.22
maintenance policy
description of the inter-relationship between the maintenance echelons, the indenture levels and the levels of maintenance to be applied for the maintenance of an item

[IEC 60050(191)]

3.23
mission
objective description of the fundamental task performed by a system

3.24
profil de mission
description théorique de la mission et de ses variations en fonction de paramètres tels que le temps, le chargement, la vitesse, la distance, les arrêts, les tunnels, etc., au cours des phases opérationnelles du cycle de vie

3.25
maintenance préventive
maintenance effectuée à intervalles prédéterminés ou selon des critères prescrits et destinée à réduire la probabilité de défaillance ou la dégradation du fonctionnement d'une entité

[CEI 60050(191)]

3.26
société d'exploitation ferroviaire
organisme financièrement responsable devant une autorité légale de l'exploitation d'un système ferroviaire

NOTE La responsabilité financière de la société d'exploitation ferroviaire relative à l'ensemble du système ou à ses différentes parties ainsi qu'aux activités liées au cycle de vie est quelquefois partagée avec un ou plusieurs organismes. Par exemple:

– le(s) propriétaire(s) d'une ou de plusieurs parties du système et le(s) concessionnaire(s);
– l'exploitant du système;
– le(s) responsable(s) de la maintenance du système;
– etc.

Cette répartition est fondée sur des textes statutaires ou des accords contractuels. Il convient par conséquent de définir clairement cette responsabilité dès les premières étapes du cycle de vie d'un système

3.27
industrie ferroviaire
expression générique qui désigne le(s) fournisseur(s) de systèmes ferroviaires complets, de sous-systèmes ou d'éléments

3.28
programme FDM
ensemble d'activités, de moyens et d'éléments, s'appuyant sur des documents et planifiés selon un calendrier, destinés à mettre en place l'organisation, les responsabilités, les procédures, les activités, les capacités et les moyens qui concourent à assurer qu'une entité satisfera aux exigences de FDM relatives à un contrat ou à un projet particulier

3.29
FDMS
acronyme signifiant «Fiabilité, Disponibilité, Maintenabilité et Sécurité», également appelé «Sûreté de Fonctionnement».

3.30
fiabilité
probabilité pour qu'une entité puisse accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné (t_1, t_2)

[CEI 60050(191)]

3.31
croissance de la fiabilité
amélioration progressive d'une caractéristique de fiabilité d'une entité au cours du temps

[CEI 60050(191)]

3.24
mission profile
outline of the expected range and variation in the mission with respect to parameters such as time, loading, speed, distance, stops, tunnels, etc. in the operational phases of the life cycle

3.25
preventive maintenance
maintenance carried out at predetermined intervals or according to prescribed criteria and intended to reduce the probability of failure or the degradation of the functioning of an item

[IEC 60050(191)]

3.26
Railway Authority
body with the overall accountability to a Regulator for operating a railway system

NOTE Railway Authority accountabilities for the overall system or its parts and life cycle activities are sometimes split between one or more bodies or entities. For example:

– the owner(s) of one or more parts of the system assets and their purchasing agents;
– the operator of the system;
– the maintainer(s) of one or more parts of the system;
– etc.

Such splits are based on either statutory instruments or contractual agreements. Such responsibilities should therefore be clearly stated at the earliest stages of a system life cycle

3.27
railway support industry
generic term denoting supplier(s) of complete railway systems, their sub-systems or component parts

3.28
reliability and maintainability programme
documented set of time scheduled activities, resources and events serving to implement the organisation structure, responsibilities, procedures, activities, capabilities and resources that together ensure that an item will satisfy given reliability performance and maintainability performance requirements relevant to a given contract or project

3.29
RAMS
acronym meaning a combination of Reliability, Availability, Maintainability and Safety

3.30
reliability
probability that an item can perform a required function under given conditions for a given time interval (t_1, t_2)

[IEC 60050(191)]

3.31
reliability growth
condition characterised by a progressive improvement of a reliability performance measure of an item with time

[IEC 60050(191)]

3.32
réparation
ensemble des opérations manuelles de maintenance corrective effectuées sur une entité

[CEI 60050(191)]

3.33
rétablissement
récupération de l'aptitude d'une entité à accomplir une fonction requise après une panne

[CEI 60050(191)]

3.34
risque
combinaison de la probabilité d'occurrence d'une situation dangereuse et de sa gravité

3.35
sécurité
absence de risque inacceptable

3.36
dossier de sécurité
document dans lequel est consigné l'ensemble des démonstrations prouvant que le produit satisfait aux exigences de sécurité spécifiées

3.37
intégrité de sécurité
degré de confiance accordé à un système pour accomplir de manière satisfaisante des fonctions de sécurité dans toutes les conditions fixées pendant une période donnée

3.38
niveau d'intégrité de sécurité (SIL)
un des niveaux discrets définis pour spécifier les exigences d'intégrité de sécurité des fonctions de sécurité allouées aux systèmes de sécurité. Le niveau d'intégrité de sécurité ayant la valeur la plus élevée est celui qui possède le plus haut niveau d'intégrité de sécurité

3.39
plan de sécurité; plan d'assurance sécurité
ensemble d'activités, de moyens et d'éléments, s'appuyant sur des documents spécifiques et planifiés selon un calendrier, destinées à mettre en œuvre l'organisation, les responsabilités, les procédures, les activités, les capacités et les moyens qui concourent à assurer qu'une entité satisfera aux exigences de sécurité relatives à un contrat ou à un projet particulier

3.40
autorité de tutelle en matière de sécurité
organisme, souvent étatique, chargé de fixer ou d'approuver les exigences en matière de sécurité pour un système ferroviaire et de s'assurer que celui-ci satisfait à ces exigences

3.41
cycle de vie du système
activités réalisées au cours d'une période de temps donnée qui commence lors de la conception du système et qui se termine lors de sa réforme, de sa mise hors service et de son démantèlement

3.42
défaillance systémique
défaillance due à des erreurs survenant lors des activités réalisées au cours des différentes phases du cycle de vie, et qui entraîne une panne lors de la combinaison de certains éléments particuliers d'entrée ou sous certaines conditions particulières d'environnement

3.32
repair
that part of a corrective maintenance in which manual actions are performed on the item

[IEC 60050(191)]

3.33
restoration
that event when the item regains the ability to perform a required function after a fault

[IEC 60050(191)]

3.34
risk
probable rate of occurrence of a hazard causing harm and the degree of severity of the harm

3.35
safety
freedom from unacceptable risk of harm

3.36
safety case
documented demonstration that the product complies with the specified safety requirements

3.37
safety integrity
likelihood of a system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time

3.38
safety integrity level (SIL)
one of a number of defined discrete levels for specifying the safety integrity requirements of the safety functions to be allocated to the safety related systems. Safety Integrity Level with the highest figure has the highest level of safety integrity

3.39
Safety Plan
documented set of time scheduled activities, resources and events serving to implement the organisational structure, responsibilities, procedures, activities, capabilities and resources that together ensure that an item will satisfy given safety requirements relevant to a given contract or project

3.40
safety regulatory authority
often a national government body responsible for setting or agreeing the safety requirements for a railway and ensuring that the railway complies with the requirements

3.41
system life cycle
activities occurring during a period of time that starts when a system is conceived and end when the system is no longer available for use, is decommissioned and is disposed of

3.42
systematic failures
failures due to errors in any safety life cycle activity, within any phase, which cause it to fail under some particular combination of inputs or under some particular environmental condition

3.43
risque admissible
pour un produit, niveau maximal de risque acceptable par la société d'exploitation ferroviaire

3.44
validation
confirmation par examen et apport de preuves tangibles que les exigences particulières pour un usage spécifique prévu ont été satisfaites

3.45
vérification
confirmation par examen et apport de preuves tangibles que les exigences spécifiées ont été satisfaites

NOTE Pour clarifier les différences de sens entre vérification et validation, se reporter à la figure 11 et en 5.2.9.

4 La FDMS dans le domaine ferroviaire

4.1 Introduction

4.1.1 Cet article donne des informations de base sur les composantes et les techniques de FDMS. L'objet de cet article est de fournir au lecteur des informations de référence suffisantes pour permettre l'application efficace de cette norme au système ferroviaire.

4.1.2 La FDMS dans le domaine ferroviaire contribue pour une grande part à la qualité de service d'une société d'exploitation ferroviaire. Elle est définie par plusieurs facteurs; en conséquence, cet article est structuré de la manière suivante:

a) le paragraphe 4.2 traite du rapport entre la FDMS dans le domaine ferroviaire et la qualité de service;

b) les paragraphes 4.3 à 4.8 traitent de certains aspects de la FDMS dans le domaine ferroviaire, notamment:

   – les composantes de la FDMS;
   – les facteurs d'influence de la FMDS et les moyens d'obtention de la FDMS;
   – le risque et l'intégrité de sécurité.

4.1.3 Lorsque cela est possible, on utilise les termes définis au niveau international, mais lorsque de nouveaux termes sont nécessaires ou lorsque des termes reconnus ont une signification spécifique dans le contexte ferroviaire, ils sont définis à l'article 3 de cette norme.

4.1.4 Dans le cadre de cette norme, la décomposition «système, sous-système, composant» est utilisée pour subdiviser toute application en parties constitutives. Le domaine précis couvert par chaque terme (système, sous-système et composant) dépend de chaque application.

4.1.5 Un système peut être défini comme un ensemble organisé de sous-systèmes et de composants, interconnectés de manière organisée, pour assurer une fonction spécifiée. La fonction est dévolue aux sous-systèmes et composants au sein d'un système donné dont le comportement et l'état sont modifiés si la fonction du sous-système ou du composant est modifiée. Un système utilise des éléments d'entrée pour créer des éléments de sortie spécifiés, dans un environnement donné avec lequel il est en interaction.

4.2 FDMS dans le domaine ferroviaire et qualité de service

4.2.1 Ce paragraphe décrit les liens existant entre FDMS et qualité de service pour une tâche donnée.

3.43
tolerable risk
maximum level of risk of a product that is acceptable to the Railway Authority

3.44
validation
confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use have been fulfilled

3.45
verification
confirmation by examination and provision of objective evidence that the specified requirements have been fulfilled.

NOTE For clarification between verification and validation, see figure 11 and 5.2.9.

4 Railway RAMS

4.1 Introduction

4.1.1 This clause provides baseline information on the subject of RAMS and RAMS engineering. The purpose of this clause is to provide the reader with sufficient background information to enable the effective application of this standard to railway systems.

4.1.2 Railway RAMS is a major contributor to the Quality of Service provided by a Railway Authority. Railway RAMS is defined by several contributory elements; consequently, this clause is structured as follows:

a) subclause 4.2 examines the relationship between railway RAMS and quality of service;.

b) subclauses 4.3 to 4.8 examine aspects of railway RAMS, namely:
   - the elements of RAMS;
   - the factors which influence RAMS and means to achieve RAMS;
   - risk and safety integrity.

4.1.3 Where possible within this clause, internationally defined terms are used, but where new terms are required or where recognised terms have been made specific in the railway context, these are defined in clause 3 of this standard.

4.1.4 Within this standard, the sequence ”system, sub-system, component” is used to demonstrate the breakdown of any complete application into its constituent parts. The precise boundary of each term (system, sub-system and component) will depend upon the specific application.

4.1.5 A system can be defined as an assembly of sub-systems and components, connected together in an organised way, to achieve specified functionality. Functionality is assigned to sub-systems and components within a system and the behaviour and state of the system is changed if the sub-system or component functionality changes. A system responds to inputs to produce specified outputs, whilst interacting with an environment.

4.2 Railway RAMS and quality of service

4.2.1 This subclause introduces the link between RAMS and quality of service for an undertaking.

4.2.2 La FDMS est une caractéristique de l'exploitation d'un système sur une longue durée et elle est assurée par des concepts d'ingénierie, des méthodes, des outils et des techniques reconnus appliqués tout au long du cycle de vie du système. La FDMS d'un système peut être caractérisée par l'aptitude, évaluée en termes qualitatif et quantitatif, du système, de ses sous-systèmes et de ses composants, à fonctionner conformément à des spécifications et à être à la fois disponibles et sûrs. La FDMS du système, dans le cadre de cette norme, est une combinaison de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité désignée par l'acronyme FDMS.

4.2.3 L'objectif d'un système ferroviaire est d'assurer un niveau défini de trafic dans un délai donné et en toute sécurité. La FDMS dans le domaine ferroviaire détermine le niveau de confiance avec lequel on obtient la garantie que le système atteint cet objectif. La FDMS dans le domaine ferroviaire a une influence évidente sur la qualité du service rendu au client. La qualité de service est tributaire d'autres éléments considérés en termes de fonctions et de performances, par exemple, la régularité du service, la fréquence et la tarification. Cette relation est représentée à la figure 1.

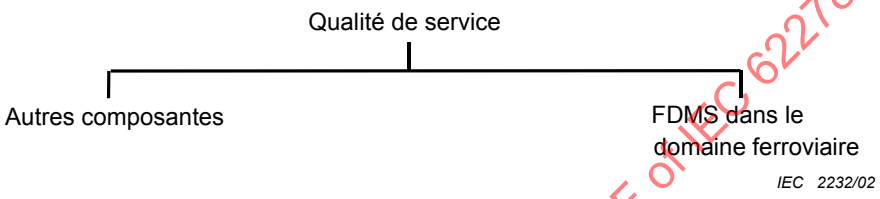


Figure 1 – Qualité de service et FDMS dans le domaine ferroviaire

4.3 Les composantes de la FDMS dans le domaine ferroviaire

4.3.1 Ce paragraphe présente l'interaction entre les composantes de la FDMS, fiabilité, disponibilité, maintenabilité et sécurité, dans le contexte des systèmes ferroviaires.

4.3.2 La sécurité et la disponibilité sont interdépendantes dans le sens où une insuffisance de l'une ou l'autre ou une mauvaise gestion des conflits entre leurs exigences peut s'opposer à l'obtention d'un système au fonctionnement sûr. L'interdépendance des composantes de la FDMS, fiabilité, disponibilité, maintenabilité et sécurité dans le domaine ferroviaire est illustrée à la figure 2.

4.3.3 Les objectifs de sécurité et de disponibilité d'un système en fonctionnement ne peuvent être atteints qu'en satisfaisant aux exigences de fiabilité et de maintenabilité et en contrôlant dans la durée, de manière permanente, les activités de maintenance et d'exploitation ainsi que l'environnement du système.

4.3.4 La vulnérabilité, en tant qu'élément qui caractérise la capacité de résistance d'un système au vandalisme et à des comportements irrationnels, peut être considérée comme une composante supplémentaire de la FDMS. Cependant, l'objet de cette norme n'est pas de traiter de la vulnérabilité.

4.2.2 RAMS is a characteristic of a system's long term operation and is achieved by the application of established engineering concepts, methods, tools and techniques throughout the life cycle of the system. The RAMS of a system can be characterised as a qualitative and quantitative indicator of the degree that the system, or the sub-systems and components comprising that system, can be relied upon to function as specified and to be both available and safe. System RAMS, in the context of this standard, is a combination of reliability, availability, maintainability and safety designated RAMS.

4.2.3 The goal of a railway system is to achieve a defined level of rail traffic in a given time, safely. Railway RAMS describes the confidence with which the system can guarantee the achievement of this goal. Railway RAMS has a clear influence on the quality with which the service is delivered to the customer. Quality of Service is influenced by other characteristics concerning functionality and performance, for example frequency of service, regularity of service and fare structure. This relationship is shown in figure 1.

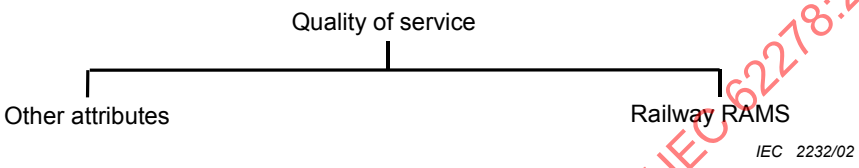


Figure 1 – Quality of Service and Railway RAMS

4.3 Elements of railway RAMS

4.3.1 This subclause introduces the interaction between RAMS elements, reliability, availability, maintainability and safety, in the context of railway systems.

4.3.2 Safety and availability are inter-linked in the sense that a weakness in either or mismanagement of conflicts between safety and availability requirements may prevent achievement of a dependable system. The inter-linking of railway RAMS elements, reliability, availability, maintainability and safety is shown in figure 2.

4.3.3 Attainment of in-service safety and availability targets can only be achieved by meeting all reliability and maintainability requirements and controlling the ongoing, long-term, maintenance and operational activities and the system environment.

4.3.4 Security, as an element that characterises the resilience of a railway system to vandalism and unreasonable human behaviour, can be considered as a further component of RAMS. However, consideration of security is outside the scope of this standard.

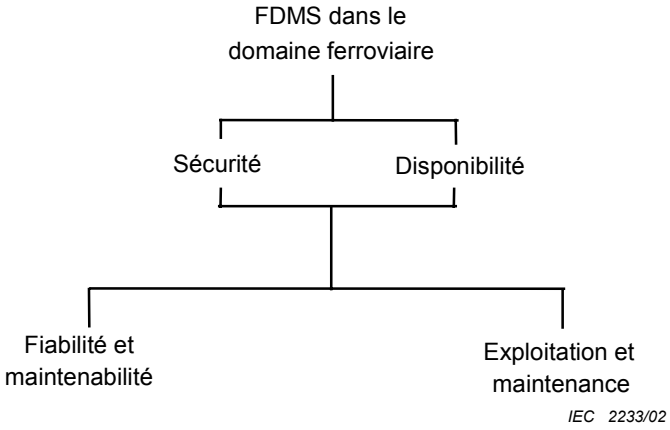


Figure 2 – Interdépendance des composantes de la FDMS dans le domaine ferroviaire

4.3.5 Les concepts techniques de disponibilité sont fondés sur la connaissance

a) des critères de fiabilité suivants:
   - l'ensemble des modes possibles de défaillance du système relatifs à l'application et à son environnement;
   - la probabilité d'occurrence de chaque défaillance ou, alternativement, le taux de défaillance;
   - l'effet de la défaillance sur la fonction du système;

b) des critères de maintenabilité suivants:
   - le temps nécessaire à l'exécution de la maintenance programmée;
   - le temps nécessaire à la détection, à l'identification et à la localisation des pannes;
   - le temps nécessaire à la remise en état du système en cas de panne (maintenance non programmée);

c) des critères d'exploitation et de maintenance suivants:
   - l'ensemble des modes d'exploitation possibles et la maintenance prescrite au cours du cycle de vie du système;
   - les facteurs humains.

4.3.6 Les concepts techniques de sécurité sont fondés sur la connaissance des éléments suivants:

a) l'ensemble des situations potentiellement dangereuses du système pour tous les modes d'exploitation et de maintenance ainsi que l'ensemble des conditions d'environnement;

b) les caractéristiques de chaque situation dangereuse en termes de gravité des conséquences;

c) les critères suivants de défaillances contraires à la sécurité:
   - tout mode de défaillance du système qui pourrait conduire à une situation dangereuse (mode de défaillance contraire à la sécurité). Il s'agit là d'un sous-ensemble des modes de défaillance relatifs à la fiabilité (4.3.5 a));
   - la probabilité d'occurrence de chaque mode de défaillance contraire à la sécurité;
   - la succession et/ou la coïncidence d'événements, de défaillances, de situations opérationnelles, de conditions d'environnement, etc., concernant l'application, qui peuvent conduire à un accident (c'est-à-dire une situation dangereuse susceptible de provoquer un accident);
   - la probabilité d'occurrence de chacun des événements, des défaillances, des situations opérationnelles, des conditions d'environnement, etc., concernant l'application;

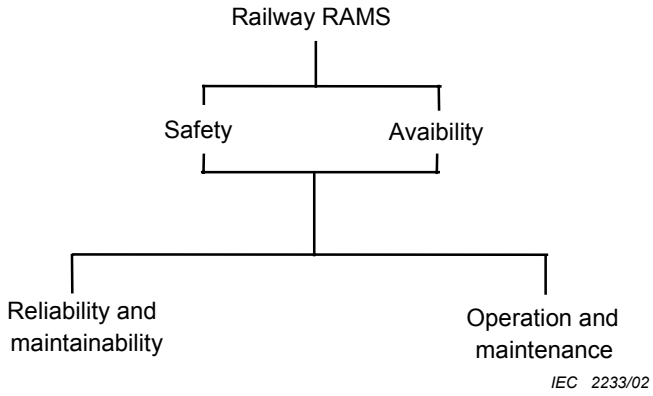


Figure 2 – Inter-relation of railway RAMS elements

4.3.5 Technical concepts of availability are based on a knowledge of

a) reliability in terms of
   - all possible system failure modes in the specified application and environment;
   - the probability of occurrence of each failure or alternatively, the rate of occurrence of each failure;
   - the effect of the failure on the functionality of the system;

b) maintainability in terms of
   - time for the performance of planned maintenance;
   - time for detection, identification and location of the faults;
   - time for the restoration of the failed system (unplanned maintenance);

c) operation and maintenance in terms of
   - all possible operation modes and required maintenance, over the system life cycle;
   - the human factor issues.

4.3.6 Technical concepts of safety are based on a knowledge of

a) all possible hazards in the system, under all operation, maintenance and environment modes;

b) the characteristic of each hazard in terms of its severity of consequences;

c) safety/safety related failures in terms of
   - all system failure modes that could lead to a hazard (safety related failure modes). This is a sub-set of all reliability failure modes (4.3.5 a));
   - the probability of occurrence of each safety related system failure mode;
   - sequence and/or coincidence of events, failures, operational states, environment conditions, etc. in the application, that may result in an accident. (i.e. a hazard resulting in an accident);
   - the probability of occurrence of each of the events, failures, operational states, environment conditions, etc. in the application;

d) les critères suivants de maintenabilité des éléments de sécurité du système:

- la facilité de mise en œuvre de la maintenance de certains aspects, éléments, ou constituants du système associés à une situation dangereuse ou à un mode de défaillance contraire à la sécurité;
- la probabilité d'erreur apparaissant pendant les opérations de maintenance de ces éléments de sécurité;
- le temps nécessaire à la remise en état du système dans un état de sûr;

e) les critères suivants d'exploitation et de maintenance des éléments de sécurité du système:

- l'influence du facteur humain sur l'efficacité de la maintenance de tous les éléments de sécurité ainsi que sur la sécurité de l'exploitation du système;
- les outils, les installations et les procédures pour assurer l'efficacité de la maintenance des éléments de sécurité et la sécurité de l'exploitation du système;
- les contrôles et les mesures efficaces permettant de traiter une situation dangereuse donnée et de pallier ses conséquences.

4.3.7 Les défaillances d'un système fonctionnant dans les limites d'une application donnée et de son environnement peuvent avoir des effets sur son comportement. Toutes les défaillances ont un effet préjudiciable sur la fiabilité du système tandis que seules certaines défaillances spécifiques peuvent affecter sa sécurité pour une application particulière. L'environnement peut également avoir une influence sur la fonction du système qui, à son tour, peut affecter la sécurité de l'application. Ces relations sont illustrées à la figure 3.

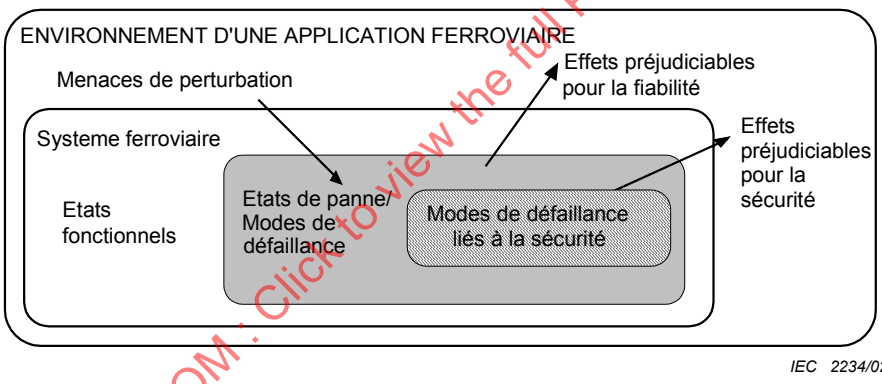


Figure 3 – Effets des défaillances au sein d'un système

4.3.8 La sûreté de fonctionnement d'un système ferroviaire ne peut être assurée que par la prise en compte des interactions entre les composantes de la FDMS du système ainsi que par la spécification et la réalisation de leur combinaison optimale.

4.4 Facteurs d'influence de la FDMS dans le domaine ferroviaire

4.4.1 Généralités

4.4.1.1 Ce paragraphe présente un processus d'identification des facteurs d'influence de la FDMS des systèmes ferroviaires en portant une attention toute particulière aux facteurs humains. Ces facteurs, ainsi que leurs effets, sont un élément d'entrée de la spécification des exigences de FDMS.

4.4.1.2 La FDMS d'un système ferroviaire dépend de trois éléments: des défaillances internes au système lors de chaque phase de son cycle de vie (conditions système), des défaillances survenant au cours de l'exploitation du système (conditions d'exploitation) et des défaillances survenant au cours des opérations de maintenance (conditions de maintenance). Il peut y avoir interaction entre ces éléments de défaillance. Cette relation est représentée à la figure 4 et décrite en détail à la figure 5.

d) maintainability of safety related parts of the system in terms of

- the ease of performing maintenance on those aspects or parts of the system or its components that are associated with a hazard or with a safety related failure mode;
- probability of errors occurring during maintenance actions on those safety related parts of the system;
- time for restoring the system to a safe state;

e) system operation and maintenance of safety related parts of the system in terms of

- human factor influence on the effective maintenance of all safety related parts of the system and safe operation of the system;
- tools, facilities and procedures for effective maintenance of the safety related parts of the system and for safe operation;
- effective controls and measures for dealing with a hazard and mitigating its consequences.

4.3.7 Failures in a system, operating within the bounds of an application and environment, will have some effect on the behaviour of the system. All failures adversely effect the system reliability whereas only some specific failures will have an adverse effect on safety within the particular application. Environment may also influence the functionality of the system and in turn the safety of the railway application. These links are shown in figure 3.

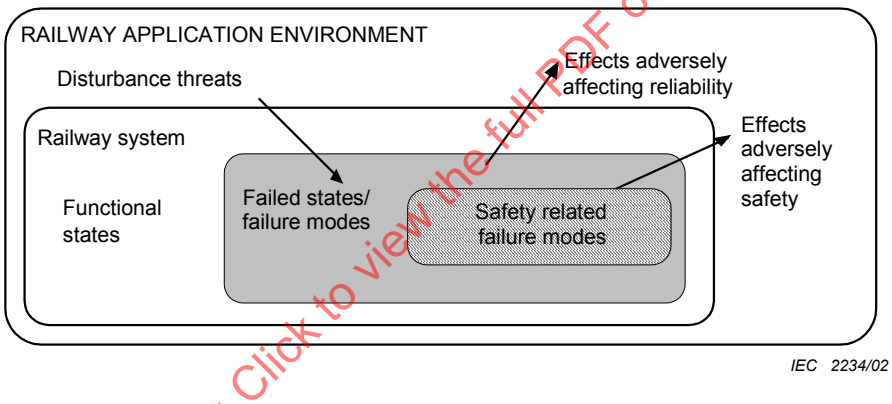


Figure 3 – Effects of failures within a system

4.3.8 A dependable railway system can only be realised through consideration of the interactions of RAMS elements within a system and the specification and achievement of the optimum RAMS combination for the system.

4.4 Factors influencing railway RAMS

4.4.1 General

4.4.1.1 This subclause introduces and defines a process to support the identification of factors which influence the RAMS of railway systems, with particular consideration given to the influence of human factors. These factors, and their effects, are an input to the specification of RAMS requirements for systems.

4.4.1.2 The RAMS of a railway system is influenced in three ways: by sources of failure introduced internally within the system at any phase of the system life cycle (system conditions), by sources of failure imposed on the system during operation (operating conditions) and by sources of failure imposed on the system during maintenance activities (maintenance conditions). These sources of failure can interact. This relationship is shown in figure 4 and detailed in figure 5.

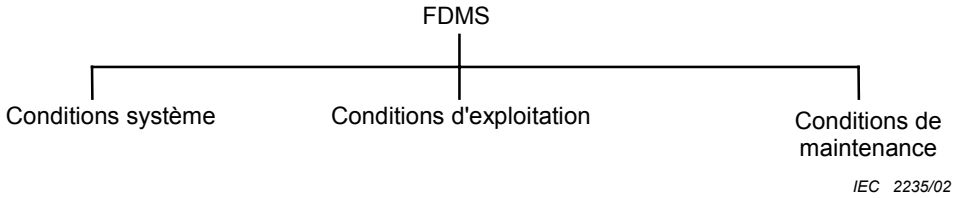


Figure 4 – Eléments d'influence de la FDMS

4.4.1.3 Pour réaliser des systèmes sûrs, il est nécessaire d'identifier les facteurs d'influence de la FDMS du système, d'en évaluer les effets ainsi que d'en maîtriser les causes tout au long du cycle de vie du système afin d'en optimiser les performances, et cela par l'application des contrôles appropriés.

4.4.2 Catégories de facteurs

4.4.2.1 Ce paragraphe décrit de manière détaillée un processus permettant de définir les facteurs susceptibles d'affecter la mise au point d'un système conforme à des exigences spécifiées de la FDMS.

4.4.2.2 A un haut niveau, les facteurs d'influence de la FDMS d'un système sont des facteurs génériques, ils concernent toutes les applications industrielles. La figure 5 présente certains de ces facteurs d'influence pour la FDMS des systèmes de transport. Elle présente également l'interaction existant entre ces facteurs. Pour identifier de manière détaillée les facteurs d'influence de la FDMS des systèmes ferroviaires, chaque facteur d'influence générique doit être considéré dans le cadre du système spécifique.

4.4.2.3 Une analyse des facteurs humains, du point de vue de leur effet sur la FDMS d'un système, fait intrinsèquement partie de «l'approche système» exigée par cette norme.

4.4.2.4 Les facteurs humains peuvent être définis, comme un ensemble de caractéristiques, d'aspirations et de comportements humains. Ces facteurs comportent des aspects anatomiques, physiologiques et psychologiques. La notion de facteurs humains est utilisée pour permettre aux hommes d'accomplir leurs tâches avec compétence et efficacité compte tenu des besoins qu'ils ressentent en termes de santé, de sécurité et de satisfaction professionnelle.

4.4.2.5 Les applications ferroviaires impliquent, en général, une grande variété de groupes humains, depuis les passagers, le personnel d'exploitation et de maintenance, et le personnel chargé de la réalisation des systèmes jusqu'aux personnes concernées par l'exploitation ferroviaire, telles que les automobilistes aux passages à niveau. Chacun est susceptible, face à une situation, de réagir de manière différente. Il est clair que le facteur humain a un impact potentiel important sur la FDMS d'un système ferroviaire. En conséquence, dans le domaine ferroviaire, l'atteinte des objectifs de FDMS nécessite, pour l'ensemble du cycle de vie du système, une maîtrise des facteurs humains plus rigoureuse que celle qui est exigée de nombreuses autres applications industrielles.

4.4.2.6 L'homme doit être considéré comme capable de contribuer de manière positive à la FDMS d'un système ferroviaire. Dans ce but, il est nécessaire, pour l'ensemble du cycle de vie, d'identifier et de contrôler la manière dont les facteurs humains peuvent influencer la FDMS. Il convient que cette analyse comprenne l'impact potentiel du facteur humain sur la FDMS lors des phases de conception et de développement du système.

4.4.2.7 Alors que la nécessité de prendre en compte les facteurs humains au cours du cycle de vie a un caractère générique, l'influence précise des facteurs humains sur la FDMS est spécifique à l'application considérée.

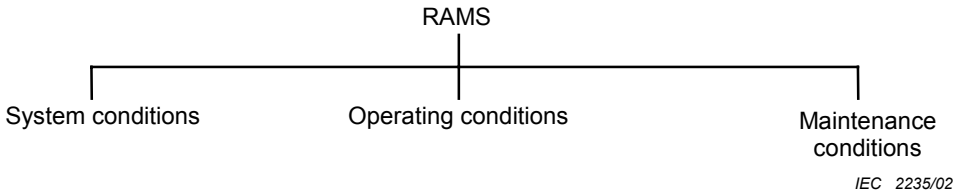


Figure 4 – Influences on RAMS

4.4.1.3 To realise dependable systems, factors which could influence the RAMS of the system need to be identified, their effect assessed and the cause of these effects managed throughout the life cycle of the system, by the application of appropriate controls, to optimise system performance.

4.4.2 Categories of factors

4.4.2.1 This subclause details a process for the definition of those factors which will affect the successful achievement of a system which complies with specified RAMS requirements.

4.4.2.2 At a high level, the factors which influence system RAMS are generic, applying across all industrial applications. Figure 5 includes some generic factors which influence transport system RAMS. This figure also shows the interaction between these factors. To identify detailed factors which influence the RAMS of railway systems, each generic influencing factor shall be considered in the context of the specific system.

4.4.2.3 An analysis of human factors, with respect to their effect on system RAMS, is inherent within the ”systems approach” required by this standard.

4.4.2.4 Human factors can be defined as the impact of human characteristics, expectations and behaviour upon a system. These factors include the anatomical, physiological and psychological aspects of humans. The concepts within human factors are used to enable people to carry out work efficiently and effectively, with due regard for human needs on issues such as health, safety and job satisfaction.

4.4.2.5 Railway applications typically involve a wide range of human groups, from passengers, operational staff and staff responsible for implementing systems to others affected by the railway operation, such as car drivers at level crossings. Each is capable of reacting to situations in different ways. Clearly, the potential impact of humans on the RAMS of a railway system is great. Consequently, the achievement of railway RAMS requires more rigorous control of human factors, throughout the entire system life cycle, than is required in many other industrial applications.

4.4.2.6 Humans shall be considered as possessing the ability to positively contribute to the RAMS of a railway system. To achieve this aim, the manner in which human factors can influence railway RAMS should be identified and managed throughout the entire life cycle. This analysis should include the potential impact of human factors on railway RAMS within the design and development phases of the system.

4.4.2.7 Whilst the need to address human factors within the life cycle is generic, the precise influence of human factors on RAMS is specific to the application under consideration.

4.4.2.8 Il convient que les facteurs génériques, y compris ceux qui sont mentionnés à la figure 5, soient examinés dans le contexte du système ferroviaire concerné. La société d'exploitation ferroviaire doit préciser dans son appel d'offres, les éventuels facteurs non retenus. Chaque facteur générique doit faire l'objet d'une évaluation et l'ensemble des facteurs d'influence spécifiques à l'application doivent être systématiquement déterminés à partir de cette évaluation. Les questions liées aux facteurs humains, éléments clés du processus de management intégré de la FDMS, doivent être examinées dans le cadre de cette évaluation.

4.4.2.9 Le processus de détermination de l'ensemble des facteurs d'influence doit être fondé sur l'utilisation de deux listes couvrant respectivement le champ des facteurs spécifiques au domaine ferroviaire (4.4.2.10) et celui des facteurs humains (4.4.2.11); il est également admis d'utiliser un autre type de présentation, voir la figure 5.

4.4.2.8 Generic factors, including those contained in figure 5, should be reviewed in the context of the railway system under consideration. The Railway Authority shall specify any non-applicable factors in their call for tenders. Each applicable generic factor shall be assessed and detailed influencing factors, specific to the application, systematically derived. Human factor issues, a core aspect within an integrated RAMS management process, shall be addressed within this assessment.

4.4.2.9 The process of deriving detailed influencing factors shall be supported by the use of the two checklists covering railway specific factors (4.4.2.10) and human factors (4.4.2.11), or as an alternative presentation, figure 5.

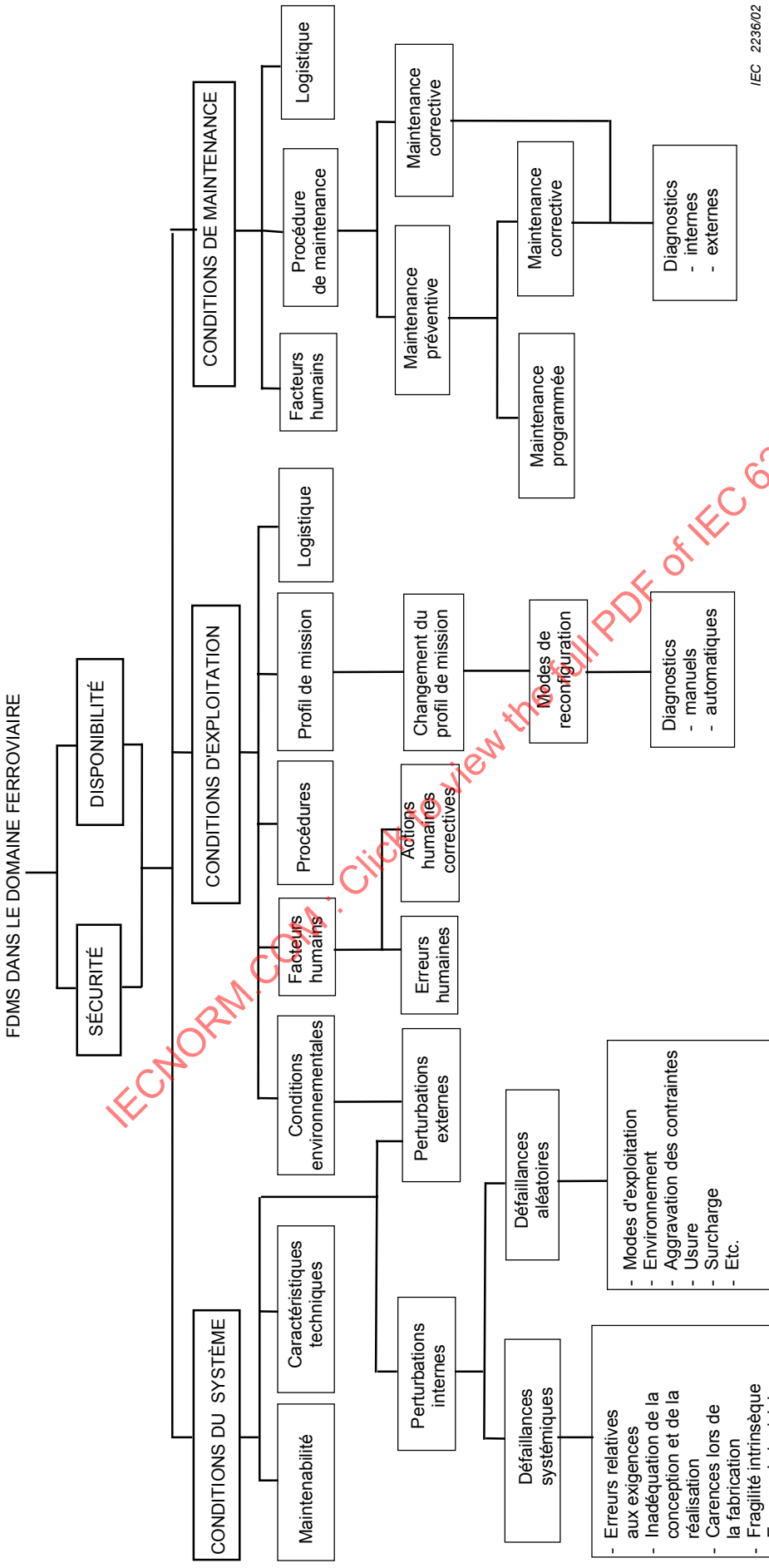


Figure 5 – Facteurs d'influence de la FDMS dans le domaine ferroviaire

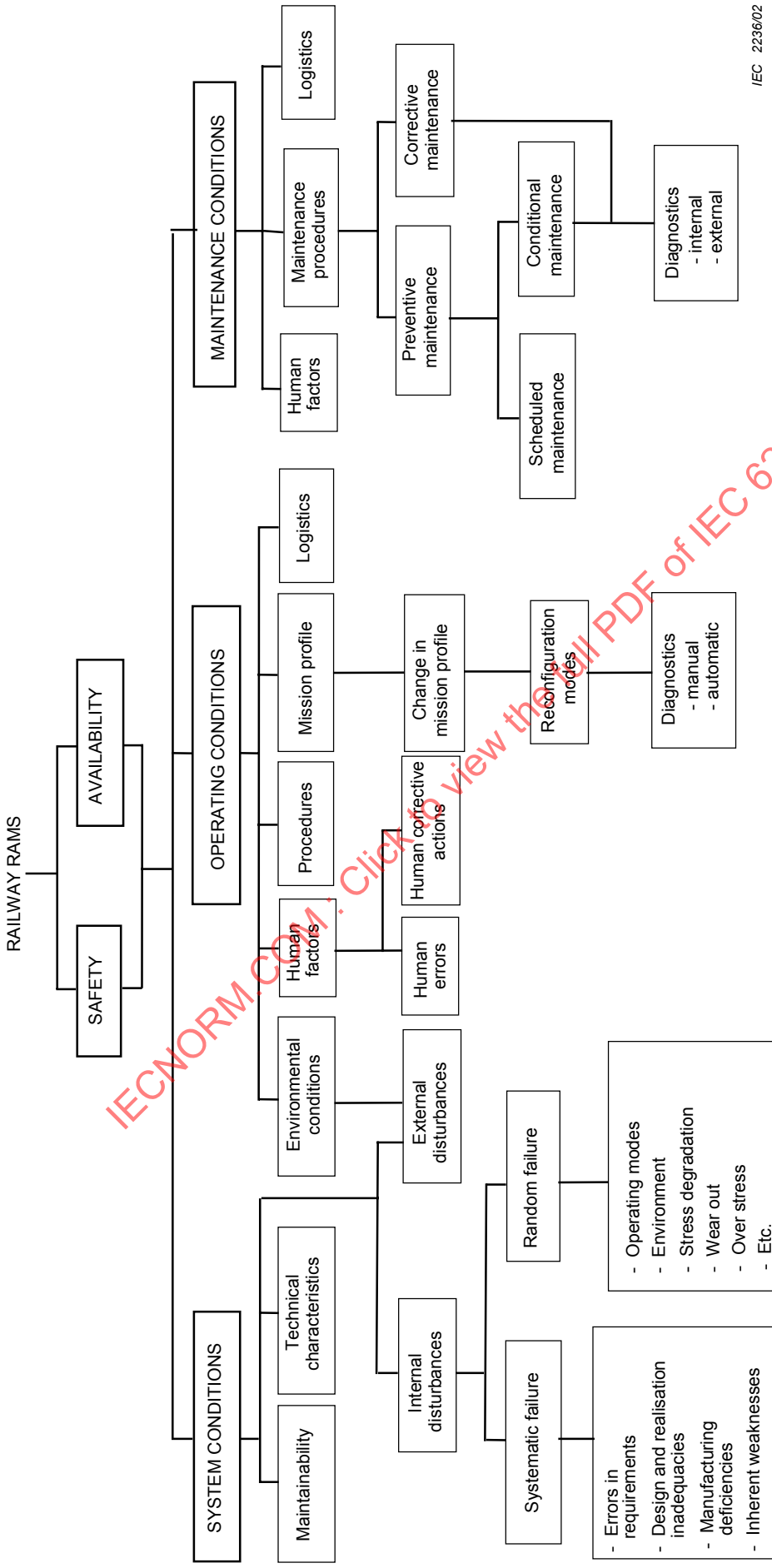


Figure 5 – Factors Influencing Railway RAMS

4.4.2.10 Il convient que la détermination de l'ensemble des facteurs d'influence spécifiques au domaine ferroviaire prenne notamment en compte chacun des facteurs suivants qui sont spécifiques à l'application ferroviaire. La liste suivante n'est aucunement limitative, elle a lieu d'être adaptée au domaine et à l'objet spécifique de l'application.

a) Exploitation du système:
   - les tâches que le système doit accomplir ainsi que les conditions dans lesquelles elles doivent l'être;
   - la coexistence de passagers, de marchandises, du personnel et de systèmes techniques dans un contexte opérationnel;
   - les exigences liées à la vie du système, y compris sa durée de vie prévue, la densité du service, ainsi que les exigences de coût global.

b) Environnement:
   - l'environnement physique;
   - le haut niveau d'intégration des systèmes ferroviaires dans l'environnement;
   - la possibilité limitée de soumettre des systèmes complets à des essais dans l'environnement ferroviaire.

c) Conditions d'application:
   - les contraintes imposées au nouveau système par les systèmes et l'infrastructure existants;
   - la nécessité de maintenir le service ferroviaire tout au long du cycle de vie.

d) Conditions d'exploitation:
   - les conditions d'installation au niveau de la voie;
   - les conditions de maintenance au niveau de la voie;
   - l'intégration des systèmes existants et des nouveaux systèmes lors de la mise en état de fonctionnement et de l'exploitation.

e) Catégories de défaillance:
   - les effets des défaillances dans un système ferroviaire perturbé.

4.4.2.11 Il convient que la détermination de l'ensemble des facteurs humains prenne notamment en compte chacun des facteurs humains suivants. La liste suivante n'est aucunement limitative, elle a lieu d'être adaptée au domaine et à l'objet spécifique de l'application.

a) Répartition des fonctions du système entre l'homme et la machine.

b) Effet sur les aspects humains du système:
   - de l'interface homme/système;
   - de l'environnement, y compris l'environnement physique et les exigences ergonomiques;
   - du régime de travail;
   - des compétences;
   - de la conception des tâches;
   - de l'interaction des tâches;
   - du processus humain de réaction;
   - de la structure de l'organisation ferroviaire;
   - de la culture ferroviaire;
   - du vocabulaire ferroviaire spécifique;
   - des problèmes résultant de l'introduction de nouvelles technologies.

4.4.2.10 The derivation of detailed railway specific influencing factors should include, but not be limited to, a consideration of each of the following railway specific factors. It should be noted that the following checklist is non-exhaustive and should be adapted to the scope and purpose of the application.

a) System operation:
   - the tasks which the system has to perform and the conditions in which the tasks have to be performed;
   - the co-existence of passengers, freight, staff and systems within the operating environment;
   - system life requirements, including system life expectancy, service intensity and life cycle cost requirements.

b) Environment:
   - the physical environment;
   - the high level of integration of railway systems within the environment;
   - the limited opportunity for testing complete systems in the railway environment.

c) Application conditions:
   - the constraints imposed by existing infrastructure and systems on the new system;
   - the need to maintain rail services during life cycle tasks.

d) Operating conditions:
   - trackside-based installation conditions;
   - trackside-based maintenance conditions;
   - the integration of existing systems and new systems during commissioning and operation.

e) Failure categories:
   - the effects of failure within a distributed railway system.

4.4.2.11 The derivation of detailed human influencing factors should include, but not be limited to, a consideration of each of the following human factors. It should be noted that the following checklist is non-exhaustive and should be adapted to the scope and purpose of the application.

a) Allocation of system functions between human and machine.

b) Effect on human performance within the system of
   - the human/system interface;
   - the environment, including the physical environment and ergonomic requirements;
   - human working patterns;
   - human competence;
   - the design of human tasks;
   - human interworking;
   - human feedback process;
   - railway organisational structure;
   - railway culture;
   - professional railway vocabulary;
   - problems arising from the introduction of new technology.

c) Exigences relatives au système et résultant
   - des compétences;
   - de la motivation et du dispositif mis en œuvre pour répondre aux aspirations de l'homme;
   - des dispositions visant à réduire les effets des variations du comportement de l'homme;
   - des dispositifs opérationnels de protection;
   - du cadre temporel et spatial de réaction de l'homme.

d) Exigences du système résultant de l'aptitude à l'homme à traiter des informations comprenant:
   - les communications homme/machine;
   - la densité des échanges d'informations;
   - le débit des échanges d'informations;
   - la qualité des informations;
   - la réaction humaine face aux situations anormales;
   - la formation des hommes;
   - les processus d'aide à la prise de décision;
   - d'autres facteurs de contraintes pesant sur l'homme.

e) Effets sur le système de l'interface homme/système, y compris:
   - la conception et l'exploitation de l'interface homme/système;
   - les effets de l'erreur humaine;
   - les effets de la violation délibérée des règles par l'homme;
   - l'implication et l'intervention de l'homme dans le système;
   - le dispositif de surveillance du système et la capacité de l'homme à dominer le système;
   - la perception humaine du risque;
   - l'implication de l'homme dans des domaines critiques du système;
   - la capacité humaine à anticiper les problèmes du système.

f) Facteurs humains relatifs à la conception et au développement du système, y compris:
   - la compétence humaine;
   - l'indépendance de l'homme pendant la conception;
   - l'implication de l'homme dans la vérification et la validation;
   - l'interface entre l'homme et les outils automatisés;
   - les processus de prévention des défaillances systémiques.

4.4.2.12 Il est recommandé de déterminer l'ensemble des facteurs par une approche schématique, telle que l'utilisation des diagrammes cause/effet. Un exemple de diagramme cause/effet très simplifié est représenté à la figure 6.

c) Requirements on the system arising from
   - human competence;
   - human motivation and aspiration support;
   - mitigating the effects of human behavioural changes;
   - operational safeguards;
   - human reaction time and space.

d) Requirements on the system arising from human information processing capabilities, including:
   - human/machine communications;
   - density of information transfer;
   - rate of information transfer;
   - the quality of information;
   - human reaction to abnormal situations;
   - human training;
   - supporting human decision making processes;
   - other factors contributing to human strain.

e) Effect on the system of human/system interface factors, including:
   - the design and operation of the human/system interface;
   - the effect of human error;
   - the effect of deliberate human rule violation;
   - human involvement and intervention in the system;
   - human system monitoring and override;
   - human perception of risk;
   - human involvement in critical areas of the system;
   - human ability to anticipate system problems.

f) Human factors in system design and development, including:
   - human competency;
   - human independence during design;
   - human involvement in verification and validation;
   - interface between human and automated tools;
   - systematic failure prevention processes.

4.4.2.12 A diagrammatic approach to the derivation of detailed factors, such as the use of cause/effect diagrams, is recommended. An example of a much simplified cause/effect diagram is shown in figure 6.

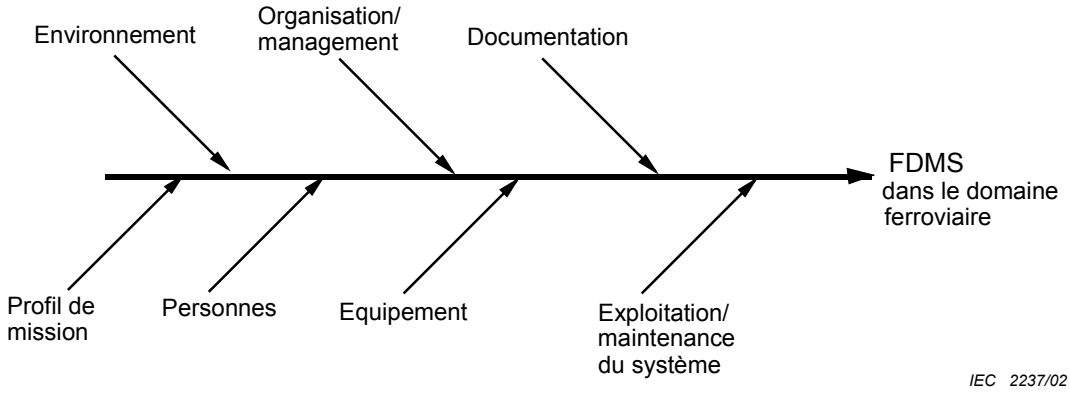


Figure 6 – Exemple de diagramme cause/effet

4.4.3 Evaluation des facteurs d'influence

L'effet potentiel de chaque facteur d'influence sur la FDMS du système ferroviaire considéré doit être évalué au niveau approprié de ce système. Cette évaluation doit tenir compte de l'effet de chaque facteur à chaque phase du cycle de vie et elle doit être réalisée au niveau approprié du système considéré. L'évaluation doit prendre en compte l'interaction des facteurs d'influence associés. Pour les facteurs humains, l'évaluation doit également tenir compte de l'effet de chacun des facteurs sur les autres.

4.5 Moyens de satisfaction des exigences de FDMS dans le domaine ferroviaire

4.5.1 Généralités

4.5.1.1 Les moyens mis en œuvre pour satisfaire aux exigences de FDMS dans le domaine ferroviaire sont liés à la maîtrise des facteurs d'influence de la FDMS pendant la durée de vie du système. L'efficacité de cette maîtrise exige la mise en œuvre de mécanismes et de procédures de défense contre les sources d'erreurs introduites pendant la réalisation et le maintien du système. Ces mécanismes et ces procédures nécessitent de prendre en compte les défaillances, qu'elles soient ou non systémiques.

4.5.1.2 Les moyens utilisés pour satisfaire aux exigences de FDMS sont fondés sur les précautions prises pour réduire au minimum une éventuelle défaillance résultant d'une erreur au cours des différentes phases du cycle de vie du système. Ces précautions sont une combinaison de

a) prévention, permettant de réduire la probabilité d'occurrence de la défaillance,

b) protection, permettant de réduire la gravité des conséquences de la défaillance.

4.5.1.3 La stratégie adoptée pour satisfaire aux exigences de FDMS du système, y compris l'utilisation de moyens de prévention et/ou de protection, doit être justifiée.

4.5.2 Spécification de la FDMS

4.5.2.1 La spécification des exigences de FDMS est un processus complexe. L'annexe A de cette norme donne un exemple général d'une spécification des exigences de FDMS fondée sur le processus décrit en détail dans cette norme. L'annexe B donne comme exemple l'aperçu d'une procédure de définition d'un programme de FDMS fondée sur les exigences de cette norme. Ces deux annexes informatives sont données à titre indicatif, elles utilisent à cet effet l'exemple d'un matériel roulant. L'annexe B comprend également une liste d'outils appropriés à une analyse de FDMS. Le choix de l'outil adéquat dépend du système pris en compte et de facteurs tels que la criticité du système, son caractère novateur, sa complexité, etc.

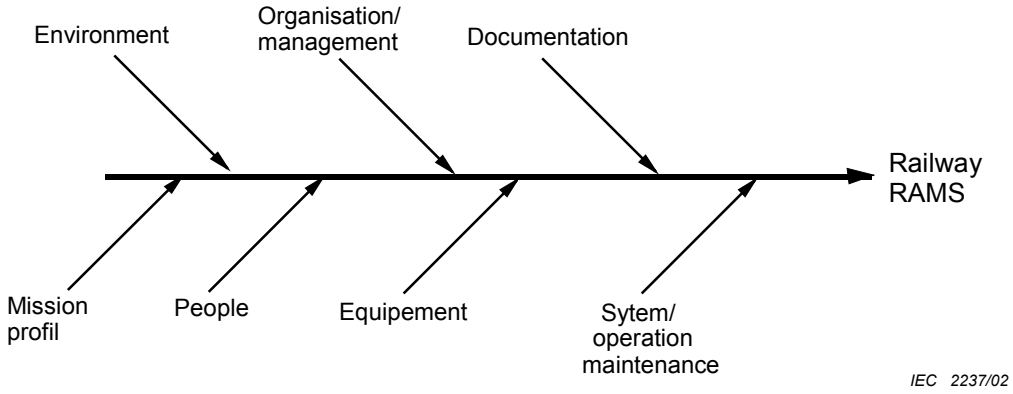


Figure 6 – Example of a cause/effect diagram

4.4.3 Evaluation of factors

The potential effect of each influencing factor on the RAMS of the railway system under consideration shall be evaluated at a level appropriate to the railway system under consideration. This evaluation shall include a consideration of the effect of each factor at each phase of the life cycle and shall be at a level which is appropriate to the system under consideration. The evaluation shall address the interaction of associated influencing factors. For human factors, the evaluation shall also consider the effect of each factor in relation to each other.

4.5 Means to achieve railway RAMS requirements

4.5.1 General

4.5.1.1 The means to achieve railway RAMS requirements relates to controlling the factors which influence RAMS throughout the life of the system. Effective control requires the establishment of mechanisms and procedures to defend against sources of error being introduced during the realisation and support of the system. Such defences need to take account of both random and systematic failures.

4.5.1.2 The means used to achieve RAMS requirements are based on the concept of taking precautions to minimise the possibility of an impairment occurring as a result of an error during the life cycle phases. Precaution is a combination of

a) prevention: concerned with lowering the probability of the impairment,

b) protection: concerned with lowering the severity of the consequences of the impairment.

4.5.1.3 The strategy to achieve RAMS requirements for the system, including the use of prevention and/or protection means, shall be justified.

4.5.2 RAMS specification

4.5.2.1 The specification of RAMS requirements is a complex process. Annex A of this standard provides an example outline of a RAMS requirements specification, based on the process detailed in this standard. Annex B of this standard provides an example outline procedure for the definition of a RAMS programme, based on the requirements of this standard. Both informative annexes are for guidance only and have been compiled using rolling stock as an example.A list of suitable tools for RAMS analysis is also included in annex B. Selection of an appropriate tool will depend on the system under consideration and on factors such as the criticality, novelty, complexity, etc. of the system.

4.5.2.2 Le tableau 1 définit les catégories des défaillances de FDM à utiliser pour les applications ferroviaires.

Tableau 1 – Catégories de défaillances de FDM

Catégorie de défaillance	Définition
Grave (Défaillance entraînant une interruption du service)	Une défaillance qui empêche la circulation du train ou entraîne un retard du service supérieur à une durée spécifiée et/ou un coût supérieur à un niveau spécifié
Importante (Défaillance entraînant des perturbations dans le service)	Une défaillance - qui doit être corrigée pour que le système remplisse sa fonction spécifiée, et - qui n'entraîne pas un retard ou un coût supérieur au seuil minimal spécifié pour une défaillance grave
Mineure	Une défaillance - qui n'empêche pas un système de remplir sa fonction spécifiée, et - qui ne remplit pas des critères applicables aux défaillances graves ou importantes

4.5.2.3 L'annexe C (informative) fournit des paramètres qui permettent de caractériser les exigences de fiabilité, de disponibilité, de maintenabilité, de soutien logistique et de sécurité pour les systèmes ferroviaires. Les paramètres spécifiques dépendent du système concerné. Il convient que tous les paramètres de FDMS utilisés fassent l'objet d'un accord entre la société d'exploitation ferroviaire et l'industrie ferroviaire. Lorsque les paramètres peuvent être exprimés en unités différentes, il est recommandé de fournir les facteurs de conversion applicables.

4.6 Risque

4.6.1 Concept de risque

Le concept de risque est la combinaison de deux éléments:

– la probabilité d'occurrence d'un événement ou d'une combinaison d'événements conduisant à une situation dangereuse, ou la fréquence de tels événements;

– les conséquences de cette situation dangereuse.

4.6.2 Analyse de risque

4.6.2.1 L'analyse de risque doit être effectuée à diverses phases du cycle de vie du système par l'autorité responsable de la phase considérée et être consignée par écrit. La documentation doit comprendre au minimum:

a) la méthodologie;

b) les hypothèses, les limites et la justification de la méthodologie utilisée;

c) les situations dangereuses identifiées;

d) les résultats de l'estimation du risque et leurs niveaux de confiance;

e) les résultats des études de compromis;

f) les données, leurs sources et leurs niveaux de confiance;

g) les références.

4.5.2.2 Table 1 defines RAM failure categories suitable for use in railway applications.

Table 1 – RAM failure categories

Failure category	Definition
Significant (Immobilising failure)	A failure that prevents train movement or causes a delay to service greater than a specified time and/or generates a cost greater than a specified level
Major (Service failure)	A failure that - must be rectified for the system to achieve its specified performance, and - does not cause a delay or cost greater than the minimum threshold specified for a significant failure
Minor	A failure that - does not prevent a system achieving its specified performance, and - does not meet criteria for significant or major failures

4.5.2.3 Suitable parameters to characterise reliability, availability, maintainability, logistic support and safety requirements of railway systems are shown in annex C (informative). Specific parameters will depend on the system under consideration. All RAMS parameters used should be agreed between the Railway Authority and the railway support industry. Where parameters may be expressed in alternative dimensions, conversion factors should be provided.

4.6 Risk

4.6.1 Risk concept

The concept of risk is the combination of two elements:

– the probability of occurrence of an event or combination of events leading to a hazard, or the frequency of such occurrences;

– the consequence of the hazard.

4.6.2 Risk analysis

4.6.2.1 Risk analysis shall be performed at various phases of the system life cycle by the authority responsible for that phase and shall be documented. The documentation shall contain, as a minimum:

a) analysis methodology;

b) assumptions, limitations and justification of the methodology;

c) hazard identification results;

d) risk estimation results and their confidence levels;

e) results of trade-off studies;

f) data, their sources and confidence levels;

g) references.

4.6.2.2 Le tableau 2 définit, en termes qualitatifs, les catégories types de probabilité d'occurrence ou de fréquence d'une situation dangereuse et une description de chaque catégorie pour un système ferroviaire donné. Pour une application donnée, les catégories, leur nombre, ainsi que l'échelle numérique, doivent être définis par la société d'exploitation ferroviaire.

Tableau 2 – Fréquence des situations dangereuses

Catégorie	Description
Fréquente	Susceptible de se produire fréquemment. La situation dangereuse est continuellement présente
Probable	Peut survenir à plusieurs reprises. On peut s'attendre à ce que la situation dangereuse survienne souvent
Occasionnelle	Susceptible de survenir à plusieurs reprises. On peut s'attendre à ce que la situation dangereuse survienne à plusieurs reprises
Rare	Susceptible de se produire à un moment donné du cycle de vie du système. On peut raisonnablement s'attendre à ce que la situation dangereuse se produise
Improbable	Peu susceptible de se produire mais possible. On peut supposer que la situation dangereuse peut exceptionnellement se produire
Invraisemblable	Extrêmement improbable. On peut supposer que la situation dangereuse ne se produira pas

4.6.2.3 Les conséquences des situations dangereuses doivent être analysées pour en estimer l'impact probable. Pour tout système ferroviaire, le tableau 3 décrit les niveaux types de gravité des situations dangereuses ainsi que les conséquences liées à chaque niveau de gravité. Pour une application donnée, la société d'exploitation ferroviaire doit définir le nombre de niveaux de gravité ainsi que les conséquences correspondant à chaque niveau de gravité.

Tableau 3 – Niveau de gravité des situations dangereuses

Niveau de gravité	Conséquence pour les personnes ou l'environnement	Conséquence pour le service
Catastrophique	Des morts et/ou plusieurs personnes gravement blessées et/ou des dommages majeurs pour l'environnement	
Critique	Un mort et/ou une personne grièvement blessée et/ou des dommages graves pour l'environnement	Perte d'un système important
Marginal	Blessures légères et/ou menace grave pour l'environnement	Dommages graves pour un (ou plusieurs) système(s)
Insignifiant	Eventuellement une personne légèrement blessée	Dommages mineurs pour un système

4.6.3 Evaluation et acceptation des risques

4.6.3.1 Ce paragraphe traite de la mise en place d'une matrice «occurrence – gravité» destinée à l'évaluation des résultats d'analyse de risque, à la catégorisation des risques, aux actions entreprises pour réduire les risques ou pour éliminer des risques intolérables ainsi qu'à l'acceptation des risques.

4.6.3.2 L'évaluation des risques doit être effectuée en combinant la fréquence d'un événement dangereux et la gravité de ses conséquences pour déterminer le niveau du risque résultant de l'événement dangereux. Le tableau 4 présente une matrice «occurrence – gravité».

4.6.2.2 Table 2 provides, in qualitative terms, typical categories of probability or frequency of occurrence of a hazardous event and a description of each category for a railway system. The categories, their numbers, and their numerical scaling to be applied shall be defined by the Railway Authority, appropriate to the application under consideration.

Table 2 – Frequency of occurrence of hazardous events

Category	Description
Frequent	Likely to occur frequently. The hazard will be continually experienced
Probable	Will occur several times. The hazard can be expected to occur often
Occasional	Likely to occur several times. The hazard can be expected to occur several times
Remote	Likely to occur sometime in the system life cycle. The hazard can reasonably expected to occur
Improbable	Unlikely to occur but possible. It can be assumed that the hazard may exceptionally occur
Incredible	Extremely unlikely to occur. It can be assumed that the hazard may not occur

4.6.2.3 Consequence analysis shall be used to estimate the likely impact. Table 3 describes typical hazard severity levels and the consequences associated with each severity level for all railway systems. The number of severity levels and the consequences for each severity level to be applied shall be defined by the Railway Authority, appropriate for the application under consideration.

Table 3 – Hazard severity level

Severity level	Consequence to persons or environment	Consequence to service
Catastrophic	Fatalities and/or multiple severe injuries and/or major damage to the environment	
Critical	Single fatality and/or severe injury and/or significant damage to the environment	Loss of a major system
Marginal	Minor injury and/or significant threat to the environment	Severe system(s) damage
Insignificant	Possible minor injury	Minor system damage

4.6.3 Risk evaluation and acceptance

4.6.3.1 This subclause deals with the formation of a "frequency - consequence" matrix for evaluation of the results of risk analysis, risk categorisation, actions for risk reduction or elimination of intolerable risks, and for risk acceptance.

4.6.3.2 Risk evaluation shall be performed by combining the frequency of occurrence of a hazardous event with the severity of its consequence to establish the level of risk generated by the hazardous event. A "frequency - consequence" matrix is shown in table 4.

Tableau 4 – Matrice «occurrence – gravité»

Fréquence d'un événement dangereux	Niveau de risque			
Fréquent				
Probable				
Occasionnel				
Rare				
Improbable				
Invraisemblable				
	Insignifiant	Marginal	Critique	Catastrophique
	Niveau de gravité des conséquences d'une situation dangereuse			

4.6.3.3 Il convient que l'acceptation du risque soit fondée sur un principe généralement admis. Un certain nombre de principes sont disponibles et peuvent être utilisés à cet égard. Voici quelques exemples (voir également l'annexe D pour plus d'informations sur ces principes):

– *As Low As Reasonably Practicable* (principe ALARP tel qu'il est pratiqué au Royaume-Uni);

– Globalement Au Moins Aussi Bon (principe GAMAB tel qu'il est pratiqué en France). La formulation complète de ce principe est la suivante:
«Tout nouveau système de transport guidé doit offrir un niveau de sécurité globalement au moins aussi bon que celui des systèmes de transport guidés existants équivalents»;

– Mortalité Endogène Minimale (principe MEM tel qu'il est pratiqué en Allemagne).

Le tableau 5 définit des catégories qualitatives de risque et les actions à mettre en œuvre pour chaque catégorie. La société d'exploitation ferroviaire doit définir les principes à adopter, le niveau d'acceptabilité d'un risque et les niveaux qui s'inscrivent dans les différentes catégories de risque.

Tableau 5 – Catégorie qualitative de risques

Catégorie de risque	Action à appliquer pour chaque catégorie
Inacceptable	Doit être éliminé
Indésirable	Acceptable uniquement lorsqu'il est impossible de réduire le risque et avec l'accord de la société d'exploitation ferroviaire ou, le cas échéant, de l'autorité de tutelle
Acceptable	Acceptable moyennant un contrôle approprié et l'accord de la société d'exploitation ferroviaire
Négligeable	Acceptable avec/sans l'accord de la société d'exploitation ferroviaire

4.6.3.4 Le tableau 6 donne un exemple d'évaluation du risque et des moyens de réduire et/ou de contrôler les risques pour les rendre acceptables.

Table 4 – Frequency - consequence matrix

Frequency of occurrence of a hazardous event	Risk levels			
Frequent				
Probable				
Occasional				
Remote				
Improbable				
Incredible				
	Insignificant	Marginal	Critical	Catastrophic
	Severity levels of hazard consequence			

4.6.3.3 Risk acceptance should be based on a generally accepted principle. A number of principles are available that may be utilised. Some examples are as follows (also see annex D for more information on these principles):

– As Low As Reasonably Practicable (ALARP principle as practised in UK);

– *Globalement Au Moins Aussi Bon* (GAMAB principle as practised in France). The complete formulation of this principle is
"*All new guided transport systems must offer a level of risk globally at least as good as the one offered by any equivalent existing system*";

– Minimum Endogenous Mortality (MEM principle as practised in Germany).

Table 5 defines qualitative categories of risk and the actions to be applied against each category. The Railway Authority shall be responsible for defining principle to be adopted and the tolerability level of a risk and the levels that fall into the different risk categories.

Table 5 – Qualitative risk categories

Risk category	Actions to be applied against each category
Intolerable	Shall be eliminated
Undesirable	Shall only be accepted when risk reduction is impracticable and with the agreement of the Railway Authority or the Safety Regulatory Authority, as appropriate
Tolerable	Acceptable with adequate control and with the agreement of the Railway Authority
Negligible	Acceptable with/without the agreement of the Railway Authority

4.6.3.4 Table 6 shows an example of risk evaluation and risk reduction/controls for risk acceptance.

Tableau 6 – Exemple d'évaluation et d'acceptation du risque

Fréquence d'un événement dangereux *	Niveau de risque			
Fréquent	Indésirable	Inacceptable	Inacceptable	Inacceptable
Probable	Acceptable	Indésirable	Inacceptable	Inacceptable
Occasionnel	Acceptable	Indésirable	Indésirable	Inacceptable
Rare	Négligeable	Acceptable	Indésirable	Indésirable
Improbable	Négligeable	Négligeable	Acceptable	Acceptable
Invraisemblable	Négligeable	Négligeable	Négligeable	Négligeable
	Insignifiant	Marginal	Critique	Catastrophique
	Niveaux de gravité des conséquences d'une situation dangereuse			
* L'échelle de fréquence des événements dangereux dépend de l'application concernée (4.6.2.2).				

Evaluation du risque	Réduction/contrôle du risque
Inacceptable	Doit être éliminé
Indésirable	Acceptable uniquement lorsque la réduction de risque est impossible et avec l'accord de la société d'exploitation ferroviaire
Acceptable	Acceptable moyennant un contrôle approprié et l'accord de la société d'exploitation ferroviaire
Négligeable	Acceptable sans condition

4.7 Intégrité de la sécurité

4.7.1 Lorsque pour une application le niveau de sécurité a été fixé, et que la réduction nécessaire du risque a été appréciée, compte tenu des résultats du processus d'évaluation du risque, il est possible de décliner les exigences d'intégrité de la sécurité pour le système et les composantes de l'application. L'intégrité de la sécurité peut être considérée comme une combinaison d'éléments quantifiables (généralement relatifs aux défaillances non systémiques affectant le matériel) et d'éléments non quantifiables (généralement relatifs à des défaillances systémiques affectant le logiciel, la spécification, les documents, les processus, etc.). Il convient que les dispositifs de réduction du risque internes et externes au système correspondent aux exigences de réduction du risque pour que l'objectif de niveau de sécurité du système soit atteint.

4.7.2 On admet que pour un système donné, on peut obtenir confiance dans l'obtention de l'intégrité de la sécurité d'une fonction par la mise en œuvre effective d'un ensemble composé d'une architecture, de méthodes, d'outils et de techniques spécifiques. L'intégrité de la sécurité est liée à la probabilité de ne pas réaliser la fonction de sécurité requise. Les fonctions qui requièrent des exigences d'intégrité d'un niveau plus élevé sont probablement d'un coût de réalisation plus élevé. Cette norme ne définit pas, pour les systèmes ferroviaires, la corrélation entre l'intégrité de la sécurité et les probabilités de défaillance, bien qu'il convienne de noter que la série de normes CEI 61508 établit une corrélation générique. Pour les applications ferroviaires, la définition de cette corrélation incombe à la société d'exploitation ferroviaire. Cependant, le processus de management défini dans cette norme est générique et, par conséquent, il peut être utilisé pour toute corrélation, après acceptation par une autorité ou conjointement par les sociétés européennes d'exploitation ferroviaire.

4.7.3 Il convient de mettre en oeuvre les fonctions de sécurité dans les systèmes en utilisant les architectures, les méthodes, les outils et les techniques définis dans d'autres normes particulières pertinentes. Ainsi, la CEI 62279 définit des méthodes, des outils et des techniques de développement de systèmes utilisant des logiciels et l'ENV 50129 définit un processus d'acceptation et d'homologation des systèmes électroniques de signalisation et de contrôle commande ferroviaires.

Table 6 – Typical example of risk evaluation and acceptance

Frequency of occurrence of a hazardous event *	Risk levels			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Remote	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Tolerable
Incredible	Negligible	Negligible	Negligible	Negligible
	Insignificant	Marginal	Critical	Catastrophic
	Severity levels of hazard consequence			

* Scaling for the frequency of occurrence of hazardous events will depend on the application under consideration (4.6.2.2).

Risk evaluation	Risk reduction/control
Unacceptable	Shall be eliminated
Undesirable	Shall only be accepted when risk reduction is impracticable and with the agreement of the Railway Authority.
Tolerable	Acceptable with adequate control and the agreement of the Railway Authority
Negligible	Acceptable without any agreement

4.7 Safety integrity

4.7.1 When the level of safety for the application has been set and the necessary risk reduction estimated, based on the results of the risk assessment process, the safety integrity requirements, for the systems and components of the application, can be derived. Safety integrity can be viewed as a combination of quantifiable elements (generally associated with hardware, i.e. random failures) and non-quantifiable elements (generally associated with systematic failures in software, specification, documents, processes, etc.). External risk reduction facilities and the system risk reduction facilities should match the necessary risk reduction required for the system to meet its target level of safety.

4.7.2 Confidence in the achievement of the safety integrity of a function within a system may be obtained through the effective application of a combination of specific architecture, methods, tools and techniques. Safety integrity correlates to the probability of failure to achieve required safety functionality. Functions with greater integrity requirements are likely to be more expensive to realise. This standard does not define the correlation between safety integrity and failure probabilities for railway systems, although it should be noted that a generic correlation is defined within the IEC 61508 series. The definition of this correlation for railway applications is the responsibility of the Railway Authority. However, the management process defined within this standard is generic and suitable for use with any correlation, as agreed by individual authorities or jointly by European Railway Authorities.

4.7.3 Safety functions within systems should be implemented using the architecture, methods, tools and techniques defined in other relevant detailed standards. For example, IEC 62279 defines methods, tools and techniques to develop software systems and ENV 50129 defines a process for the acceptance and approval of electronic railway signalling systems.

4.7.4 Les spécifications relatives à l'intégrité de la sécurité se rapportent, à la base, aux fonctions de sécurité. Il convient d'affecter ces fonctions de sécurité à des systèmes de sécurité et/ou à des dispositifs externes de réduction du risque. Ce processus d'affectation est itératif afin d'optimiser la conception et le coût du système global.

4.7.5 Le Plan de Sécurité et le Programme de FDM, lorsqu'ils sont effectivement mis en oeuvre, donnent confiance dans l'aptitude du système final à satisfaire aux exigences de FDMS.

4.7.6 Les points suivants relatifs à l'intégrité de la sécurité d'un produit doivent être notés:

a) les fonctions de sécurité exigées d'un système ainsi que l'intégrité de la sécurité correspondante subissent l'influence de l'environnement dans lequel le système est utilisé;

b) lorsque pour développer un produit, on utilise des méthodes, des outils et des techniques correspondant à une intégrité de sécurité spécifique, il est possible de déclarer que ce produit possède un niveau «X» d'intégrité de la sécurité. Cela signifie que le produit a une fonction spécifique, dans un environnement donné et à un niveau déterminé d'intégrité;

c) la figure 7 montre que l'utilisation de produits standards disponibles dans le commerce peut varier en fonction des différentes applications. Ainsi, le produit A est utilisé pour assurer des fonctions différentes dans des systèmes 1 et 2. En conséquence, il est admis que l'intégrité de la sécurité requise d'un produit varie selon les applications. Avant d'affecter un produit à un système donné, il convient donc d'évaluer les limites et les contraintes relatives à la fonction et à l'environnement effectif du produit afin de s'assurer qu'elles sont compatibles avec les exigences globales du système.

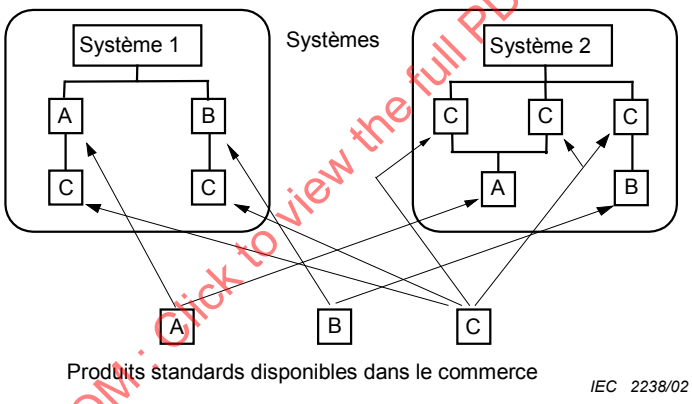


Figure 7 – Produits certifiés dans les systèmes de sécurité

4.7.7 Avant d'utiliser le concept de SIL, il convient de tenir compte des exigences suivantes.

a) Il convient que le niveau adéquat d'utilisation du SIL soit déterminé par des experts en sécurité. Il convient de ne pas utiliser plus de quatre niveaux de SIL.

b) Un niveau donné de SIL ne doit être alloué qu'à un «élément», à savoir à un équipement considéré isolément qui remplit une ou plusieurs fonctions simples et qui peut être remplacé par un autre équipement assurant la (les) même(s) fonction(s). En général, un tel «élément» correspond à l'équipement du plus bas niveau susceptible d'être remplacé lors d'une opération de maintenance corrective de premier niveau.

c) Dans la mesure où l'environnement dans lequel un produit est placé est d'une importance primordiale, la portée de la certification d'un produit standard disponible dans le commerce en termes de SIL, ainsi que la signification de cette certification eu égard aux exigences de sécurité, doivent être examinées pour décider de la conformité du système étudié à toutes les conditions qui lui sont applicables.

4.7.4 Safety integrity is basically specified for safety functions. Safety functions should be assigned to safety systems and/or to external risk reduction facilities. This assignment process is iterative, in order to optimise the design and cost of the overall system.

4.7.5 It is the Safety Plan and the RAM Programme which, when implemented effectively, give confidence in the ability of the final system to achieve compliance with RAMS requirements.

4.7.6 The following points concerning product safety integrity shall be noted:

a) safety functionality required of a system, and its corresponding safety integrity, is influenced by the environment in which the system is used;

b) when a product is developed using methods, tools and techniques appropriate to a specific safety integrity, claims may be made that the product is a safety integrity level "X" product. This claim means that the product will exhibit specific functionality, within a stated environment, at a certain integrity;

c) figure 7 shows that the use of commercial "off the shelf" products may differ within different applications. For example Product A is being used to implement different functions within Systems 1 and 2. Consequently, the safety integrity required of a product may differ between applications. Therefore, before applying a product within any system, the limitations and constraints applying to the functionality and the stated environment of the product should be assessed to ensure that they are consistent with the overall requirements of the system.

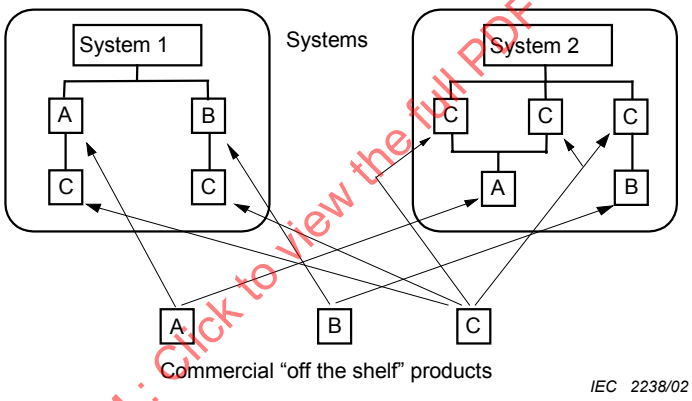


Figure 7 – Certified products in safety systems

4.7.7 Before applying the concept of SIL, the following requirements should be considered.

a) The adequate level of SIL applicability should be established by safety experts. It is recommended that no more than 4 levels should be used.

b) A SIL shall only be allocated to an "element", namely a stand-alone equipment which performs one or more simple functions and which can be replaced by another one performing the same function(s). Generally, such an "element" is often the lowest level equipment that can be replaced during a first level corrective maintenance operation.

c) Insofar as the environment in which a product will be inserted is of the utmost importance, the extent in terms of SIL to which an off-the-shelf product is certified and what certification means when compared to its safety requirements shall be examined to state whether all the conditions are met for the system under study.

d) Un SIL donné ne concerne qu'un niveau attendu de confiance dans la sécurité d'un produit. Conformément aux explications de 4.3 de cette norme, les exigences de sécurité et de disponibilité sont interdépendantes dans le domaine du transport ferroviaire. Le concept de SIL ne couvre pas tous les aspects d'un système et par conséquent, la prise en compte du seul SIL peut être insuffisante (par exemple: exploitation en modes dégradés ou états de repli comportant des exigences de sécurité différentes, etc.).

4.8 Concept de sécurité intrinsèque

4.8.1 Cette norme adopte vis-à-vis de la sécurité, une approche extensive de management du risque. Cette approche est cohérente avec le concept de sécurité intrinsèque bien établi dans l'ingénierie ferroviaire.

4.8.2 Le concept de sécurité intrinsèque a été utilisé dès les premiers temps du chemin de fer. Ce concept, qui repose sur un ensemble d'hypothèses, est fondé sur l'utilisation de composants dont les modes de défaillance sont bien établis, et sur le fait qu'il existe un état «sûr» en cas de défaillance de l'une de leurs parties constitutives. Tous ces composants sont agencés de telle sorte qu'un système, par construction, ne peut pas admettre un état plus permissif que celui qui existe en l'absence de défaillance.

4.8.3 La validité de ce concept est en général fondée sur l'expérience mais, lorsqu'il s'agit du développement et de l'exploitation de grands systèmes complexes utilisant des micro-processeurs disponibles dans le commerce, son application est limitée. La croissance exponentielle du nombre de combinaisons de défaillances à prendre en compte lorsqu'on utilise de tels composants rend en général peu pratique une approche déterministe. Pour ces systèmes complexes, l'approche probabiliste se révèle plus efficace.

4.8.4 La validité de l'approche par la sécurité intrinsèque est admise pour des parties d'un système et, comme d'autres approches déterministes, elle n'est pas exclue par cette norme. Pour toutes ces approches, il est nécessaire de démontrer que les exigences de FDMS spécifiées pour le système sont satisfaites.

5 Management de la FDMS dans le domaine ferroviaire

5.1 Généralités

5.1.1 Cet article définit un processus de management, fondé sur le cycle de vie du système, rendant possible la maîtrise des facteurs de FDMS spécifiques aux applications ferroviaires. Ce processus traite des points suivants:

– la définition des exigences de FDMS;
– l'évaluation et la maîtrise des éléments susceptibles d'affecter la FDMS;
– la programmation et la mise en œuvre des activités de FDMS;
– l'obtention de la satisfaction des exigences de FDMS;
– le contrôle continu de la satisfaction de ces exigences pendant tout le cycle de vie du système.

5.1.2 Bien que la FDMS ferroviaire constitue le thème central de cette norme elle n'est qu'un des nombreux aspects du système ferroviaire global. Cet article définit un processus systématique de maîtrise de la FDMS de telle sorte que ce processus constitue un des composants d'une approche intégrée de management couvrant tous les aspects du système ferroviaire global.

d) A SIL is only addressing an expected level of confidence in the safety for a product. As explained in 4.3 of this standard, safety requirements and availability requirements are inter-related in the context of railway transport. The SIL concept does not cover all aspects of a system and therefore considering SIL alone may not be sufficient (e.g. degraded operation modes or fall-back states with different safety requirements, etc.).

4.8 Fail-safe concept

4.8.1 This standard adopts a broad, risk-management approach to safety. This approach is consistent with the fail-safe concept, well-established with railway engineers.

4.8.2 From the early days of railways, the inherent fail-safe concept has been used. The concept, dependent upon a set of hypotheses, is based on the use of components with well-established failure modes and that a safe condition exists in case of failure of one of its parts. All those components are arranged so that a system, so constructed, cannot allow a more permissive condition than that existing in the absence of a failure.

4.8.3 The validity of the concept is, in general, based on experience but it has limited applicability to the development and use of large, complex systems employing commercial microprocessors. The exponential growth in the number of failure combinations to be considered when using such components means that a deterministic approach is, generally, not practicable. With such complex systems, the probabilistic approach can be used effectively.

4.8.4 The fail-safe approach may be valid for parts of a system and, like other deterministic approaches, it is not precluded by this standard. For all approaches, it is necessary to achieve compliance with the specified RAMS requirements for the system.

5 Management of railway RAMS

5.1 General

5.1.1 This clause defines a management process, based on the system life cycle, which will enable the control of RAMS factors specific to railway applications. The process supports the

– definition of RAMS requirements;
– assessment and control of threats to RAMS;
– planning and implementation of RAMS tasks;
– achievement of compliance with RAMS requirements;
– on-going monitoring, during the life cycle, of compliance.

5.1.2 Although railway RAMS is the focus of this standard, it is one of many aspects of a total railway system. This clause defines a systematic process for RAMS management so that the process is one component of an integrated management approach which addresses all aspects of the complete railway system.

5.1.3 Pour un système ferroviaire, en termes de sécurité, le risque acceptable de la part d'une société d'exploitation ferroviaire, dépend des critères de sécurité fixés par l'autorité de tutelle nationale, ou par la société d'exploitation ferroviaire elle-même en accord avec l'autorité de tutelle. La responsabilité première en matière d'évaluation, de contrôle et de réduction du risque incombe néanmoins à la société d'exploitation ferroviaire. Dans certains cas, la législation exige la démonstration, à l'aide de preuves formelles, du caractère adéquat de la sécurité du système.

5.2 Cycle de vie du système

5.2.1 Le cycle de vie du système est constitué d'une succession de phases, chacune comportant des tâches, et couvrant l'ensemble de la durée de vie du système, depuis le concept initial jusqu'au retrait du service et à la dépose définitive. Le cycle de vie fournit un cadre pour la programmation, le management, le contrôle et la surveillance du système sous tous ses aspects, y compris la FDMS, au fur et à mesure de son passage par les différentes phases de développement, afin de livrer le bon produit au bon prix et dans les délais convenus. Le concept de cycle de vie est primordial à la réussite de l'application de cette norme.

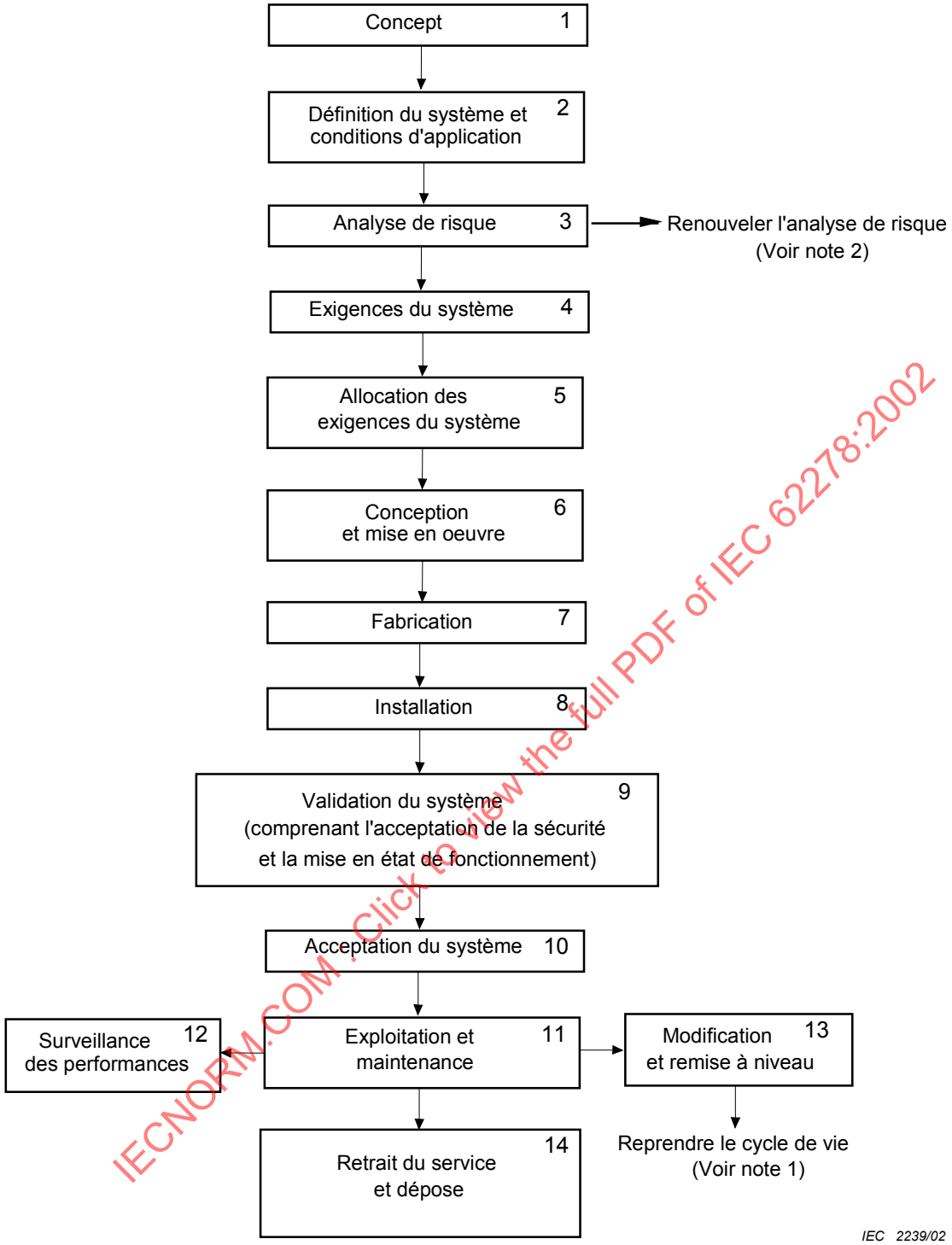
5.2.2 La figure 8 présente le cycle de vie d'un système, en l'occurrence celui d'une application ferroviaire. La figure 9 résume les principales tâches de chaque phase du cycle de vie. Les tâches de FDMS y sont présentées en tant qu'éléments de l'ensemble des tâches du projet. Ces dernières ne font pas partie du domaine d'application de cette norme mais elles sont représentatives de pratiques communément utilisées dans l'industrie. Les tâches de FDMS contribuent aux tâches générales du projet lors de chaque phase et le détail des exigences relatives aux tâches de FDMS est donné dans les articles suivants de cette norme.

5.1.3 The tolerable safety risk of a railway system for any Railway Authority is dependent upon the safety criteria set by the national Safety Regulatory Authority, or by the Railway Authority itself in agreement with the Safety Regulatory Authority. The primary responsibility for assessing, controlling and minimising risk rests with the Railway Authority. In some cases, legislation requires the formal presentation of evidence to demonstrate the adequacy of system safety.

5.2 System life cycle

5.2.1 The system life cycle is a sequence of phases, each containing tasks, covering the total life of a system from initial concept through to decommissioning and disposal. The life cycle provides a structure for planning, managing, controlling and monitoring all aspects of a system, including RAMS, as the system progresses through the phases, in order to deliver the right product at the right price within the agreed time scales. The life cycle concept is fundamental to the successful implementation of this standard.

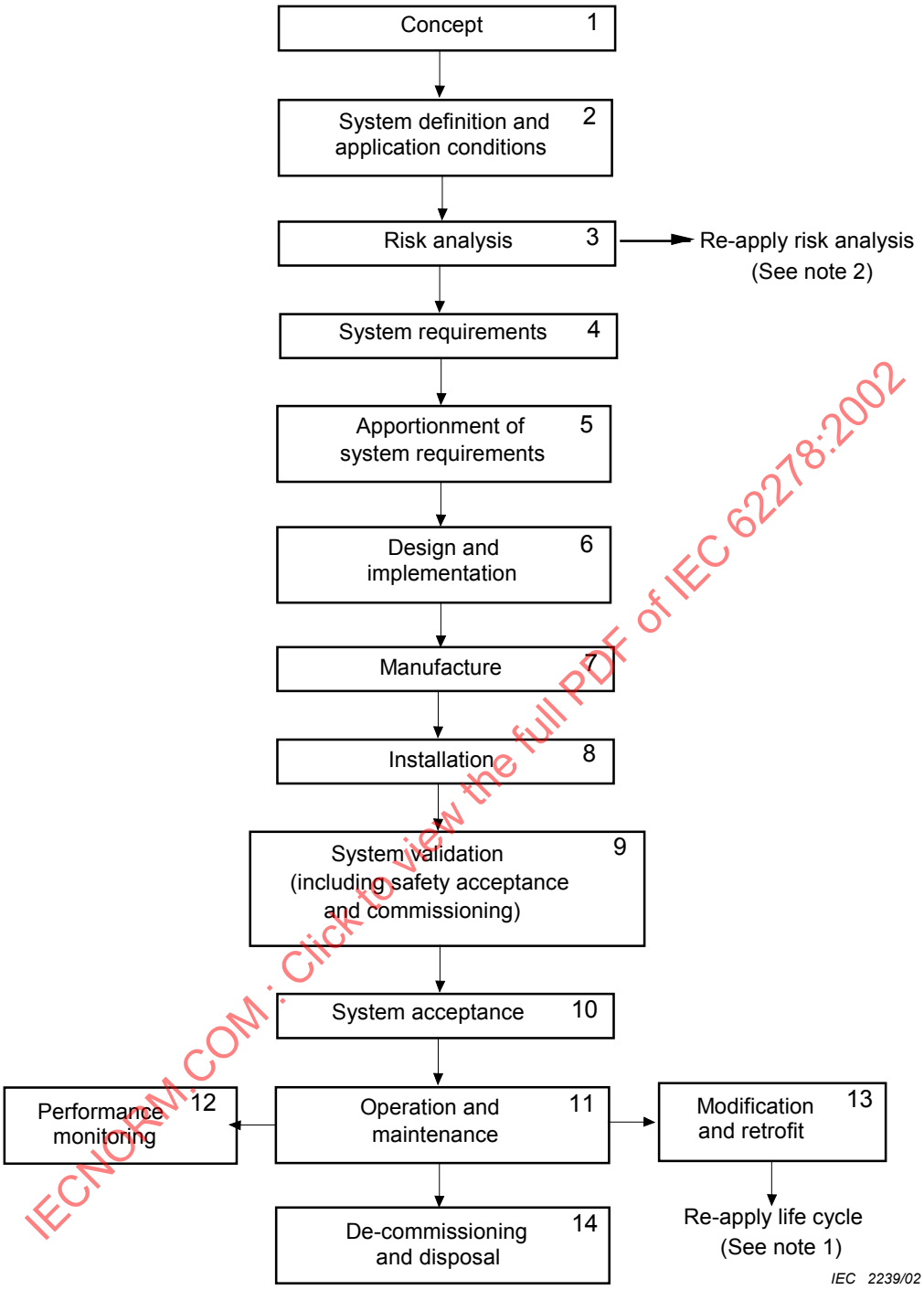
5.2.2 A system life cycle, appropriate in the context of railway application, is shown in figure 8. For each phase of the life cycle, the main tasks are summarised in figure 9. This figure shows RAMS tasks as components of general project tasks. The general tasks are outside the scope of this standard, but are representative of common industry practice. RAMS tasks contribute to the general project tasks for each phase and requirements for the RAMS tasks are detailed in subsequent clauses of this standard.



NOTE 1 La phase au cours de laquelle une modification est introduite dans le cycle de vie dépend à la fois du système modifié et de la modification particulière considérée.

NOTE 2 Il peut être nécessaire de renouveler l'analyse de risque à plusieurs étapes du cycle de vie (voir le point d) de 6.3.1).

Figure 8 – Cycle de vie du système



NOTE 1 The phase at which a modification enters the life cycle will be dependent upon both the system being modified and the specific modification under consideration.

NOTE 2 Risk analysis may have to be repeated at several stages of the life cycle (see item d) of 6.3.1).

Figure 8 – System life cycle

PHASE DU CYCLE DE VIE	TACHES GENERALES LIEES A CHAQUE PHASE	TACHES DE FDM LIEES A CHAQUE PHASE	TACHES DE SECURITE LIEES A CHAQUE PHASE
1. Concept	• Définir le domaine d'application et l'objectif du projet • Définir le concept du projet • Entreprendre l'analyse financière et les études de faisabilité • Etablir le management du projet	• Examiner les performances de FDM précédemment obtenues • Tenir compte des aspects de FDM du projet	• Examiner les performances de sécurité précédemment obtenues • Tenir compte des aspects sécuritaire du projet • Examiner la politique et les objectifs de sécurité
2. Définition du système et conditions d'application	• Définir le profil de mission du système • Préparer la description du système • Identifier les stratégies d'exploitation et de maintenance • Identifier les conditions d'exploitation • Identifier les conditions de maintenance • Identifier l'influence des contraintes de l'infrastructure existante sur le système	• Evaluer les données du retour d'expérience relatives à la FDM • Effectuer l'analyse préliminaire de FDM • Etablir la politique de FDM • Identifier les conditions d'exploitation et de maintenance à long terme • Identifier l'influence des contraintes de l'infrastructure existante sur la FDM du système	• Evaluer les données du retour d'expérience relative à la sécurité • Effectuer l'analyse préliminaire des situations dangereuses • Etablir le Plan (Global) de Sécurité • Définir les critères d'acceptabilité du risque • Identifier les contraintes de l'infrastructure existante sur la sécurité du système
3. Analyse de risques (voir note 6)	• Entreprendre l'analyse de risques liée au projet		• Effectuer l'analyse des situations dangereuses et des risques pour la sécurité du système • Ouvrir le Registre des Situations Dangereuses • Procéder l'évaluation du risque
4. Exigences du système	• Analyser les exigences • Spécifier le système (exigences globales) • Spécifier l'environnement • Définir les critères de démonstration et d'acceptation du système (exigences globales) • Etablir le Plan de Validation • Définir les exigences en termes de management, de qualité et d'organisation • Mettre en œuvre la procédure de maîtrise des modifications	• Spécifier les exigences (globales) de FDM du système • Définir les critères (globaux) d'acceptation de la FDM • Définir la structure fonctionnelle du système • Etablir le Programme de FDM • Définir le management de la FDM	• Spécifier les exigences (globales) de sécurité du système • Définir les critères (globaux) d'acceptation de la sécurité • Définir les exigences fonctionnelles relatives à la sécurité • Définir le management de la Sécurité

Figure 9 – Tâches liées aux différentes phases du projet (feuille 1 sur 4)

IEC 2240/02

LIFE CYCLE PHASE	PHASE RELATED GENERAL TASKS	PHASE RELATED RAM TASKS	PHASE RELATED SAFETY TASKS
1. Concept	• Establish scope and purpose of railway project • Define railway project concept • Undertake financial analysis and feasibility studies • Establish management	• Review previously achieved RAM performance • Consider RAM implications of project	• Review previously achieved safety performance • Consider safety implications of project • Review safety policy and safety targets
2. System definition and application conditions	• Establish system mission profile • Prepare system description • Identify operation and maintenance strategies • Identify operating conditions • Identify maintenance conditions • Identify influence of existing infrastructure constraints	• Evaluate past experience data for RAM • Perform preliminary RAM analysis • Set RAM policy • Identify long-term operation and maintenance conditions • Identify influence on RAM of existing infrastructure constraints	• Evaluate past experience data for safety • Perform preliminary hazard analysis • Establish Safety Plan (overall) • Define tolerability of risk criteria • Identify influence on safety of existing infrastructure constraints
3. Risk analysis (see note 6)	• Undertake project related risk analysis		• Perform system hazard and safety risk analysis • Set up Hazard Log • Perform risk assessment
4. System requirements	• Undertake requirements analysis • Specify system (overall requirements) • Specify environment • Define system demonstration and acceptance criteria (overall requirements) • Establish Validation Plan • Establish management, quality and organisation requirements • Implement change control procedure	• Specify system RAM requirements (overall) • Define RAM acceptance criteria (overall) • Define system functional structure • Establish RAM programme • Establish RAM management	• Specify system safety requirements (overall) • Define safety acceptance criteria (overall) • Define safety related functional requirements • Establish safety management

IEC 2240/02

Figure 9 – Project phase related tasks (sheet 1 of 4)

PHASE DU CYCLE DE VIE	TACHES GENERALES LIEES A CHAQUE PHASE	TACHES DE FDM LIEES A CHAQUE PHASE	TACHES DE SECURITE LIEES A CHAQUE PHASE
5. Allocation des exigences du système	• Allouer les exigences du système – Spécifier les exigences des sous-systèmes et des composants – Définir les critères d'acceptation des sous-systèmes et des composants	• Allouer les exigences de FDM – Spécifier les exigences de FDM des sous-systèmes et des composants – Définir les critères d'acceptation des sous-systèmes et des composants en termes de FDM	• Allouer les exigences et les objectifs de sécurité – Spécifier les exigences de sécurité des sous-systèmes et des composants – Définir les critères d'acceptation des sous-systèmes et des composants en termes de Sécurité • Mettre à jour le Plan de Sécurité du système
6. Conception et réalisation	• Mettre au point la planification • Réaliser la conception et le développement • Effectuer l'analyse de la conception et les essais • Procéder à la vérification de la conception • Procéder à la mise en œuvre et à la validation • Réaliser la conception des moyens du soutien logistique	• Mettre en œuvre le Programme de FDM par examen, analyse, essai et évaluation des données, prenant en compte – la fiabilité et la disponibilité – la maintenance et la maintenabilité – la politique optimale de maintenance – le soutien logistique • Procéder au contrôle du Programme, prenant en compte: – le management du Programme de FDM – le contrôle des sous-traitants et fournisseurs	• Mettre en œuvre le Plan de Sécurité par examen, analyse, essai et évaluation des données, prenant en compte – le Registre des Situations Dangereuses – l'analyse des situations dangereuses et l'évaluation du risque • Justifier les choix de conception liés à la sécurité • Procéder au contrôle du Programme, prenant en compte – le management de la sécurité – le contrôle des sous-traitants et des fournisseurs • Préparer le Dossier de Sécurité Générique • Préparer (le cas échéant) le Dossier de Sécurité Générique de l'Application
7. Fabrication	• Mettre au point la programmation de la production • Procéder à la fabrication • Procéder à la fabrication et aux essais des sous-ensembles de composants • Préparer la documentation • Mettre au point la formation	• Procéder aux essais d'environnement • Procéder aux essais d'amélioration de la FDM • Lancer le Système de Signalement, d'Analyse et de Correction des Défaillances (SSACD)	• Mettre en œuvre le Plan de Sécurité par examen, analyse, essai et évaluation des données • Utiliser le Registre des Situations Dangereuses

IEC 2241/02

Figure 9 – Tâches liées aux différentes phases du projet (feuille 2 sur 4)

LIFE CYCLE PHASE	PHASE RELATED GENERAL TASKS	PHASE RELATED RAM TASKS	PHASE RELATED SAFETY TASKS
5. Apportionment of system requirements	• Apportion system requirements – Specify sub-system and component requirements – Define sub-system and component acceptance criteria	• Apportion system RAM requirements – Specify sub-system and component RAM requirements – Define sub-system and component RAM acceptance criteria	• Apportion system safety targets and requirements – Specify sub-system and component safety requirements – Define sub-system and component safety acceptance criteria • Update system Safety Plan
6. Design and implementation	• Perform planning • Perform design and development • Perform design analysis and testing • Perform design verification • Perform implementation and validation • Perform design of logistic support resources	• Implement RAM Programme by review, analysis, testing and data assessment, covering: – reliability and availability – maintenance and maintainability – optimal maintenance policy – logistic support • Undertake Programme control, covering: – RAM Programme management – control of sub-contractors and suppliers	• Implement Safety Plan by review, analysis, testing and data assessment, addressing: – Hazard Log – hazard analysis and risk assessment • Justify safety related design decisions • Undertake Programme control, covering: – safety mnagement – control of sub-contractors and suppliers • Prepare Generic Safety Case • Prepare (if appropriate) Generic Application Safety Case
7. Manufacturing	• Perform production planning • Manufacture • Manufacture and test sub-assembly of components • Prepare documentation • Establish training	• Perform environmental stress screening • Perform RAM improvement testing • Commence Failure Reporting Analysis and Corrective Action System (FRACAS)	• Implement Safety Plan by review, analysis, testing and data assessment • Use Hazard Log

IEC 2241/02

Figure 9 – Project phase related tasks (sheet 2 of 4)

PHASE DU CYCLE DE VIE	TACHES GENERALES LIEES A CHAQUE PHASE	TACHES DE FDM LIEES A CHAQUE PHASE	TACHES DE SECURITE LIEES A CHAQUE PHASE
8. Installation	• Assembler le système • Installer le système	• Démarrer la formation du personnel chargé de la maintenance • Prévoir la fourniture des pièces de rechange et de l'outillage	• Etablir le Plan d'Installation • Mettre en œuvre le Plan d'Installation
9. Validation du système (comprenant l'acceptation de la sécurité et la mise en état de fonctionnement)	• Mettre le système en état de fonctionnement • Exploiter pendant la période probatoire • Entreprendre la formation	• Effectuer la démonstration de la FDM	• Etablir le Plan de Mise en état de fonctionnement • Mettre en œuvre le Plan de Mise en état de fonctionnement • Préparer le Dossier de Sécurité à l'Application
10. Acceptation du système	• Conduire les procédures d'acceptation, sur la base des critères d'acceptation • Rassembler les preuves pour l'acceptation • Mettre en exploitation • Continuer la période probatoire d'exploitation (le cas échéant)	• Evaluer la démonstration de la FDM	• Evaluer le Dossier de Sécurité à l'Application
11. Exploitation et maintenance	• Exploitation courante du système • Procéder aux opérations courantes de maintenance • Réaliser la formation continue	• S'approvisionner régulièrement en pièces de rechange et en outillage • Mettre en œuvre une maintenance et un soutien logistique fondés sur la fiabilité	• Mettre en œuvre les opérations de maintenance courante fondées sur la sécurité • Surveiller régulièrement les performances de sécurité et tenir le Registre des Situations Dangereuses
12. Surveillance des performances	• Rassembler les statistiques de performances opérationnelles • Acquérir, analyser et évaluer les données	• Recueillir, analyser, évaluer et utiliser les statistiques de performances et de FDM	• Recueillir, analyser, évaluer et utiliser les statistiques de performances et de sécurité
13. Modification et remise à niveau	• Appliquer les procédures de demande de modification • Appliquer les procédures de modification et de remise à niveau	• Prendre en compte les aspects de la FDM relatifs aux modifications et à la remise à niveau	• Prendre en compte les aspects de la sécurité relatifs aux modifications et à la remise à niveau
14. Retrait du service et dépose	• Programmer le retrait du service et la dépose • Procéder au retrait du service • Procéder à la dépose	• Pas d'activité de FDM	• Etablir un Plan de Sécurité • Procéder à l'analyse des situations dangereuses et à l'évaluation du risque • Mettre en œuvre le Plan de Sécurité

IEC 2242/02

Figure 9 – Tâches liées aux différentes phases du projet (feuille 3 sur 4)

LIFE CYCLE PHASE	PHASE RELATED GENERAL TASKS	PHASE RELATED RAM TASKS	PHASE RELATED SAFETY TASKS
8. Installation	• Assemble system • Install system	• Start maintainer training • Establish spare parts and tool provision	• Establish Installation Programme • Implement Installation Programme
9. System validation (including safety acceptance and commissioning)	• Commission • Perform probationary period of operation • Undertake training	• Perform RAM demonstration	• Establish Commissioning Programme • Implement Commissioning Programme • Prepare Application Specific Safety Case
10. System acceptance	• Undertake acceptance procedures, based on acceptance criteria • Compile evidence for acceptance • Entry into service • Continue probationary period of operation (if appropriate)	• Assess RAM demonstration	• Assess Application Specific Safety Case
11. Operation and maintenance	• Long-term system operation • Perform On Going Maintenance • Undertake On Going Training	• On-going procurement of spare parts and Tools • Perform on-going reliability-centred maintenance logistic support	• Undertake on-going safety-centred maintenance • Perform on-going safety performance monitoring and Hazard Log maintenance
12. Performance monitoring	• Collect operational performance statistics • Acquire, analyse and evaluate data	• Collect, analyse, evaluate and use performance and RAM statistics	• Collect, analyse, evaluate and use performance and safety statistics
13. Modification and retrofit	• Implement change request procedures • Implement modification and retrofit procedures	• Consider RAM implications for modification and retrofit	• Consider safety implications for modification and retrofit
14. Decommissioning and disposal	• Plan decommissioning and disposal • Undertake decommissioning • Undertake disposal	• No activity for RAM	• Establish Safety Plan • Perform hazard analysis and risk assessment • Implement Safety Plan

IEC 2242/02

Figure 9 – Project phase related tasks (sheet 3 of 4)

NOTE 1 Les activités de contrôle des modifications ou de gestion de configuration s'appliquent à toutes les phases du projet.

NOTE 2 Les activités de vérification et de validation s'appliquent à la plupart des phases du cycle de vie et sont incluses dans le corps du texte.

NOTE 3 Pour la FDM, le terme «Programme de FDM» est d'un usage courant et a été adopté par cette norme. Pour la sécurité, le terme «Plan de Sécurité» est d'un usage courant et a été adopté par cette norme.

NOTE 4 Il est à noter que le domaine d'application de cette norme se limite à la FDMS et que celle-ci ne traite pas de l'ensemble des activités d'assurance systèmes. Il est cependant nécessaire d'assurer la synchronisation entre les phases de FDM et les phases correspondantes au projet, et de convenir, du point de vue des exigences de FDMS, des conditions de transition d'une phase à l'autre.

NOTE 5 Selon l'application considérée, il est permis de regrouper les activités des phases 9 et 10.

NOTE 6 Il peut être nécessaire de renouveler l'analyse de risque à plusieurs étapes différentes (voir 4.6.2 et 6.3.1d)).

IEC 2243/02

Figure 9 – Tâches liées aux différentes phases du projet (feuille 4 sur 4)

NOTE 1 Change control or configuration management activity applies to all project phases.

NOTE 2 Verification and validation activities apply within most life cycle phases and are included in the main text.

NOTE 3 For RAM, the term “RAM Programme” is in common use and is adopted by this standard. For safety, the term “Safety Plan” is in common use and is adopted by this standard.

NOTE 4 Note that the scope of this standard is limited to RAMS and does not address all systems assurance activities. However, it is necessary to ensure the synchronisation between RAMS phases and project related phases, and to agree on the conditions for passing from one phase to another, from RAMS point of view.

NOTE 5 Activities within phases 9 and 10 may be integrated, depending upon the application under consideration.

NOTE 6 Risk analysis may have to be repeated at several stages (see 4.6.2 and 6.3.1d)).

IEC 2243/02

Figure 9 – Project phase related tasks (sheet 4 of 4)

5.2.3 Cette norme admet la nécessité d'établir un équilibre entre les performances de FDMS d'un système et le coût de développement et d'usage de ce système, connu sous l'appellation coût global. Cette norme exige que le coût global d'un système soit pris en compte en liaison avec les aspects de FDMS de ce système. Cependant, elle n'impose pas de réponses aux questions concernant la FDMS fondées sur le coût car elles incombent à la société d'exploitation ferroviaire.

5.2.4 L'article 6 définit, sous une même forme et dans un contexte global de projet, les objectifs, les exigences, les éléments d'entrée et les éléments de sortie des tâches de FDMS propres à chaque phase du cycle de vie.

5.2.5 Le processus fournit, sous forme séquentielle, le détail des tâches à accomplir au cours des différentes phases du cycle de vie. Il sert de base pour conclure en toute connaissance de cause des accords relatifs soit à des tâches particulières de FDMS, soit à une combinaison de tâches dans le cadre d'un processus intégré de management. La responsabilité d'exécution de ces tâches dépend du système concerné et des conditions contractuelles applicables. Certaines lignes directrices d'ordre général permettant de déterminer cette responsabilité sont données à l'annexe E.

5.2.6 Cette norme présente le cycle de vie du système de manière séquentielle. Cette représentation fait apparaître chaque phase isolément ainsi que les liens entre les différentes phases. La représentation en «V» est une des nombreuses représentations du cycle de vie répandues dans l'industrie.

5.2.7 Une représentation en «V» du cycle de vie est donnée à la figure 10 de cette norme. La branche descendante (à gauche) est généralement appelée conception et développement; il s'agit d'un processus de plus en plus détaillé qui s'achève par la fabrication des composants du système. La branche ascendante (côté droit) concerne l'assemblage, l'installation, la réception ainsi que l'exploitation du système global.

5.2.8 La représentation en «V» suppose que les activités d'acceptation sont intrinsèquement liées aux activités de conception et de développement dans la mesure où ce qui est effectivement conçu doit *in fine* être vérifié eu égard aux exigences. Ainsi, les activités de validation liées à l'acceptation, lors des différentes étapes de l'élaboration d'un système, sont fondées sur les spécifications de ce système et il est recommandé de les prévoir très tôt, c'est-à-dire dès le début des étapes de conception et de développement du cycle de vie. Cette liaison est illustrée à la figure 11.

5.2.9 Cette représentation montre de manière efficace les tâches de vérification et de validation au cours du cycle de vie. L'objectif de la vérification est de démontrer que, pour des éléments d'entrée spécifiques, les éléments de sortie de chaque phase satisfont en tous points aux exigences de cette phase. L'objectif de la validation est de démontrer que le système concerné, à toutes les étapes de son développement et après son installation, satisfait en tous points aux exigences applicables.

5.2.10 Dans cette norme, des tâches de vérification sont incluses dans chaque phase du cycle de vie. Cette norme n'aborde l'assurance qualité du système que sous les aspects liés à la FDMS; or, les tâches de vérification et de validation (V et V) font partie intégrante de la démonstration globale de l'assurance qualité du système. En conséquence, les tâches de V et V de la FDMS contribuent aux tâches de V et V de l'assurance du système global.

5.2.3 This standard acknowledges the balance between the RAMS performance of a system and the costs of development and ownership of the system, known as life cycle costs. This standard requires a consideration of the life cycle costs associated with the RAMS aspects of a system. However, it does not dictate solutions to RAMS issues on the basis of cost, as this is the responsibility of the Railway Authority.

5.2.4 Clause 6 and its subclauses define the objectives, requirements, inputs and deliverables for RAMS tasks in a consistent format, and within an overall project context, for each life cycle phase.

5.2.5 The process supports procurement by providing a comprehensive sequence of tasks within life cycle phases. This provides a basis for the informed contracting of either individual RAMS tasks or a combination of tasks within an integrated management process. Responsibilities for carrying out the tasks will depend on the system under consideration and the contract conditions applicable. Some general guidelines for establishing these responsibilities are given in annex E.

5.2.6 This standard represents the system life cycle sequentially. This representation shows individual phases and the links between phases. Other life cycle representations are widespread within industry and include the ”V” model.

5.2.7 A ”V” representation of the life cycle contained within this standard is shown in figure 10. The top-down branch (left side) is generally called design and development and is a refining process ending with the manufacturing of system components. The bottom-up branch (right side) is related to the assembly, the installation, the receipt and then the operation of the whole system.

5.2.8 The "V" representation assumes that the activities of acceptance are intrinsically linked to the design and development activities insofar as what is actually designed has to be finally checked in regard to the requirements. So the validation activities for acceptance at various stages of a system are based on the specification of the system and should be planned in the earlier stages, i.e. starting at the corresponding design and development phases of the life cycle. Such a link is shown in figure 11.

5.2.9 This representation is effective in showing verification and validation tasks within the life cycle. The objective of verification is to demonstrate that, for the specific inputs, the deliverables of each phase meet in all respects the requirements of that phase. The objective of validation is to demonstrate that the system under consideration, at any step of its development and after its installation, meets its requirements in all respects.

5.2.10 In this standard, verification tasks are included within each life cycle phase. Although this standard is concerned with system assurance in the context of RAMS, verification and validation (V&V) tasks are integral to the overall demonstration of systems assurance. Consequently, RAMS V&V contributes to overall system assurance V&V.

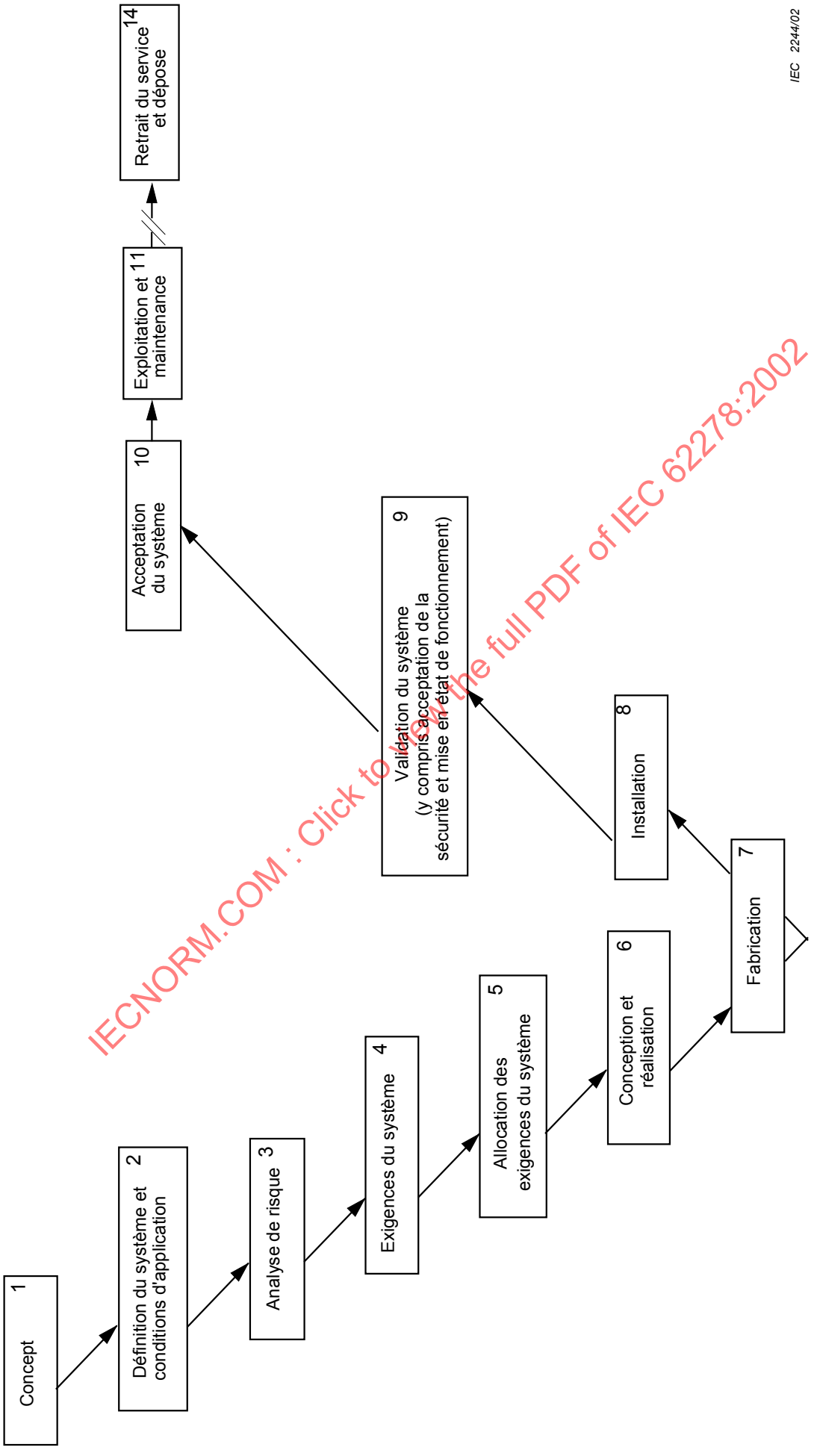


Figure 10 – Représentation en «V»

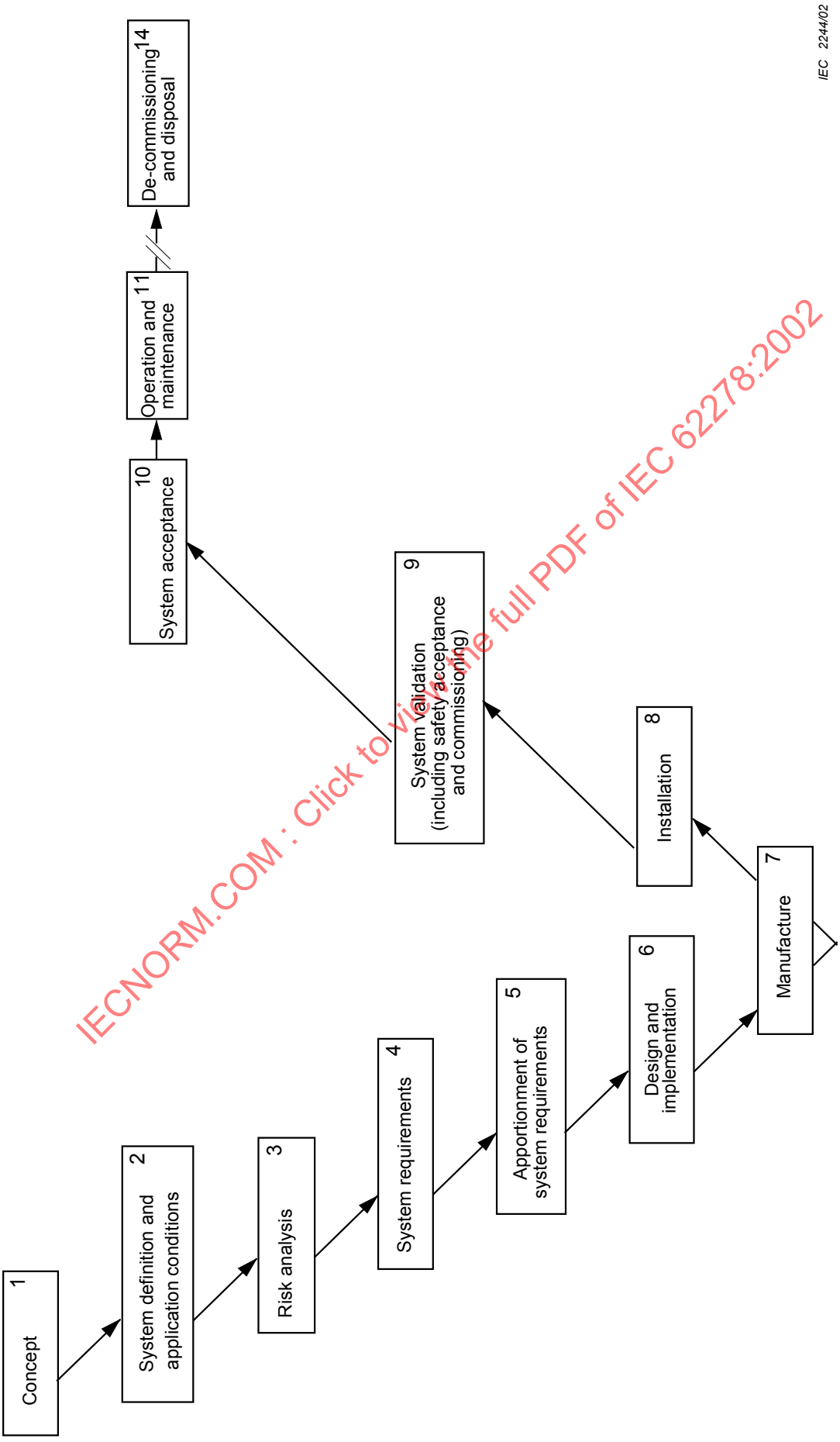
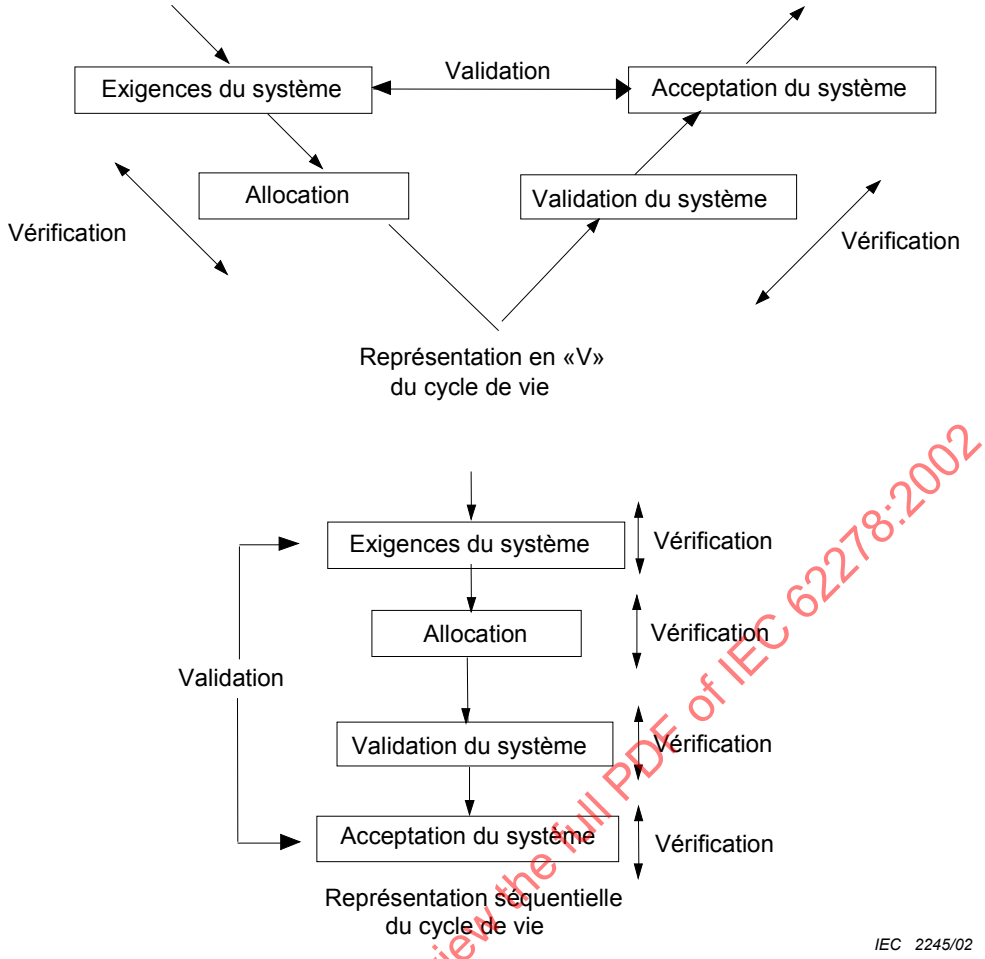


Figure 10 – The "V" representation



NOTE Le paragraphe 5.2.9 fournit des informations supplémentaires quant au rôle de la vérification et de la validation. La validation est indiquée pour inclure le bloc acceptation du système car des tâches de validation peuvent être conduites dans cette phase (voir aussi 6.9.1 et 6.10.1).

Figure 11 – Vérification et validation

5.3 Application de cette norme

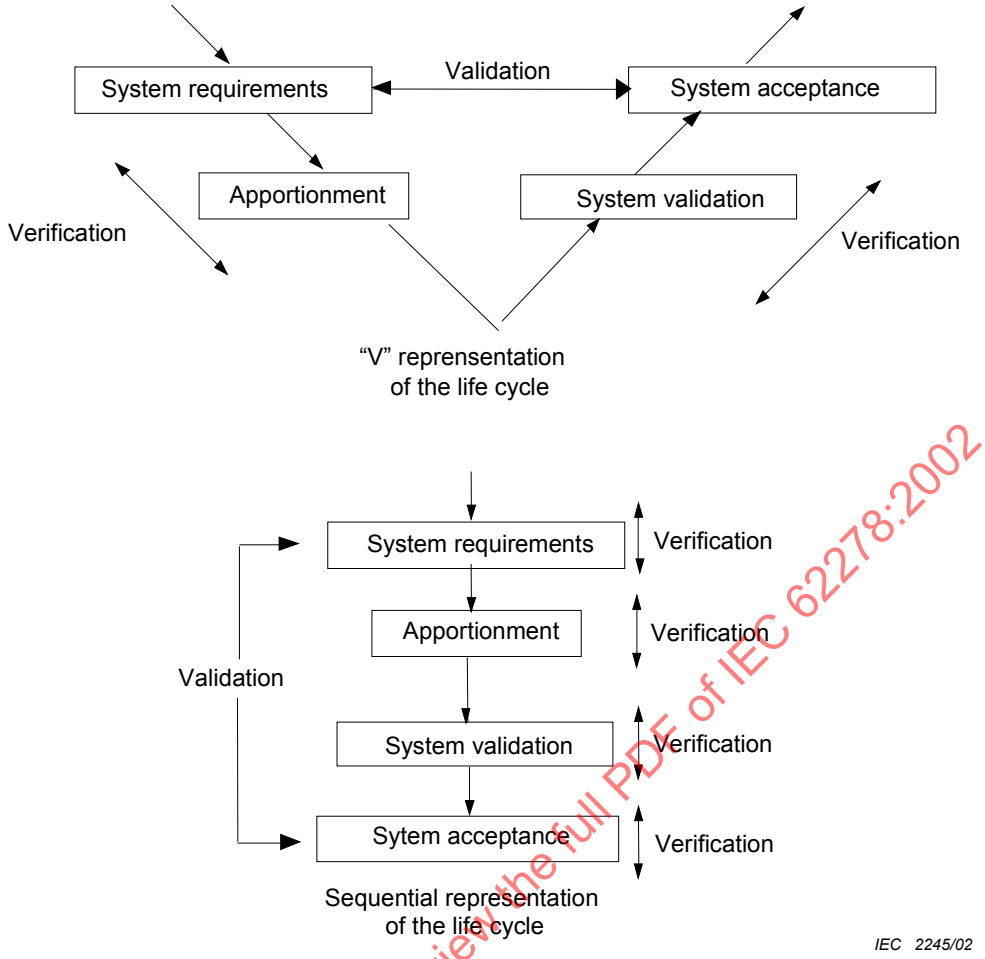
5.3.1 Ce paragraphe décrit les conditions requises pour appliquer, de manière souple et efficace, cette norme aux systèmes ferroviaires, compte tenu de leur dimension, de leur complexité et de leur coût.

5.3.2 Les exigences définies dans cette norme sont génériques, elles sont applicables à tout type de système ferroviaire. La société d'exploitation ferroviaire doit définir les conditions d'application des exigences de cette norme au système concerné. Cette définition doit être fondée sur l'aptitude des exigences à s'appliquer à un système particulier. L'évaluation de la succession des tâches effectuées lors de la phase 9 (Validation du système), et lors de la phase 10 (Acceptation du système), doit faire l'objet d'une attention particulière.

5.3.3 En cas de rénovation d'un système donné, il y a souvent une «phase mixte» au cours de laquelle il y a une exploitation simultanée ou concomitante du système existant et du système rénové. Dans ce cas, une étude de sécurité doit traiter, de manière spécifique, les éventuels effets d'une interaction entre le système existant et le système rénové.

5.3.4 L'application de cette norme doit être adaptée aux exigences spécifiques du système considéré. Pour appliquer cette norme au système considéré, il faut

a) préciser, en les justifiant, les phases du cycle de vie qui sont nécessaires à l'élaboration du système considéré, en démontrant que les tâches effectuées dans le cadre de ces phases sont conformes aux principes relatifs aux exigences de cette norme;



NOTE Subclause 5.2.9 provides additional information on the role of verification and validation. Validation is shown to include system acceptance block because some validation tasks may be covered in that phase (also see 6.9.1 and 6.10.1)

Figure 11 – Verification and validation

5.3 Application of this standard

5.3.1 This subclause gives requirements to provide a flexible and effective application of this standard to railway systems, in terms of size, complexity and cost.

5.3.2 The requirements defined in this standard are generic and are applicable to all types of railway systems. The Railway Authority shall define the application of the requirements of this standard to the system under consideration. This assessment shall be based on the applicability of the requirements to the particular system. Particular care is required during the assessment of the task sequences undertaken in phase 9 (System validation) and phase 10 (System acceptance).

5.3.3 In cases of renewal of a system, there is often a "mixed phase" stage where the operation with the existing and the renewed systems is mixed, or that they are operated at the same time. In such cases, safety study shall specifically address the possible effects of interaction between the existing and the renewed systems.

5.3.4 The application of this standard shall be adapted to the specific requirements of the system under consideration. The assessment of the application of this standard to the system under consideration shall:

a) specify the life cycle phases which are required to realise the system under consideration, providing a justification for the life cycle phases specified and demonstrating that the tasks undertaken within these life cycle phases comply with the principles of the requirements of this standard;

b) préciser les activités obligatoires et les exigences de chaque phase requise du cycle de vie en utilisant la liste de la figure 9 ainsi que les éléments de l'article 6 relatifs à chaque phase, ce qui comprend

   – le domaine d'application de chaque exigence eu égard au système considéré;

   – les méthodes, les outils et les techniques requis au regard de chaque exigence, leur domaine d'application et leur portée;

   – les activités de vérification et de validation requises au regard de chaque exigence et leur du domaine d'application;

   – l'ensemble de la documentation correspondante;

c) justifier tout écart par rapport aux activités et aux exigences de la norme;

d) justifier l'adéquation des tâches retenues pour l'application considérée.

5.3.5 Pour toutes les applications de cette norme, les exigences suivantes sont obligatoires:

a) l'attribution de l'exécution de toutes les tâches de FDMS au cours de chaque phase du cycle de vie, y compris celle des interfaces entre tâches connexes, doit être définie et convenue pour le système concerné;

b) l'ensemble des personnes ayant des responsabilités dans le cadre du processus de management de la FDMS doit disposer des compétences nécessaires;

c) l'établissement et la mise en œuvre du Programme de FDM et du Plan de Sécurité sont des éléments essentiels à la réalisation de systèmes sûrs. Alors que le contenu de ces derniers documents est spécifique au système concerné, de nombreuses tâches de FDMS nécessitent des analyses de même type. Cependant, les contraintes relatives à ces activités peuvent être différentes. Pour les tâches purement liées à la FDM, les considérations d'ordre économique sont susceptibles de constituer une priorité, tandis que la priorité des tâches centrées sur la sécurité consiste à éviter les accidents et les incidents. De ce point de vue, il est possible que les exigences de FDMS soient en conflit entre elles, étant donné que les conséquences économiques relatives à la FDMS peuvent être différentes, en fonction des exigences de la société d'exploitation ferroviaire. Le Programme de FDM et le Plan de Sécurité doivent prendre en compte la nécessité d'identifier et de traiter les conflits de FDMS et doivent comporter les détails de l'analyse de FDMS, du fait que les analyses peuvent être plus ou moins approfondies en fonction des tâches de FDMS;

d) les exigences de cette norme doivent être mises en oeuvre dans le cadre des politiques suivies par l'entreprise sur la base d'un Système de Management de la Qualité (SMQ) conforme aux dispositions de l'ISO 9001, adaptée au système concerné;

e) un système approprié et efficace de gestion de configuration, traitant des tâches de FDMS dans chacune des phases du cycle de vie, doit être établi et mis en oeuvre. Le domaine d'application de la gestion de configuration dépend du système considéré, mais il doit normalement inclure l'ensemble de la documentation du système ainsi que l'ensemble des autres éléments de sortie du système.

5.3.6 L'article 6 traite des moyens de satisfaire aux exigences de FDMS en minimisant les effets d'éventuelles défaillances et en maîtrisant les facteurs figurant à l'article 4, par la définition d'un processus de management fondé sur le cycle de vie du système. Des méthodes, des outils et des techniques appropriés à la réalisation de systèmes techniques sûrs sont présentés dans d'autres normes (voir annexe B). Il est important de noter que le choix des méthodes, des outils et des techniques, leur domaine d'application et leur portée, ainsi que ceux de la documentation correspondante, doivent être adaptés aux exigences du système considéré. Il convient que la société d'exploitation ferroviaire et le fournisseur s'entendent sur ces éléments pour le système considéré. La figure 12 donne un aperçu général de la manière dont ces différents aspects sont liés pour servir de support aux techniques et au management de la FDMS.

5.3.7 Les exigences figurant dans cette norme sont présentées de façon à permettre la conduite d'audits. La société d'exploitation ferroviaire et l'industrie ferroviaire doivent convenir d'un plan d'audit et le mettre en oeuvre; ce plan traite de l'application des exigences de cette norme en les adaptant au système considéré.

b) specify the mandatory activities and requirements of each required life cycle phase, using figure 9 and the relevant phase related information of clause 6 as a checklist, including:

- the scope of each requirement in relation to the system under consideration;
- the methods, tools and techniques required against each requirement and the scope and depth of their application;
- the verification and validation activities required against each requirement and the scope of their application;
- all supporting documentation.

c) justify any deviation from the activities and requirements of the standard;

d) justify the adequacy of the tasks chosen for the application under consideration.

5.3.5 Within all applications of this standard, the following requirements are mandatory:

a) responsibilities for carrying out all RAMS tasks within each phase of the life cycle, including the interfaces between associated tasks, shall be defined and agreed for the system under consideration;

b) all personnel with responsibilities within the RAMS management process shall be competent to discharge those responsibilities;

c) the establishment and implementation of the RAM Programme and Safety Plan are essential components in the realisation of dependable systems. Whilst the content of these planning documents will be specific to the system under consideration, many RAMS tasks will require similar analysis activities. However, the constraints on these activities may be different. For RAM-focused tasks, cost considerations are likely to be the prime driver, whereas for safety-focused tasks, it is the avoidance of accidents and incidents. Within this context, RAMS requirements can conflict, as the economic consequences pertaining to RAMS may be different, depending upon the requirements of the Railway Authority. Recognition of the need to identify and manage RAMS conflicts shall be included within RAMS planning documents, along with details of all RAMS analysis, as the depth of analysis activities may vary between RAMS tasks;

d) the requirements of this standard shall be implemented within the business processes, supported by a Quality Management System (QMS) compliant with the requirements of ISO 9001 appropriate for the system under consideration.

e) an adequate and effective configuration management system shall be established and implemented, addressing RAMS tasks within all life cycle phases. The scope of configuration management will depend on the system under consideration, but shall normally include all system documentation and all other system deliverables.

5.3.6 Clause 6 of this standard elaborates the means to ensure achievement of RAMS requirements through minimising the effects of any impairments and controlling the factors discussed in clause 4, by defining a management process based on the system life cycle. Methods, tools and techniques appropriate to engineering dependable systems are presented in other standards (see annex B). It is important to note that the choice of methods, tools and techniques, and the depth and scope of their application and that of the documentation, shall be commensurate with the requirements of the system under consideration. These should be agreed between the Railway Authority and the supplier for the system under consideration. A general overview of the manner in which these different aspects relate to support RAMS engineering and management is shown in figure 12.

5.3.7 The requirements detailed in this standard are written in order to support an audit process. The Railway Authority and the railway support industry for the system under consideration shall agree and implement an audit plan which addresses the application of the requirements of this standard, as adapted to the system.

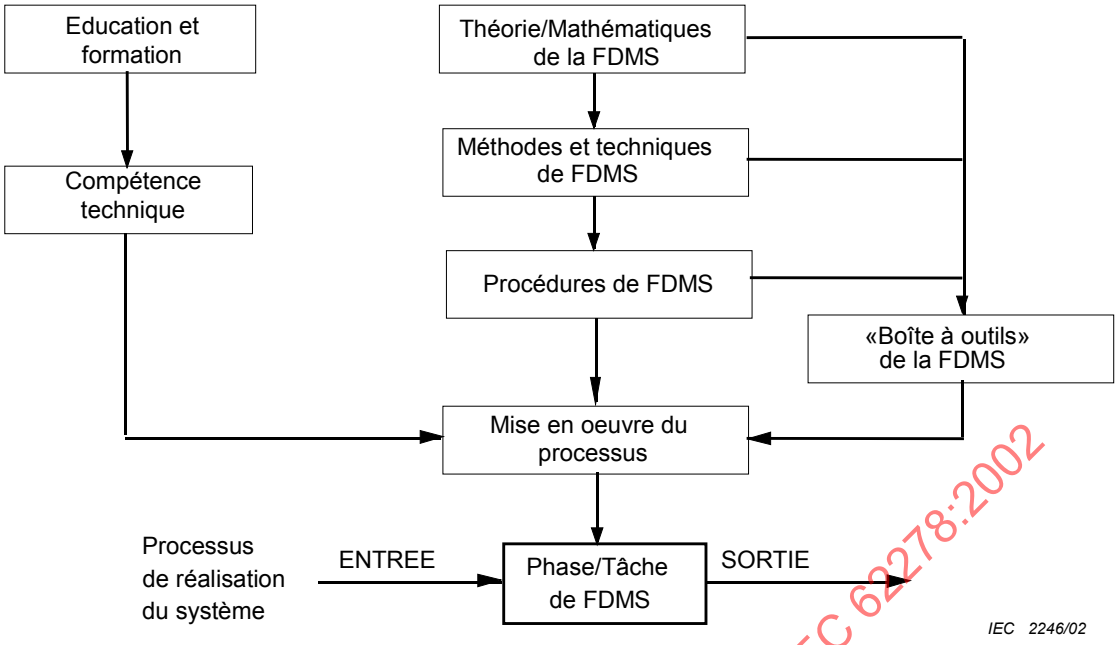


Figure 12 – Technique et management de la FDMS mis en oeuvre dans le cadre du processus de réalisation d'un système

6 Cycle de vie de la FDMS

Cet article décrit, de manière détaillée, les objectifs, les exigences, les éléments de sortie ainsi que les activités de vérification et de validation à entreprendre lors de chaque phase du cycle de vie du système. La portée des prescriptions de cette norme et leurs conditions d'application doivent être évaluées et adaptées aux exigences spécifiques du système considéré. Pour plus d'informations à ce sujet, voir 5.3.

6.1 Phase 1: Concept

6.1.1 Objectifs

L'objectif de la présente phase est de développer un niveau suffisant de compréhension du système pour permettre de réaliser de manière satisfaisante les tâches ultérieures du cycle de vie de la FDMS.

6.1.2 Eléments d'entrée

Les éléments d'entrée de la présente phase doivent comporter toutes les informations pertinentes et, le cas échéant, les données nécessaires pour satisfaire aux exigences de cette phase, par exemple, les considérations concernant le domaine d'application et le but du projet.

6.1.3 Exigences

6.1.3.1 L'exigence n° 1 de la présente phase doit être d'acquérir, du point de vue des performances de FDMS, la compréhension

a) du domaine d'application, du contexte et du but du système;

b) de l'environnement du système, y compris:

- les aspects physiques;
- les aspects relatifs aux interfaces potentielles du système;
- les aspects sociaux;
- les aspects politiques;

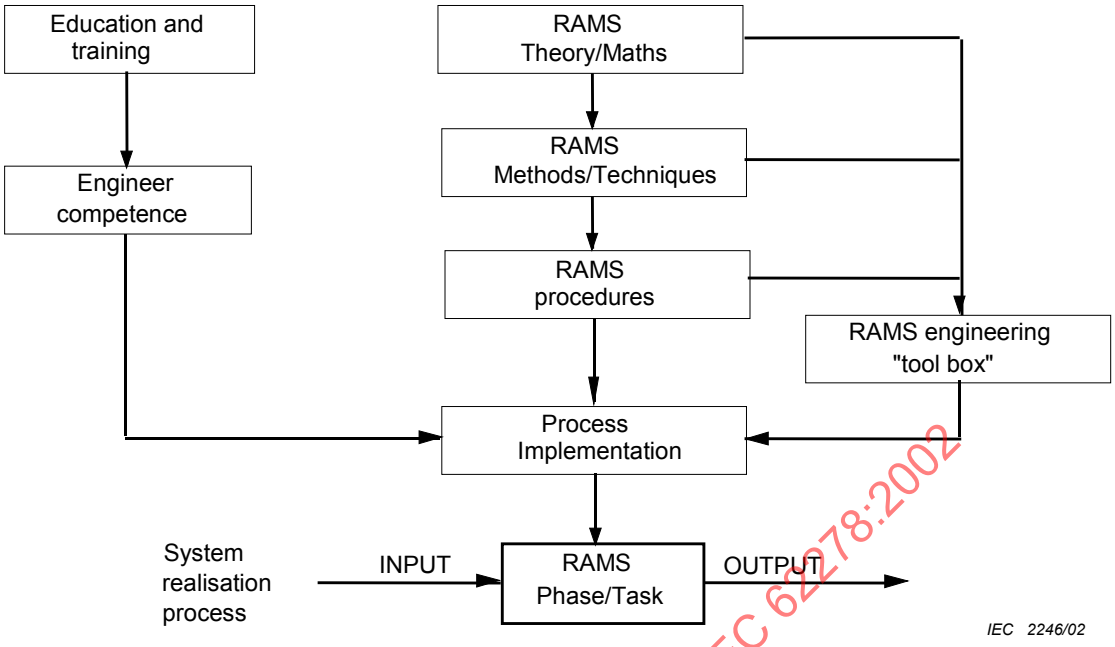


Figure 12 – RAMS engineering and management implemented within a system realisation process

6 RAMS life cycle

This clause details objectives, requirements, deliverables and verification and validation activities to be undertaken throughout each life cycle phase. The scope and application of the requirements shall be assessed and adapted to meet the particular requirements of the system under consideration. For further information on this topic, see 5.3.

6.1 Phase 1: Concept

6.1.1 Objectives

The objective of this phase shall be to develop a level of understanding of the system sufficient to enable all subsequent RAMS life cycle tasks to be satisfactorily performed.

6.1.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirements of the phase, for example the scope and purpose statements for the project.

6.1.3 Requirements

6.1.3.1 Requirement 1 of this phase shall be to acquire, in the context of RAMS performance, an understanding of

a) the scope, context and purpose of the system;

b) the environment of the system, including:

- physical issues;
- potential system interface issues;
- social issues;
- political issues;

– les aspects d'ordre légal;
– les aspects économiques;

c) des implications générales de la FDMS du système.

6.1.3.2 L'exigence n° 2 de la présente phase doit être d'examiner

a) les implications de toute analyse financière du système en termes de FDMS;
b) les implications de toutes les études de faisabilité du système en termes de FDMS.

6.1.3.3 L'exigence n° 3 de la présente phase doit être d'identifier les sources de situations dangereuses qui pourraient affecter les performances de FDMS du système, y compris:

– l'interaction avec d'autres systèmes;
– l'interaction avec l'homme.

6.1.3.4 L'exigence n° 4 de la présente phase doit être d'obtenir les informations relatives

a) aux exigences et performances antérieures de FDMS de systèmes similaires et/ou apparentés;
b) aux sources identifiées de situations dangereuses, du point de vue des performances de FDMS;
c) à la politique et aux objectifs de sécurité de la société d'exploitation ferroviaire;
d) à la réglementation de sécurité.

6.1.3.5 L'exigence n° 5 de la présente phase doit être de définir le domaine d'application des exigences en termes de management concernant les tâches de FDMS à accomplir dans la suite du cycle de vie du système.

6.1.4 Eléments de sortie

6.1.4.1 Les résultats de la présente phase doivent être documentés et comprendre les hypothèses et justificatifs correspondants.

6.1.4.2 Les éléments de sortie doivent inclure une organisation permettant de mettre en oeuvre les exigences de FDMS des phases 2, 3 et 4 du cycle de vie.

6.1.4.3 Les éléments de sortie de la présente phase constituent un point d'entrée déterminant pour les phases suivantes du cycle de vie.

6.1.5 Vérification

Les tâches de vérification suivantes doivent être effectuées lors de la présente phase:

a) l'évaluation de la pertinence des informations et, le cas échéant, des données et des autres informations statistiques, utilisées comme éléments d'entrée pour les tâches de FDMS de la présente phase;
b) l'évaluation de la pertinence des éléments d'environnement système définis au titre de l'exigence n° 1;
c) l'évaluation de l'exhaustivité de la liste des sources de situations dangereuses définie au titre de l'exigence n° 3;
d) l'évaluation de la pertinence des méthodes, des outils et des techniques utilisés au cours de la présente phase;
e) l'évaluation de la compétence de l'ensemble des personnes chargées d'effectuer des tâches au cours de la présente phase.

- legislative issues;
- economical issues;

c) the general RAMS implications of the system.

6.1.3.2 Requirement 2 of this phase shall be to review

a) the RAMS implications of any financial analysis of the system;

b) the RAMS implications of any system feasibility studies.

6.1.3.3 Requirement 3 of this phase shall be to identify sources of hazards which could affect the RAMS performance of the system, including:

- interaction with other systems;
- interaction with humans.

6.1.3.4 Requirement 4 of this phase shall be to obtain information about

a) previous RAMS requirements and past RAMS performance of similar and/or related systems;

b) identified sources of hazards to RAMS performance;

c) current Railway Authority safety policy and targets;

d) safety legislation.

6.1.3.5 Requirement 5 of this phase shall be to define the scope of the management requirements for subsequent system life cycle RAMS tasks.

6.1.4 Deliverables

6.1.4.1 The results from this phase shall be documented, along with any assumptions and justifications made during the phase.

6.1.4.2 The deliverables shall include a management structure adequate to implement the RAMS requirements of life cycle phases 2, 3 and 4

6.1.4.3 The deliverables from this phase are a key input to subsequent life cycle phases.

6.1.5 Verification

The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to RAMS tasks within this phase;

b) assessment of the adequacy of the system environment statement defined under Requirement 1;

c) assessment of the completeness of the hazard source listing defined under Requirement 3;

d) assessment of the adequacy of the methods, tools and techniques used within the phase;

e) assessment of the competence of all personnel undertaking tasks within the phase.

6.2 Phase 2: Définition du système et conditions d'application

6.2.1 Objectifs

Les objectifs de la présente phase sont

a) de définir le profil de mission du système;

b) de définir les frontières du système;

c) de définir les conditions d'application ayant une influence sur les caractéristiques du système;

d) de définir le domaine d'analyse des situations dangereuses du système;

e) de définir la politique de FDMS du système;

f) d'établir le Plan de Sécurité du système;

dans la mesure où ils affectent les performances potentielles de FDMS du système.

6.2.2 Eléments d'entrée

Les éléments d'entrée de la présente phase doivent comporter toutes les informations pertinentes et, le cas échéant, les données nécessaires pour satisfaire aux exigences de la phase, y compris les éléments de sortie de la phase 1.

6.2.3 Exigences

6.2.3.1 L'exigence n° 1 de la présente phase doit être de définir

a) le profil de mission du système, y compris:
   - les exigences de performances;
   - les objectifs de FDMS;
   - la stratégie et les conditions d'exploitation à long terme;
   - la stratégie et les conditions de maintenance à long terme;
   - les aspects relatifs à la durée de vie du système, y compris les questions concernant le coût global;
   - les problèmes d'ordre logistique;

b) les frontières du système, y compris:
   - les interfaces avec l'environnement physique;
   - les interfaces avec les autres systèmes technologiques;
   - les interfaces avec l'homme;
   - les interfaces avec les autres sociétés d'exploitation ferroviaire;

c) les conditions d'application qui influencent le système, y compris:
   - les contraintes imposées par l'infrastructure existante;
   - les conditions d'exploitation du système;
   - les conditions de maintenance du système;
   - les considérations relatives au soutien logistique;
   - l'examen du retour d'expérience dans des systèmes similaires;

6.2 Phase 2: System definition and application conditions

6.2.1 Objectives

The objectives of this phase are to

a) define the mission profile of the system;
b) define the boundary of the system;
c) establish the application conditions influencing the characteristics of the system;
d) define the scope of system hazard analysis;
e) establish the RAMS policy for the system;
f) establish the Safety Plan for the system;

insofar as they affect the potential RAMS performance of the system.

6.2.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirements of the phase, including the deliverables of phase 1.

6.2.3 Requirements

6.2.3.1 Requirement 1 of this phase shall be to define

a) the system mission profile, including:
   – performance requirements;
   – RAMS targets;
   – long-term operating strategy and conditions;
   – long-term maintenance strategy and conditions;
   – system life considerations, including life cycle costing issues;
   – logistic considerations;
b) the system boundary, including:
   – interfaces with physical environment;
   – interfaces with other technological systems;
   – interfaces with humans;
   – interfaces with other Railway Authorities;
c) the scope of application conditions influencing the system, including:
   – constraints imposed by existing infrastructure;
   – system operating conditions;
   – system maintenance conditions;
   – logistic support considerations;
   – review of past experience data for similar systems;

d) le domaine d'analyse des situations dangereuses du système, y compris l'identification
   - des situations dangereuses inhérentes au processus à maîtriser;
   - des situations dangereuses pour l'environnement;
   - des situations dangereuses du point de vue de la vulnérabilité;
   - de l'influence des événements extérieurs;
   - des frontières du système à analyser;
   - de l'influence des contraintes de l'infrastructure existante sur la FDMS.

6.2.3.2 L'exigence n° 2 de la présente phase doit être de réaliser

a) l'analyse préliminaire de FDM destinée à conforter les objectifs;
b) l'analyse préliminaire des situations dangereuses:
   - l'identification des sous-systèmes associés aux situations dangereuses identifiées;
   - l'identification des types d'événements potentiellement dangereux dont il est nécessaire de tenir compte, y compris les défaillances de composants, les erreurs de procédure, les erreurs humaines ainsi que les processus de défaillances qui en résultent;
   - la définition des critères initiaux d'acceptabilité du risque.

6.2.3.3 L'exigence n° 3 de la présente phase doit être d'établir la politique générale de FDMS du système, y compris les exigences liées à la sécurité et la politique de la société d'exploitation ferroviaire en matière de traitement des éventuels conflits entre «disponibilité» et «sécurité».

6.2.3.4 L'exigence n° 4 de la présente phase doit être d'établir le Plan de Sécurité du système. Le Plan de Sécurité doit être approuvé par la société d'exploitation ferroviaire et par les industries ferroviaires concernées; il doit être mis en œuvre et suivi tout au long du cycle de vie du système. Il convient que le Plan de Sécurité comporte

a) la politique et la stratégie relative à la sécurité;
b) le champ d'application du plan;
c) la description du système;
d) la description détaillée des fonctions, des responsabilités, de la compétence et des relations des organismes chargés d'accomplir des tâches au cours du cycle de vie;
e) la présentation du cycle de vie du système et des tâches de sécurité à accomplir au cours du cycle de vie ainsi que des éventuelles tâches associées;
f) les processus d'analyse de sécurité, d'ingénierie et d'évaluation à mettre en œuvre au cours du cycle de vie, y compris les processus
   - permettant d'assurer un degré adéquat d'indépendance du personnel dans l'accomplissement des tâches, en fonction des risques du système;
   - d'identification et d'analyse des situations dangereuses;
   - d'estimation et de management continu du risque;
   - de détermination des critères d'acceptabilité du risque;
   - de mise en place et de suivi continu de l'adéquation des exigences de sécurité;
   - de conception du système;
   - de vérification et de validation;
   - d'évaluation de la sécurité de nature à obtenir un résultat conforme aux exigences du système;
   - d'audit de sécurité de nature à obtenir un processus de management conforme au plan de sécurité;
   - d'évaluation de la sécurité de nature à assurer la cohérence entre l'analyse de sécurité des sous-systèmes et celle du système;

d) the scope of the system hazard analysis, including the identification of
   - hazards inherent within the process to be controlled;
   - environmental hazards;
   - security hazards;
   - the influence of external events;
   - the boundaries of the system to be analysed;
   - the influence on RAMS of existing infrastructure constraints.

6.2.3.2 Requirement 2 of this phase shall be to perform

a) preliminary RAM analysis to support targets;
b) preliminary hazard identification to
   - identify sub-systems associated with identified hazards;
   - identify types of accident initiating events that need to be considered, including component failure, procedural faults, human error and dependent failure mechanisms;
   - define initial risk tolerability criteria.

6.2.3.3 Requirement 3 of this phase shall be to establish the general RAMS policy for the system, including requirements of safety concept and the Railway Authority's policy for resolving any conflicts arising between "availability" and "safety".

6.2.3.4 Requirement 4 of this phase shall be to establish the Safety Plan for the system. The Safety Plan shall be agreed by the Railway Authority and the railway support industry for the system under consideration and shall be implemented, reviewed and maintained throughout the life cycle of the system. The Safety Plan should include

a) the policy and strategy for achieving safety;
b) the scope of the plan;
c) a description of the system;
d) details of roles, responsibilities, competencies and relationships of bodies undertaking tasks within the life cycle;
e) description of the system life cycle and safety tasks to be undertaken within the life cycle along with any dependencies;
f) the safety analysis, engineering and assessment processes to be applied during the life cycle, including processes for
   - ensuring an appropriate degree of personnel independence in tasks, commensurate with the risk of the system;
   - hazard identification and analysis;
   - risk assessment and on-going risk management;
   - risk tolerability criteria;
   - the establishment and on-going review of the adequacy of the safety requirements;
   - system design;
   - verification and validation;
   - safety assessment, to achieve compliance between system requirements and realisation;
   - safety audit, to achieve compliance of the management process with the Safety Plan;
   - safety assessment to achieve compliance between sub-system and system safety analysis;

g) la description détaillée de l'ensemble des éléments de sortie relatives à la sécurité issues du cycle de vie, y compris:
   – la documentation;
   – le matériel;
   – le logiciel;
h) le processus d'élaboration des Dossiers de Sécurité du système;
i) le processus d'approbation de la sécurité du système;
j) le processus d'approbation de la sécurité concernant les modifications du système;
k) le processus d'analyse des performances du système en situations d'exploitation et de maintenance afin de s'assurer de la conformité de sa sécurité aux exigences;
l) le processus de maintenance de la documentation relative à la sécurité, y compris le Registre des Situations Dangereuses;
m) les interfaces avec les autres programmes et les autres plans associés;
n) les contraintes et les hypothèses prises en compte dans le plan;
o) les dispositions relatives au management des sous-traitants;
p) les exigences relatives aux audits périodiques de sécurité, à l'évaluation de la sécurité et au suivi de la sécurité, pendant tout le cycle de vie, et en fonction de la nature plus ou moins sécuritaire du système considéré, y compris les éventuelles exigences relative à l'indépendance du personnel.

6.2.4 Eléments de sortie

6.2.4.1 Les résultats de la présente phase doivent être documentés et comprendre les hypothèses et justificatifs correspondants.

6.2.4.2 Les éléments de sortie doivent inclure la Politique de FDMS du système.

6.2.4.3 Les éléments de sortie doivent inclure le Plan de Sécurité du système.

6.2.4.4 Les éléments de sortie de la présente phase constituent un point d'entrée déterminant pour les phases suivantes du cycle de vie.

6.2.5 Vérification

6.2.5.1 Les tâches de vérification suivantes doivent être effectuées lors de la présente phase:

a) l'évaluation de la pertinence des informations et, le cas échéant, des données et des autres informations statistiques, utilisées comme éléments d'entrée pour les tâches de la présente phase;
b) la vérification des aspects de FDMS des éléments de sortie de la phase 2 par rapport aux éléments de sortie de la phase 1 et, notamment, l'évaluation de la conformité de la politique de FDMS aux exigences du système définies au cours de la phase 1;
c) l'évaluation de l'exhaustivité de l'analyse de FDM et de l'analyse des situations dangereuses;
d) l'évaluation de l'adéquation du Plan de Sécurité, y compris l'examen de l'adéquation de toutes les sources de données incluses dans le Plan de Sécurité;
e) l'évaluation de la pertinence des méthodes, des outils et des techniques utilisés au cours de la présente phase;
f) l'évaluation de la compétence de l'ensemble des personnes chargées d'effectuer des tâches au cours de la présente phase.

g) details of all safety related deliverables from the life cycle, including:
   – documentation;
   – hardware;
   – software;
h) a process to prepare system Safety Cases;
i) a process for the safety approval of the system;
j) a process for safety approval of system modifications;
k) a process for analysing operation and maintenance performance to ensure realised safety is compliant with requirements;
l) a process for the maintenance of safety-related documentation, including a Hazard Log;
m) interfaces with other related programmes and plans;
n) constraints and assumptions made in the plan;
o) subcontractor management arrangements.
p) requirements for periodic safety audit, safety assessment and safety review, throughout the life cycle and appropriate to the safety relevance of the system under consideration, including any personnel independence requirements.

6.2.4 Deliverables

6.2.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.2.4.2 The deliverables shall include the RAMS Policy for the system.

6.2.4.3 The deliverables shall include the Safety Plan for the system.

6.2.4.4 The deliverables from this phase form a key input to subsequent life cycle phases.

6.2.5 Verification

6.2.5.1 The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase;
b) RAMS aspects of the phase 2 deliverables shall be verified against the phase 1 deliverables, in particular, the RAMS Policy shall be assessed for compliance against the system requirements defined in phase 1;
c) the completeness of the RAM analysis and hazard identification process shall be assessed;
d) assessment of the adequacy of the Safety Plan, including a review of the adequacy of any data sources included within the Safety Plan;
e) assessment of the adequacy of the methods, tools and techniques used within the phase;
f) assessment of the competence of all personnel undertaking tasks within the phase.

6.2.5.2 D'éventuelles erreurs ou lacunes peuvent nécessiter la reprise de tout ou partie des activités d'une ou de plusieurs phases précédentes du cycle de vie.

6.3 Phase 3: Analyse de risque

NOTE Il peut être nécessaire de renouveler l'analyse de risque à plusieurs étapes du cycle de vie (voir le point d) de 6.3.1 ci-dessous).

6.3.1 Objectifs

Les objectifs de la présente phase sont

a) d'identifier les situations dangereuses associées au système;

b) d'identifier les événements donnant lieu à des situations dangereuses;

c) de déterminer le risque associé aux situations dangereuses;

d) d'établir un processus de management continu des risques.

6.3.2 Eléments d'entrée

Les éléments d'entrée de la présente phase doivent comporter toutes les informations pertinentes et, le cas échéant, les données nécessaires pour satisfaire aux exigences de la phase et, notamment, les éléments de sortie de la phase 2.

6.3.3 Exigences

6.3.3.1 L'exigence n° 1 de la présente phase doit être

a) d'identifier systématiquement, en les classant par ordre de priorité, l'ensemble des situations dangereuses raisonnablement prévisibles eu égard au système dans son environnement, y compris les situations dangereuses résultant
   - de l'exploitation normale du système;
   - des conditions de panne du système;
   - de l'exploitation du système en situation d'urgence;
   - de la mauvaise utilisation du système;
   - des interfaces du système;
   - des fonctions du système;
   - de l'exploitation et de la maintenance du système ainsi que de ses aspects logistiques;
   - des considérations relatives à la dépose du système;
   - des facteurs humains;
   - des aspects concernant l'hygiène et la sécurité du travail;
   - de l'environnement mécanique;
   - de l'environnement électrique;
   - des conditions naturelles d'environnement telles que la neige, les inondations, les tempêtes, la pluie, les glissements de terrain, etc.;

b) d'identifier les séquences d'événements conduisant à des situations dangereuses;

c) d'évaluer la fréquence d'occurrence de chaque situation dangereuse (voir tableau 2);

d) d'évaluer la gravité probable des conséquences de chaque situation dangereuse (voir tableau 3);

e) d'évaluer le risque de chaque situation dangereuse pour le système.

6.2.5.2 Any errors or shortfalls may require the re-application of some or all of the activities of one or more previous life cycle phases.

6.3 Phase 3: Risk analysis

NOTE Risk analysis may need to be repeated at several stages of the life cycle (see item d) of 6.3.1 below).

6.3.1 Objectives

The objectives of this phase are to

a) identify hazards associated with the system;
b) identify the events leading to the hazards;
c) determine the risk associated with the hazards;
d) establish a process for on-going risk management.

6.3.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirements of the phase and in particular, the deliverables produced in phase 2.

6.3.3 Requirements

6.3.3.1 Requirement 1 of this phase shall be to

a) systematically identify and prioritise all reasonably foreseeable hazards associated with the system in its application environment, including hazards arising from
   – system normal operation;
   – system fault conditions;
   – system emergency operation;
   – system misuse;
   – system interfaces;
   – system functionality;
   – system operation, maintenance and support issues;
   – system disposal considerations;
   – human factors;
   – occupational health issues;
   – mechanical environment;
   – electrical environment;
   – natural environment to cover such matters as snow, floods, storms, rain, landslides, etc.;
b) identify the sequence of events leading to hazards;
c) evaluate the frequency of occurrence of each hazard (see table 2);
d) evaluate the likely severity of the consequences of each hazard (see table 3);
e) evaluate the risk to the system for each hazard.

6.3.3.2 L'exigence n° 2 de la présente phase doit être de déterminer et de classer l'acceptabilité du risque associé à chaque situation dangereuse identifiée, compte tenu des éventuels conflits entre sécurité et disponibilité ainsi qu'entre sécurité et exigences de coût global du système.

6.3.3.3 L'exigence n° 3 de la présente phase doit être de constituer le Registre des Situations Dangereuses en tant qu'outil de base du management continu des risques. Le Registre des Situations Dangereuses doit être mis à jour, dès qu'intervient un changement affectant une situation dangereuse identifiée ou qu'une nouvelle situation dangereuse est identifiée, tout au long du cycle de vie. Le Registre des Situations Dangereuses doit comprendre une description détaillée

a) de l'objet et du but du Registre des Situations Dangereuses;
b) de chaque événement dangereux et des éléments qui y contribuent;
c) des conséquences probables et de la fréquence des événements associés à chaque situation dangereuse;
d) du risque de chaque situation dangereuse;
e) des critères d'acceptabilité du risque pour l'application considérée;
f) des mesures prises pour réduire les risques à un niveau acceptable ou éliminer le risque pour chaque événement dangereux;
g) du processus de réexamen de l'acceptabilité du risque;
h) du processus de réexamen de l'efficacité des mesures de réduction du risque;
i) du processus mis en œuvre pour rendre compte de manière continue des risques et des accidents;
j) du processus de gestion du Registre des Situations Dangereuses;
k) des limites des analyses effectuées;
l) des hypothèses admises pendant les analyses;
m) du degré de confiance, et de ses limites, accordé aux données utilisées pendant les analyses;
n) des méthodes, des outils et des techniques utilisés;
o) du personnel impliqué dans le processus et de ses compétences.

6.3.4 Eléments de sortie

6.3.4.1 Les résultats de la présente phase doivent être documentés et comprendre les hypothèses et justificatifs correspondants.

6.3.4.2 Les résultats de l'analyse de risque doivent être consignés dans le Registre des Situations Dangereuses.

6.3.4.3 Les éléments de sortie de la présente phase constituent un point d'entrée déterminant pour les phases suivantes du cycle de vie.

6.3.5 Vérification

6.3.5.1 Les tâches de vérification suivantes doivent être effectuées lors de la présente phase:

a) l'évaluation de la pertinence des informations et, le cas échéant, des données et des autres informations statistiques, utilisées comme éléments d'entrée pour les tâches de la présente phase;
b) les éléments de sortie de phase 3 doivent être vérifiés par rapport aux éléments de sortie de phase 2;
c) l'estimation de l'exhaustivité de l'évaluation du risque;

6.3.3.2 Requirement 2 of this phase shall be to determine and classify the acceptability of the risk associated with each identified hazard, having considered the risk in terms of any conflicts with availability and life cycle cost requirements of the system.

6.3.3.3 Requirement 3 of this phase shall be to establish a Hazard Log as the basis for on-going risk management. The Hazard Log shall be updated, whenever a change to any identified hazard occurs or a new hazard is identified, throughout the life cycle. The Hazard Log shall include details of

a) the aim and purpose of the Hazard Log;
b) each hazardous event and contributing components;
c) likely consequences and frequencies of the sequence of events associated with each hazard;
d) the risk of each hazard;
e) risk tolerability criteria for the application;
f) the measures taken to reduce risks to a tolerable level, or remove, the risk for each hazardous event;
g) a process to review risk tolerability;
h) a process to review the effectiveness of risk reduction measures;
i) a process for on-going risk and accident reporting;
j) a process for management of the Hazard Log;
k) the limits of any analysis carried out;
l) any assumptions made during the analysis;
m) any confidence limits applying to data used within the analysis;
n) the methods, tool and techniques used;
o) the personnel, and their competencies, involved in the process.

6.3.4 Deliverables

6.3.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.3.4.2 The results of the risk analysis shall be recorded within the Hazard Log.

6.3.4.3 The deliverables from this phase form a key input to subsequent life cycle phases.

6.3.5 Verification

6.3.5.1 The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase;
b) the phase 3 deliverables shall be verified against the phase 2 deliverables;
c) assessment of the completeness of the risk assessment;

d) l'évaluation du classement de l'acceptabilité du risque;

e) l'évaluation de l'adaptation du processus de consignation des situations dangereuses au système considéré;

f) l'évaluation de la pertinence des méthodes, des outils et des techniques utilisés au cours de la présente phase;

g) l'évaluation de la compétence de l'ensemble des personnes chargées d'effectuer des tâches au cours de la présente phase.

6.3.5.2 D'éventuelles erreurs ou lacunes peuvent nécessiter la reprise de tout ou partie des activités d'une ou de plusieurs phases précédentes du cycle de vie.

6.4 Phase 4: Exigences du système

6.4.1 Objectifs

Les objectifs de la présente phase sont

a) de spécifier, pour le système, les exigences globales de FDMS;

b) de spécifier, pour le système, les critères généraux de démonstration et d'acceptation de la FDMS;

c) d'établir le Programme de FDM pour conduire les tâches de FDM lors des phases suivantes du cycle de vie.

6.4.2 Eléments d'entrée

Les éléments d'entrée de la présente phase doivent comporter toutes les informations pertinentes et, le cas échéant, les données nécessaires pour satisfaire aux exigences de la phase et, notamment, les éléments de sortie des phases 2 et 3.

6.4.3 Exigences

6.4.3.1 L'exigence n° 1 de la présente phase doit être de spécifier (en référence à 6.2.3.1) les exigences globales de FDMS pour l'ensemble du système. Les exigences de FDMS pour le système considéré doivent comporter

– la définition du système et ses frontières;

– le profil de mission;

– les exigences relatives aux fonctions et à leurs performances, y compris les exigences fonctionnelles de sécurité et les exigences d'intégrité de la sécurité pour chaque fonction de sécurité;

– les exigences de soutien logistique;

– les interfaces;

– l'environnement de l'application considérée;

– les niveaux admissibles de risque pour les situations dangereuses identifiées;

– les mesures externes nécessaires pour satisfaire aux exigences;

– les exigences de soutien au système;

– la description détaillée des limites de l'analyse;

– la description détaillée de toutes les hypothèses prises en compte.

d) assessment of the risk acceptability classification;

e) assessment of the suitability of the Hazard Log process for the system under consideration;

f) assessment of the adequacy of the methods, tools and techniques used within the phase;

g) assessment of the competence of all personnel undertaking tasks within the phase.

6.3.5.2 Any errors or shortfall may require the re-application of some or all of the activities of one or more previous life cycle phases.

6.4 Phase 4: System requirements

6.4.1 Objectives

The objectives of this phase are to

a) specify the overall RAMS requirements for the system;

b) specify the overall demonstration and acceptance criteria for RAMS for the system;

c) establish the RAM Programme for controlling RAM tasks during subsequent life cycle phases.

6.4.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirements of the phase and in particular, the deliverables of phase 2 and phase 3.

6.4.3 Requirements

6.4.3.1 Requirement 1 of this phase shall be to specify (with reference to 6.2.3.1) the overall RAMS requirements for the total system. The RAMS requirements, for the system under consideration, shall include

– definition of the system and boundaries;

– mission profile;

– functional requirements and supporting performance requirements, including safety functional requirements and safety integrity requirements for each safety function;

– logistic support requirements;

– interfaces;

– application environment;

– tolerable risk levels for identified hazards;

– external measures necessary to achieve the requirements;

– system support requirements;

– details of the limits of the analysis;

– details of any assumptions made.

6.4.3.2 L'exigence n° 2 de la présente phase doit être de spécifier (en référence à 6.2.3.3) les exigences globales pour obtenir un système conforme aux exigences de FDMS, y compris:

– les critères d'acceptation pour les exigences globales de FDMS;

– le processus de démonstration et d'acceptation des exigences globales de FDMS que prévoit le plan de validation de la FDMS du système; il convient que ce plan comporte

- la description du système;
- les principes de validation de la FDMS à appliquer au système;
- les essais et les analyses de FDMS à effectuer pour la validation, y compris la description détaillée de l'environnement, des outils, des dispositifs et des autres éléments requis, etc.;
- l'organisation de la validation y compris les exigences relatives à l'indépendance du personnel;
- la description détaillée du programme de validation (séquence et planning);
- les procédures de traitement des non-conformités.

6.4.3.3 L'exigence n° 3 de la présente phase doit être d'établir le programme détaillé de FDM pour les tâches restantes du cycle de vie (en référence en 6.2.3.3). Le Programme de FDM doit comporter les tâches considérées comme les mieux à même de permettre de satisfaire aux exigences de FDM pour le système considéré. Le Programme de FDM doit être approuvé par la société d'exploitation ferroviaire et par les industries ferroviaires concernées et il doit être mis en œuvre tout au long du cycle de vie du système. Dans le Programme de FDM, il convient d'inclure les tâches suivantes:

a) le management, y compris la description détaillée des éléments suivants:
   – la politique et la stratégie relatives aux exigences de FDM;
   – le domaine d'application du programme;
   – la description du système;
   – le cycle de vie du système ainsi que les tâches et les processus de FDM à réaliser au cours du cycle de vie, notamment l'ordre des tâches de FDM permettant l'optimisation de la conception du système;
   – les fonctions, les responsabilités, la compétence et les relations des organismes chargés d'accomplir des tâches au cours du cycle de vie;
   – un Système de Signalement, d'Analyse et de Correction des Défaillances (SSACD) à mettre en œuvre pour le système à partir de la phase 7 du cycle de vie (par la société d'exploitation ferroviaire ou l'industrie ferroviaire, selon le cas), en enregistrant les éléments suivants:
     - les informations techniques relatives au système;
     - la motivation des actions de maintenance;
     - les types d'action de maintenance;
     - la durée des actions de maintenance calculée en heure et en homme/heure;
     - la durée d'immobilisation pour maintenance;
     - l'effectif et le niveau de qualification du personnel;
     - les pièces de rechange utilisées;
     - le coût des consommables;
     - les comptes rendus et les actions correctives;
   – les dispositions prises pour assurer la coordination des différentes composantes de la FDM;
   – la description détaillée de tous les éléments de sortie du cycle de vie, relatifs aux tâches de FDM;

6.4.3.2 Requirement 2 of this phase shall be to specify (with reference to 6.2.3.3) the overall requirements for achieving compliance with RAMS requirements for the system, including

– acceptance criteria for the overall RAMS requirements;
– demonstration and acceptance process for the overall RAMS requirements facilitated by the system RAMS validation plan, which should include
  - a description of the system;
  - the RAMS validation principles to be applied to the system;
  - the RAMS tests and analysis to be carried out for the validation including details of the required environment, tools, facilities etc.;
  - the validation management structure including requirements for personnel independence;
  - details of the validation programme (sequence and schedule);
  - procedures for dealing with non-compliance.

6.4.3.3 Requirement 3 of this phase shall be to establish the detailed RAM Programme for the remaining life cycle tasks (with reference to 6.2.3.3). The RAM Programme shall include the tasks which are judged to be the most effective to the attainment of the RAM requirements for the system under consideration. The RAM Programme shall be agreed by the Railway Authority and the railway support industry for the system under consideration and shall be implemented throughout the life cycle of the system. Within the RAM Programme, consideration should be given to including the following tasks:

a) management, including details of
  – the policy and strategy for achieving RAM requirements;
  – the scope of the programme;
  – a description of the system;
  – the system life cycle and RAM tasks and processes to be undertaken within the life cycle, specifically the order of RAM tasks to ensure maximum benefit to system design;
  – the roles, responsibilities, competencies and relationships of organisations undertaking tasks within the life cycle;
  – A Failure Reporting Analysis and Corrective Action System (FRACAS) to be applied to the system from phase 7 of the life cycle (by the Railway Authority and the railway support industry, as appropriate), with records including:
    - technical data on system;
    - reason for maintenance action;
    - type of maintenance action;
    - man-hours and elapsed time for maintenance action;
    - maintenance down time;
    - number and skill level of personnel;
    - spare parts used;
    - cost of consumables;
    - reporting and corrective action;
  – the arrangements to ensure co-ordination of individual RAM elements;
  – details of all RAM related deliverables from the life cycle;

- la description détaillée des tâches d'acceptation de la FDM;
- les interfaces avec les autres programmes et les autres plans associés;
- les contraintes et les hypothèses prises en compte dans le programme FDM;
- les dispositions relatives au management des sous-traitants;

b) la fiabilité, y compris:

- l'analyse prévisionnelle de la fiabilité, comprenant:
  - l'analyse fonctionnelle et la détermination des défaillances du système;
  - l'analyse déductive, par exemple l'analyse par arbre des causes ou par diagramme de fiabilité;
  - l'analyse inductive, par exemple l'Analyse des Modes de Défaillance et de leurs Effets (AMDE);
  - l'analyse des défaillances de mode commun ou l'analyse des défaillances multiples;
  - l'étude de sensibilité et les études de compromis;
  - l'allocation d'objectifs spécifiques de fiabilité;
  - l'analyse de l'interface homme-machine;
  - l'analyse des contraintes;
  - la prévision du «pire cas» et l'analyse de la tolérance;
- la programmation de la fiabilité, comprenant:
  - le programme de revue de la fiabilité en conception;
  - le plan d'assurance de la fiabilité des composants;
  - le plan d'assurance qualité/fiabilité du logiciel;
- les essais de fiabilité, comprenant:
  - les tests de croissance de la fiabilité, fondés sur l'introduction de défaillances dans le système;
  - les tests de démonstration de la fiabilité, fondés sur les modes de défaillances prévus;
  - les tests portant sur l'environnement;
  - les tests portant sur la durée de vie des composants;
  - les tests portant sur la durée de vie du système au début de son exploitation;
  - l'acquisition et l'évaluation des données de fiabilité;
  - l'analyse des données destinée à améliorer la fiabilité;

c) la maintenabilité, y compris:

- l'analyse prévisionnelle de la maintenabilité, comprenant:
  - l'analyse et la vérification de la maintenabilité;
  - l'analyse des tâches de maintenance;
  - les études et les essais portant sur la facilité des opérations de maintenance;
  - la prise en compte des facteurs humains dans la maintenabilité;
- la programmation de la maintenabilité, comprenant:
  - le programme de revue de la maintenabilité en conception;
  - la mise en œuvre de la politique de maintenance;
  - la revue des choix de maintenance fondés sur la fiabilité;
  - le programme de maintenance du logiciel;

- details of RAM acceptance tasks;
- interfaces with other related programmes and plans;
- constraints and assumptions made in the RAM programme;
- subcontractor management arrangements;

b) reliability, including:
   - reliability analysis and prediction, including:
     - functional analysis and system failure definition;
     - top down analysis, for example fault tree analysis and block diagram analysis;
     - bottom up analysis, for example Failure Modes Effects Analysis (FMEA);
     - common cause failure or multiple failure analysis;
     - sensitivity analysis and trade-off studies;
     - reliability apportionment;
     - human machine interface analysis;
     - stress analysis;
     - “worst case” prediction and tolerance analysis;
   - reliability planning, including:
     - reliability design review programme;
     - component reliability assurance programme;
     - software quality/reliability assurance programme;
   - reliability testing, including:
     - reliability growth testing, based on failure generation;
     - reliability demonstration testing, based on expected failure modes;
     - environmental stress screening;
     - life testing of components;
     - system life testing during early operation.
     - reliability data acquisition and assessment;
     - data analysis for reliability improvement;

c) maintainability, including:
   - maintainability analysis and prediction, including:
     - maintainability analysis and verification;
     - maintenance task analysis;
     - ease-of-maintenance studies and testing;
     - human factors maintainability considerations;
   - maintainability planning, including:
     - maintainability design review programme;
     - establishment of the maintenance strategy;
     - review of reliability centred maintenance options;
     - software maintenance programme;

- l'évaluation du soutien logistique, comprenant:
  - la définition des exigences de maintenance;
  - la définition de la politique de pièces de rechange et l'approvisionnement;
  - le personnel et les moyens de maintenance;
  - les mesures relatives à la sécurité du personnel;
  - les exigences de soutien au système;
  - les exigences du programme de formation;
  - les conditions de transport, de conditionnement, de manutention et de stockage du système;
- l'acquisition et l'évaluation des données de maintenabilité;
- l'analyse des données destinée à améliorer la maintenabilité;

d) la disponibilité, y compris:
- l'analyse prévisionnelle de la disponibilité;
- l'étude de sensibilité et les études de compromis;
- la démonstration de la disponibilité au début de l'exploitation;
- l'acquisition et l'évaluation des données de disponibilité;
- l'analyse prévisionnelle des données destinée à améliorer la disponibilité.

6.4.3.4 L'exigence n° 4 de la présente phase doit être de mettre à jour le Plan de Sécurité afin de s'assurer que l'ensemble des tâches prévues sont conformes aux exigences de FDMS concernant le système.

6.4.4 Eléments de sortie

6.4.4.1 Les résultats de la présente phase doivent être documentés et comprendre les hypothèses et justificatifs correspondants.

6.4.4.2 Le Plan de Sécurité et le Plan d'Acceptation doivent être mis à jour durant la présente phase.

6.4.4.3 Les éléments de sortie de la présente phase constituent un point d'entrée déterminant pour les phases suivantes du cycle de vie.

6.4.5 Vérification

6.4.5.1 Les tâches de vérification suivantes doivent être effectuées lors de la présente phase:

a) l'évaluation de la pertinence des informations et, le cas échéant, des données et des autres informations statistiques, utilisées comme éléments d'entrée pour les tâches de la présente phase;

b) la vérification de la conformité des exigences du système avec les éléments de sortie des phases 2 et 3, y compris l'évaluation du coût global;

c) la vérification de la conformité des exigences de sécurité avec les objectifs de sécurité et la politique de sécurité éventuels de la société d'exploitation ferroviaire;

d) la vérification de la conformité des exigences de FDM avec les éventuels objectifs et politiques de FDM de la société d'exploitation ferroviaire;

e) l'évaluation de la pertinence et de l'exhaustivité du Plan d'Acceptation et du Plan de Validation;

f) l'évaluation de la pertinence du Programme de FDM, y compris celle des sources de données utilisées;

- logistic support evaluation including:
  - definition of maintenance requirements;
  - definition of spares policy and support resource;
  - maintenance personnel and facilities;
  - personnel safety precautions;
  - system support requirements;
  - training programme requirements;
  - system transportation, packaging, handling and storage conditions;
- maintainability data acquisition and assessment;
- data analysis for maintainability improvement;

d) availability, including:
- availability analysis;
- sensitivity analysis and trade-off studies;
- availability demonstration during early operation;
- availability data acquisition and assessment;
- data analysis for availability improvement and prediction.

6.4.3.4 Requirement 4 of this phase shall be to amend the Safety Plan to ensure that all future planned tasks are consistent with the system's emergent RAMS requirements.

6.4.4 Deliverables

6.4.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.4.4.2 The phase shall produce an updated Safety Plan and Acceptance Plan.

6.4.4.3 The deliverables from this phase are an input to subsequent life cycle phases.

6.4.5 Verification

6.4.5.1 The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase;

b) system requirements shall be verified against the deliverables produced within phase 2 and phase 3, including life cycle costings;

c) safety requirements shall be verified against any safety targets and safety policies of the Railway Authority;

d) RAM requirements shall be verified against any RAM targets and RAM policies of the Railway Authority;

e) assessment of the adequacy and completeness of the Acceptance Plan and the Validation Plan;

f) assessment of the adequacy of the RAM Programme, including a review of the adequacy of any data sources used;

g) l'évaluation des méthodes, des outils et des techniques utilisés au cours de la présente phase;

h) l'évaluation de la compétence de l'ensemble des personnes chargées d'effectuer des tâches au cours de la présente phase.

6.4.5.2 D'éventuelles erreurs ou lacunes peuvent nécessiter la reprise de tout ou partie des activités d'une ou de plusieurs phases précédentes du cycle de vie.

6.5 Phase 5: Allocation des exigences du système

6.5.1 Objectifs

Les objectifs de la présente phase sont

a) d'allouer les exigences globales de FDMS du système aux sous-systèmes, aux composants et aux éléments externes;

b) de définir, en termes de FDMS, les critères d'acceptation des sous-systèmes, des composants et des éléments externes.

6.5.2 Eléments d'entrée

Les éléments d'entrée de la présente phase doivent comporter toutes les informations pertinentes et, le cas échéant, les données nécessaires pour satisfaire aux exigences de la phase et, notamment, l'ensemble des éléments de sortie de la phase 4.

6.5.3 Exigences

6.5.3.1 L'exigence n° 1 de la présente phase doit être

a) d'allouer des exigences fonctionnelles aux sous-systèmes, aux composants et aux éléments externes;

b) d'allouer des exigences de sécurité aux sous-systèmes, aux composants et aux dispositifs externes de réduction du risque;

c) de spécifier les sous-systèmes, les composants et les éléments externes pour satisfaire à la totalité des exigences de FDM du système, en prenant en compte l'impact des modes communs de défaillances et des défaillances multiples;

d) de réexaminer le programme de FDM.

6.5.3.2 L'exigence n° 2 de la présente phase doit être de spécifier les exigences nécessaires pour démontrer que les sous-systèmes, les composants et les éléments externes sont conformes à leurs propres exigences, y compris:

– les critères d'acceptation des exigences des sous-systèmes, des composants et des éléments externes;

– les processus et les procédures de démonstration et d'acceptation des exigences des sous-systèmes, des composants et des éléments externes.

6.5.3.3 L'exigence n° 3 de la présente phase doit être de réexaminer et de mettre à jour le Plan de Sécurité et le Plan de Validation afin de s'assurer qu'après allocation les tâches planifiées sont conformes aux exigences du système. Une attention toute particulière est apportée aux exigences relatives à l'indépendance du personnel ainsi qu'au contrôle des interfaces du système au niveau desquelles les fonctions de sécurité peuvent être compromises.

g) assessment of the methods, tools and techniques used within the phase;

h) competence assessment of personnel undertaking tasks within the phase.

6.4.5.2 Any errors or shortfall may require the re-application of some or all of the activities of one or more previous life cycle phases.

6.5 Phase 5: Apportionment of system requirements

6.5.1 Objectives

The objectives of this phase are to

a) apportion the overall RAMS requirements for the system to designated sub-systems, components and external facilities;

b) define the RAMS acceptance criteria for the designated sub-systems, components and external facilities.

6.5.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirements of the phase and in particular, all deliverables produced in phase 4.

6.5.3 Requirements

6.5.3.1 Requirement 1 of this phase shall be to

a) allocate functional requirements to designated sub-systems, components and external facilities;

b) allocate safety requirements to designated sub-systems, components and external risk reduction facilities;

c) specify the designated sub-systems, components and external facilities to achieve complete system RAM requirements, including the impact of common cause and multiple failures;

d) review the RAM programme.

6.5.3.2 Requirement 2 of this phase shall be to specify requirements for compliance with sub-system, component and external facilities requirements, including:

– acceptance criteria for sub-system, component and external facilities requirements;

– demonstration and acceptance processes and procedures for sub-system, component and external facilities requirements.

6.5.3.3 Requirement 3 of this phase shall be to review and update the Safety Plan and the Validation Plan to ensure that planned tasks are consistent with the requirements of the system following apportionment. Key areas of concern include requirements for personnel independence and the control of system interfaces where safety functionality may be compromised.

6.5.4 Eléments de sortie

6.5.4.1 Les résultats de la présente phase doivent être documentés et comprendre les hypothèses et justificatifs correspondants.

6.5.4.2 Le Plan de Sécurité doit être mis à jour durant la présente phase.

6.5.4.3 Les documents issus de la présente phase doivent comprendre les exigences du système allouées aux sous-systèmes, aux composants et aux installations externes.

6.5.4.4 Les éléments de sortie de la présente phase constituent un point d'entrée déterminant pour les phases suivantes du cycle de vie.

6.5.5 Vérification

6.5.5.1 Les tâches de vérification suivantes doivent être effectuées lors de la présente phase:

a) l'évaluation de la pertinence des informations et, le cas échéant, des données et des autres informations statistiques, utilisées comme éléments d'entrée pour les tâches de la présente phase;

b) la vérification de la conformité des exigences du système, des sous-systèmes, des composants et des éléments externes avec les éléments de sortie de la phase 4, ainsi que le réexamen des exigences eu égard au coût global du système;

c) la vérification de l'architecture de l'ensemble composé des sous-systèmes, des composants et des éléments externes afin de s'assurer qu'ils sont conformes aux exigences de FDMS applicables au système global;

d) la vérification des exigences de FDMS des sous-systèmes, des composants et des éléments externes afin de s'assurer de leur traçabilité au regard des exigences de FDMS du système;

e) la vérification des exigences de FDMS des sous-systèmes, des composants et des éléments externes afin de s'assurer qu'elles sont exhaustives et que les fonctions sont cohérentes entre elles;

f) la vérification de la mise à jour du Plan de Sécurité et du Plan de Validation pour s'assurer qu'ils demeurent applicables;

g) l'évaluation de la pertinence des méthodes, des outils et des techniques utilisés au cours de la présente phase;

h) l'évaluation de la compétence de l'ensemble des personnes chargées d'effectuer des tâches au cours de la présente phase.

6.5.5.2 D'éventuelles erreurs ou lacunes peuvent nécessiter la reprise de tout ou partie des activités d'une ou de plusieurs phases précédentes du cycle de vie.

6.6 Phase 6: Conception et réalisation

6.6.1 Objectifs

Les objectifs de la présente phase sont

a) de créer des sous-systèmes et des composants conformes aux exigences de FDMS;

b) de démontrer que les sous-systèmes et les composants sont conformes aux exigences de FDMS;

c) de planifier les tâches ultérieures du cycle de vie liées à la FDMS.

6.5.4 Deliverables

6.5.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.5.4.2 This phase shall produce an updated Safety Plan.

6.5.4.3 The documents resulting from this phase shall include the allocated system requirements to the designated sub-systems, components and external facilities.

6.5.4.4 The deliverables from this phase form a key input to subsequent life cycle phases.

6.5.5 Verification

6.5.5.1 The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase;

b) verification of system, sub-system, component and external facility requirements against the deliverables produced in phase 4, and including a review of the requirements against the life cycle cost for the system;

c) the architecture for the total combination of designated sub-systems, components and external facilities shall be verified to ensure it complies with the RAMS requirements for the total system;

d) the RAMS requirements for sub-system, component and external facilities shall be verified to ensure that they are traceable to the RAMS requirements for the system;

e) the RAMS requirements for sub-system, component and external facilities shall be verified to ensure completeness and consistency between functions;

f) the revised Safety Plan and Validation plan shall be verified to ensure its continued applicability;

g) assessment of the adequacy of the methods, tools and techniques used within the phase;

h) assessment of the competence of all personnel undertaking tasks within the phase.

6.5.5.2 Any errors or shortfall may require the re-application of some or all of the activities of one or more previous life cycle phases.

6.6 Phase 6: Design and implementation

6.6.1 Objectives

The objectives of this phase are to

a) create sub-systems and components conforming to RAMS requirements;

b) demonstrate sub-systems and components conform to RAMS requirements;

c) establish plans for future life cycle tasks involving RAMS.

6.6.2 Eléments d'entrée

Les éléments d'entrée de la présente phase doivent comporter toutes les informations pertinentes et, le cas échéant, les données nécessaires pour satisfaire aux exigences de la phase et, notamment, l'ensemble des éléments de sortie des phases 4 et 5.

6.6.3 Exigences

6.6.3.1 L'exigence n° 1 de la présente phase doit être de concevoir les sous-systèmes et composants de manière à satisfaire aux exigences de FDMS.

6.6.3.2 L'exigence n° 2 de la présente phase doit être de réaliser les sous-systèmes et les composants de manière à satisfaire aux exigences de FDMS.

6.6.3.3 L'exigence n° 3 de la présente phase doit être d'établir, en termes de FDMS, des plans, concernant les tâches ultérieures du cycle de vie, y compris:

– l'installation;
– la mise en état de fonctionnement;
– l'exploitation et la maintenance, y compris la définition des procédures d'exploitation et de maintenance;
– l'acquisition et l'évaluation des données en cours d'exploitation.

6.6.3.4 L'exigence n° 4 de la présente phase doit être de définir, de vérifier et de mettre en œuvre un processus de fabrication capable de produire des sous-systèmes et des composants conformes en termes de FDMS, en tenant compte

– des essais d'environnement;
– des essais d'amélioration de la FDM;
– des contrôles et des essais résultant des modes de panne liés à la FDMS;
– de la mise en œuvre du Plan de Sécurité (point d) de 6.2.3.4).

6.6.3.5 L'exigence n° 5 de la présente phase doit être

a) d'élaborer le Dossier de Sécurité Générique du système, permettant de justifier la conformité du système aux exigences de sécurité, du point de vue de sa conception et indépendamment de son application. Ce Dossier de Sécurité doit être approuvé par la société d'exploitation ferroviaire et il est recommandé qu'il comprenne
   – une présentation globale du système;
   – un résumé des exigences de sécurité ou la référence à ces exigences, y compris la présentation de la justification du SIL retenu pour les fonctions de sécurité;
   – un résumé des contrôles relatifs au management de la qualité et de la sécurité adoptés au cours du cycle de vie;
   – un résumé de l'évaluation de la sécurité et des tâches d'audit de sécurité;
   – un résumé des tâches d'analyse de sécurité;
   – une vue d'ensemble des techniques de sécurité utilisées dans le système;
   – la vérification du processus de fabrication;
   – la justification de la conformité aux exigences de sécurité, y compris la conformité aux exigences du système en termes de SIL;
   – un résumé des éventuelles limites et contraintes applicables au système;
   – tout écart (ou spécificité) justifié par rapport aux exigences de cette norme, imposé par le contrat;

6.6.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirement, and in particular the deliverables produced in phase 4 and phase 5.

6.6.3 Requirements

6.6.3.1 Requirement 1 of this phase shall be to design the sub-systems and components to meet RAMS requirements.

6.6.3.2 Requirement 2 of this phase shall be to realise the design of the sub-systems and components to meet RAMS requirements.

6.6.3.3 Requirement 3 of this phase shall be to establish plans, in the context of RAMS, for future life cycle tasks, including:

– installation;
– commissioning;
– operation and maintenance, including definition of operation and maintenance procedures;
– data acquisition and assessment during operation.

6.6.3.4 Requirement 4 of this phase shall be to define, verify and establish a manufacturing process capable of producing RAMS-validated sub-systems and components, giving consideration to the use of

– environmental stress screening;
– RAM improvement testing;
– inspection and testing for RAMS-related failure modes;
– implementation of requirement 4 of the Safety Plan (item d) of 6.2.3.4).

6.6.3.5 Requirement 5 of this phase shall be to

a) prepare a Generic Safety Case for the system, justifying that the system, as designed and independent of application, meets safety requirements. The Safety Case requires approval by the Railway Authority, and should include
   – an overview of the system;
   – a summary or reference to the safety requirements, including a consideration of the SIL justifications for safety functions;
   – a summary of the quality and safety management controls adopted within the life cycle;
   – a summary of safety assessment and safety audit tasks;
   – a summary of safety analysis tasks;
   – an overview of the safety engineering techniques employed within the system
   – verification of the manufacturing process;
   – adequacy of compliance with safety requirements, including any SIL requirements of the system;
   – a summary of any limitations and constraints applying to the system;
   – any special exemption (or specificity) imposed and justified by the contract, to the usual requirements of this standard;

b) d'élaborer, le cas échéant dès cette étape, le Dossier de Sécurité de l'Application. Le Dossier de Sécurité de l'Application se construit sur la base du Dossier de Sécurité Générique en démontrant que la conception du système et sa réalisation concrète, y compris au cours des phases d'installation et d'essais, satisfont aux exigences de sécurité pour une application spécifique. Le Dossier de Sécurité de l'Application doit être approuvé par la société d'exploitation ferroviaire et il est recommandé qu'il comprenne

   – l'ensemble des informations supplémentaires nécessaires pour justifier la sécurité de l'application considérée;

   – toutes les limites ou contraintes particulières à l'application du système.

6.6.4 Eléments de sortie

6.6.4.1 Les résultats de la présente phase doivent être documentés et comprendre les hypothèses et justificatifs correspondants.

6.6.4.2 Toutes les tâches de validation de la FDMS entreprises au cours de la phase doivent être consignées.

6.6.4.3 Les plans détaillés concernant les tâches ultérieures du cycle de vie, en termes de FDMS, doivent être établis.

6.6.4.4 Les procédures d'exploitation et de maintenance comportant toutes les informations pertinentes relatives à la fourniture de pièces de rechange, notamment celles qui sont liées à la sécurité, doivent être rédigées au cours de la présente phase.

6.6.4.5 Le Dossier de Sécurité Générique doit être établi au cours de la présente phase.

6.6.4.6 Le Dossier de Sécurité de l'Application peut être établi au cours de la présente phase.

6.6.4.7 Les éléments de sortie de la présente phase constituent un point d'entrée déterminant pour les phases suivantes du cycle de vie.

6.6.5 Vérification

6.6.5.1 Les tâches de vérification suivantes doivent être effectuées lors de la présente phase:

a) l'évaluation de la pertinence des informations et, le cas échéant, des données et des autres informations statistiques, utilisées comme éléments d'entrée pour les tâches de la présente phase;

b) la vérification, au moyen d'analyses et de tests, de la conformité de la conception des sous-systèmes et des composants aux exigences de FDMS;

c) la vérification, au moyen d'analyses et de tests, de la conformité de la réalisation des sous-systèmes et des composants à leur conception;

d) la validation de la réalisation des sous-systèmes et des composants pour s'assurer que celle-ci est conforme aux critères d'acceptation de la FDMS pour les sous-systèmes et les composants, y compris aux exigences du cycle de vie;

e) la vérification, au moyen d'analyses et de tests, que le processus de fabrication permet de produire des sous-systèmes et des composants validés en termes de FDMS;

f) la vérification que l'ensemble des plans concernant les activités ultérieures du cycle de vie sont conformes aux exigences de FDMS, y compris aux exigences de coût global;

g) l'évaluation de la pertinence et de l'exhaustivité du Dossier de Sécurité Générique et, le cas échéant, du Dossier de Sécurité de l'Application;

h) l'évaluation de la pertinence des méthodes, des outils et des techniques utilisés au cours de la présente phase;

b) prepare an Application Safety Case, if appropriate at this stage, for the system. The Application Safety Case builds on the Generic Safety Case, justifying that the design of the system and its physical realisation, including installation and test phases, for a specific class of application, meet safety requirements. The Application Safety Case requires approval by the Railway Authority, and should include

   – all additional information necessary to justify system safety for the class of application under consideration;

   – any limitations or constraints relevant to the application of the system.

6.6.4 Deliverables

6.6.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.6.4.2 A record of all RAMS validation tasks undertaken within the phase shall be maintained.

6.6.4.3 Detailed plans for future life cycle tasks, in the context of RAMS, shall be produced.

6.6.4.4 Operation and Maintenance Procedures including all the relevant information for providing spare parts, particularly safety related items, shall be produced within this phase.

6.6.4.5 A Generic Safety Case shall be produced within this phase.

6.6.4.6 An Application Safety Case may be produced within this phase.

6.6.4.7 The deliverables from this phase form a key input to subsequent life cycle phases.

6.6.5 Verification

6.6.5.1 The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase;

b) verification, by analysis and test, that sub-system and component design complies with the RAMS requirements;

c) verification, by analysis and test, that sub-systems and components realisation complies with designs;

d) validation of sub-system and component realisation to ensure that the realisation complies with RAMS acceptance criteria for sub-system and components, including life cycle requirements;

e) verification, by analysis and test, that the manufacturing arrangements produce RAMS-validated sub-systems and components;

f) verification that all future life cycle activity plans are consistent with RAMS requirements for the system, including life cycle cost requirements;

g) assessment of the adequacy and completeness of the generic safety case and where appropriate, the application safety case;

h) assessment of the adequacy of the methods, tools and techniques used within the phase;

i) l'évaluation de la compétence de l'ensemble des personnes chargées d'effectuer des tâches au cours de la présente phase;

j) la vérification que le Plan de Validation de la FDMS demeure applicable.

6.6.5.2 D'éventuelles erreurs ou lacunes peuvent nécessiter la reprise de tout ou partie des activités d'une ou de plusieurs phases précédentes du cycle de vie.

6.7 Phase 7: Fabrication

6.7.1 Objectifs

Les objectifs de la présente phase sont

a) de mettre en œuvre un processus de fabrication de sous-systèmes et de composants validés en termes de FDMS;

b) de mettre en place, pour le processus, un dispositif d'assurance fondé sur la FDMS;

c) de mettre en place un dispositif de soutien des sous-systèmes et des composants en termes de FDMS.

6.7.2 Eléments d'entrée

Les éléments d'entrée de la présente phase doivent comporter toutes les informations pertinentes et, le cas échéant, les données nécessaires pour satisfaire aux exigences de la phase et, notamment, les éléments de sortie de la phase 6 relatifs à la conception.

6.7.3 Exigences

6.7.3.1 L'exigence n° 1 de la présente phase doit être de vérifier et de mettre en œuvre le processus de fabrication.

6.7.3.2 L'exigence n° 2 de la présente phase doit être de mettre en place un dispositif de soutien des sous-systèmes et des composants, y compris:

– la préparation, la vérification et la validation de la documentation des sous-systèmes et des composants relative à la FDMS;

– la préparation, la vérification et la validation des procédures d'exploitation et de maintenance en termes de FDMS;

– la préparation, la vérification et la validation du dispositif de formation pour les sous-systèmes et les composants en termes de FDMS.

La documentation, les procédures et le dispositif de formation indiqués ci-dessus doivent être tenus à jour au cours de toutes les phases suivantes.

6.7.3.3 L'exigence n° 3 de la présente phase est, le cas échéant

a) de planifier la fabrication pour satisfaire aux exigences;

b) de mettre en oeuvre la fabrication pour satisfaire aux exigences;

c) de mettre en place, pour le processus, un dispositif d'assurance en termes de FDMS, destiné à éviter les modes de défaillances potentiels liés à la FDMS.

6.7.4 Eléments de sortie

6.7.4.1 Les résultats de la présente phase doivent être documentés et comprendre les hypothèses et justificatifs correspondants.

6.7.4.2 Toutes les tâches de validation FDMS entreprises au cours de la présente phase doivent être consignées.

i) assessment of the competence of all personnel undertaking tasks within the phase;

j) ensure the continued applicability of the RAMS validation plan.

6.6.5.2 Any errors or shortfalls may require the re-application of some or all of the activities of one or more previous life cycle phases.

6.7 Phase 7: Manufacturing

6.7.1 Objectives

The objectives of this phase are to

a) implement a manufacturing process which produces RAMS-validated sub-systems and components;

b) establish RAMS-centred process assurance arrangements;

c) establish sub-system and component RAMS support arrangements.

6.7.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirement, and in particular the design deliverables produced in phase 6.

6.7.3 Requirements

6.7.3.1 Requirement 1 of this phase shall be to verify and implement the manufacturing process.

6.7.3.2 Requirement 2 of this phase shall be to establish sub-system and component support arrangements, including:

– preparation, verification and validation of sub-system and component RAMS support documentation;

– preparation, verification and validation of operation and maintenance procedures in the context of RAMS;

– preparation, verification and validation of sub-system and component training material in the context of RAMS.

The above documentation, procedures and training material shall be reviewed in all subsequent phases.

6.7.3.3 Requirement 3 of this phase may, if appropriate, be to

a) plan manufacturing to meet requirements;

b) implement manufacturing to meet requirements;

c) implement RAMS process assurance to avoid potential RAMS-related failure modes.

6.7.4 Deliverables

6.7.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.7.4.2 A record of all RAMS validation tasks undertaken within the phase shall be maintained.

6.7.4.3 Les éléments de sortie de la présente phase constituent un point d'entrée déterminant pour les phases suivantes du cycle de vie.

6.7.5 Vérification

6.7.5.1 Les tâches de vérification suivantes doivent être effectuées dans le cadre de la présente phase:

a) l'évaluation de la pertinence des informations et, le cas échéant, des données et des autres informations statistiques, utilisées comme éléments d'entrée pour les tâches de la présente phase;

b) la vérification de la documentation de la FDMS pour s'assurer qu'elle est correcte, pertinente et conforme aux exigences de coût global ainsi qu'aux objectifs de FDMS définis pour le système;

c) une évaluation pour s'assurer que les produits fabriqués satisfont aux exigences du système;

d) l'évaluation de la pertinence des méthodes, des outils et des techniques utilisés au cours de la présente phase;

e) l'évaluation de la compétence de l'ensemble des personnes chargées d'effectuer des tâches au cours de la présente phase.

6.7.5.2 D'éventuelles erreurs ou lacunes peuvent nécessiter la reprise de tout ou partie des activités d'une ou de plusieurs phases précédentes du cycle de vie.

6.8 Phase 8: Installation

6.8.1 Objectifs

Les objectifs de la présente phase sont

a) d'assembler et d'installer l'ensemble des sous-systèmes et des composants constitutifs du système global;

b) d'amorcer la logistique du système.

6.8.2 Eléments d'entrée

Les éléments d'entrée de la présente phase doivent comporter toutes les informations pertinentes et, le cas échéant, les données nécessaires pour satisfaire aux exigences de la phase et, notamment, le Plan d'Installation préparé lors de la phase 6, les sous-systèmes et les composants fabriqués lors de la phase 7 ainsi que la documentation de la FDMS préparée lors de la phase 7.

6.8.3 Exigences

6.8.3.1 L'exigence n° 1 de la présente phase doit être d'assembler et d'installer l'ensemble des sous-systèmes, des composants et des éléments externes constitutifs du système global conformément au Plan d'Installation.

6.8.3.2 L'exigence n° 2 de la présente phase doit être de documenter le processus d'installation, y compris:

– la mise à jour des plans conformément à l'exigence n° 3 de la phase de conception et de réalisation (6.6.3.3);

– les tâches d'installation;

– les actions entreprises pour résoudre les problèmes de défaillances et d'incompatibilités.

6.7.4.3 The deliverables from this phase form a key input to subsequent life cycle phases.

6.7.5 Verification

6.7.5.1 The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase;

b) verification that RAMS support documentation is correct, adequate and consistent with life cycle cost requirements and any target RAMS requirements defined for the system;

c) assessment to ensure that the products being produced manufactured comply with system requirements;

d) assessment of the adequacy of the methods, tools and techniques used within the phase;

e) assessment of the competence of all personnel undertaking tasks within the phase.

6.7.5.2 Any errors or shortfalls may require the re-application of some or all of the activities of one or more previous life cycle phases.

6.8 Phase 8: Installation

6.8.1 Objectives

The objectives of this phase are to

a) assemble and install the total combination of sub-systems and components required to form the complete system;

b) initiate system support arrangements.

6.8.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirement, and in particular the Installation Plan prepared in phase 6, the sub-systems and components manufactured in phase 7 and the RAMS support documentation prepared in phase 7.

6.8.3 Requirements

6.8.3.1 Requirement 1 of this phase shall be to assemble and install the total combination of sub-systems, components and external facilities required to form the complete system, according to the Installation Plan.

6.8.3.2 Requirement 2 of this phase shall be to document the installation process, including:

– review plans in the context of requirement 3 of the design and implementation phase (6.6.3.3);

– installation tasks;

– action taken to resolve failures and incompatibilities.

6.8.3.3 L'exigence n° 3 de la présente phase doit être de mettre à jour le Plan de Sécurité, une fois l'installation achevée, pour s'assurer que les éventuelles modifications apportées au système ou aux procédures sont consignées et seront effectivement prises en compte lors des tâches ultérieures du cycle de vie.

6.8.3.4 L'exigence n° 4 de la présente phase doit être

a) de débuter la formation du personnel;

b) de mettre à disposition les procédures de soutien logistique;

c) d'assurer l'approvisionnement en pièces de rechange;

d) d'assurer la fourniture de l'outillage.

6.8.4 Eléments de sortie

6.8.4.1 Les résultats de la présente phase doivent être documentés et comprendre les hypothèses et justificatifs correspondants.

6.8.4.2 Toutes les tâches de validation de la FDMS entreprises au cours de la présente phase, y compris les tâches d'installation, doivent être consignées.

6.8.4.3 Le Plan de Sécurité doit être mis à jour au cours de la présente phase.

6.8.4.4 Les éléments de sortie de la présente phase constituent un point d'entrée déterminant pour les phases suivantes du cycle de vie.

6.8.5 Vérification

6.8.5.1 Les tâches de vérification suivantes doivent être effectuées dans le cadre de la présente phase:

a) l'évaluation de la pertinence des informations et, le cas échéant, des données et des autres informations statistiques, utilisées comme éléments d'entrée pour les tâches de la présente phase;

b) la vérification de la réalisation des tâches d'installation conformément au Plan d'Installation;

c) la vérification, au moyen d'analyses et de tests, de la conformité du système installé aux exigences de FDMS;

d) l'évaluation du plan de sécurité pour s'assurer qu'il demeure applicable;

e) l'évaluation de la pertinence et de l'efficacité du dispositif de soutien logistique;

f) l'évaluation de la pertinence des méthodes, des outils et des techniques utilisés au cours de la présente phase;

g) l'évaluation de la compétence de l'ensemble des personnes chargées d'effectuer des tâches au cours de la présente phase.

6.8.5.2 D'éventuelles erreurs ou lacunes peuvent nécessiter la reprise de tout ou partie des activités d'une ou de plusieurs phases précédentes du cycle de vie.

6.8.3.3 Requirement 3 of this phase shall be to review and update the Safety Plan following completion of installation to ensure that any changes to either system or procedures are recorded and effectively managed in future life cycle tasks.

6.8.3.4 Requirement 4 of this phase shall be to

a) start staff training;

b) make support procedures available;

c) establish spare parts provision;

d) establish tool provision.

6.8.4 Deliverables

6.8.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.8.4.2 A record of all RAMS validation tasks undertaken within the phase, including the installation activity, shall be maintained.

6.8.4.3 An updated Safety Plan shall be produced within this phase.

6.8.4.4 The deliverables from this phase form a key input to subsequent life cycle phases.

6.8.5 Verification

6.8.5.1 The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase;

b) verification that the installation activity was carried out in accordance with the Installation Plan;

c) verification, by analysis and test, that the installed system meets the RAMS requirements;

d) assessment of the Safety Plan to ensure its continued applicability;

e) assessment of the adequacy and effectiveness of system support arrangements;

f) assessment of the adequacy of the methods, tools and techniques used within the phase;

g) assessment of the competence of all personnel undertaking tasks within the phase.

6.8.5.2 Any errors or shortfalls may require the re-application of some or all of the activities of one or more previous life cycle phases.

6.9 Phase 9: Validation du système (y compris l'acceptation de la sécurité et la mise en état de fonctionnement)

6.9.1 Objectifs

6.9.1.1 Les objectifs de la présente phase sont

a) de valider le fait que, pour le système, l'ensemble combiné des sous-systèmes, des composants et des dispositifs externes de réduction du risque est conforme aux exigences de FDMS;

b) de mettre en état de fonctionnement l'ensemble combiné des sous-systèmes, des composants et des dispositifs externes de réduction du risque;

c) de préparer, et le cas échéant d'accepter, le Dossier de Sécurité de l'Application;

d) de procéder à l'acquisition et à l'évaluation des données.

6.9.1.2 Il est important de noter que les exigences de la phase 10, Acceptation du Système, peuvent être intégrées à celles de la présente phase 9, eu égard au système considéré. Dans ce cas, les éléments de sortie de la présente phase doivent démontrer que les exigences de la phase 10 ont été satisfaites lors de la réalisation de la phase 9.

6.9.2 Eléments d'entrée

Les éléments d'entrée de la présente phase doivent comporter toutes les informations pertinentes et, le cas échéant, les données nécessaires pour satisfaire aux exigences de la phase et, notamment, les exigences du système définies lors de la phase 4, le Plan de Vérification et de Validation élaboré lors de la phase 4, le Plan de Mise en état de fonctionnement élaboré lors de la phase 6 et les supports de formation préparés lors de la phase 7.

6.9.3 Exigences

6.9.3.1 L'exigence n° 1 de la présente phase doit être de valider l'ensemble combiné des sous-systèmes, des composants et des dispositifs externes de réduction du risque conformément au Plan de Validation et d'assurer la traçabilité du processus de validation, qui comporte notamment:

– la description détaillée des tâches de validation de la FDMS, en regard des critères d'acceptation, comportant les études de FDM et les analyses de sécurité;

– la description détaillée des processus, des méthodes et des outils utilisés pour les tâches de validation, en regard des critères d'acceptation;

– le résultat des tâches de validation de l'ensemble des critères d'acceptation;

– les éventuelles limites et contraintes applicables au système;

– les actions entreprises pour résoudre les problèmes de défaillances et d'incompatibilités.

6.9.3.2 L'exigence n° 2 de la présente phase doit être

a) de mettre en état de fonctionnement l'ensemble combiné des sous-systèmes, des composants et des dispositifs externes de réduction du risque, conformément au Plan de Mise en état de fonctionnement et d'assurer la traçabilité du processus de mise en état de fonctionnement, qui comporte notamment:

   – les tâches de mise en état de fonctionnement;

   – les tâches de signalement et d'évaluation des défaillances;

   – les actions entreprises pour résoudre les problèmes de défaillances et d'incompatibilités;

   – une description détaillée des éventuelles limites ou contraintes d'utilisation du système;

6.9 Phase 9: System validation (including safety acceptance and commissioning)

6.9.1 Objectives

6.9.1.1 The objectives of this phase are to

a) validate that the total combination of sub-systems, components and external risk reduction measures comply with the RAMS requirements for the system;

b) commission the total combination of sub-systems, components and external risk reduction measures;

c) prepare, and if appropriate accept, the Application Specific Safety Case for the system;

d) provide for data acquisition and assessment.

6.9.1.2 It is important to note that the requirements of phase 10, System Acceptance, may be integrated with the requirements of this phase, phase 9, if appropriate to the system under consideration. If this is the case, then the deliverables from this Phase shall demonstrate that the requirements of phase 10 have been adequately fulfilled in the realisation of phase 9.

6.9.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirement, and in particular the system requirements produced in phase 4, the Verification and Validation Plan produced in phase 4, the Commissioning Plan produced in phase 6 and the training material prepared in phase 7.

6.9.3 Requirements

6.9.3.1 Requirement 1 of this phase shall be to validate the total combination of sub-systems, components and external risk reduction measures according to the Validation Plan and record the validation process, including:

– details of RAMS validation tasks against acceptance criteria, including RAM demonstrations and safety analysis;

– details of process, tools, equipment used for validation tasks against acceptance criteria;

– results of validation tasks for all acceptance criteria;

– any limitations and constraints applying to the system;

– action taken to resolve failures and incompatibilities.

6.9.3.2 Requirement 2 of this phase shall be to

a) commission the total combination of sub-systems, components and external risk reduction measures according to the Commissioning Plan and record the commissioning process, including:

   – commissioning tasks;

   – failure reporting and assessment tasks;

   – action taken to resolve failures and incompatibilities;

   – details of any limitations or constraints on the use of the system;

b) d'exploiter, si nécessaire, le système pendant une période probatoire pour permettre de résoudre les problèmes rencontrés en service. Lorsque l'acceptation du système implique l'utilisation d'une période probatoire d'exploitation, on doit prendre en compte la nécessité de démontrer la sécurité de ce système avant qu'il soit exploité en service commercial.

6.9.3.3 L'exigence n° 3 de la présente phase doit être, si cela n'a pas déjà été effectué au cours de la phase 6 (point b) de 6.6.3.5), de préparer le Dossier de Sécurité de l'Application, afin de démontrer que, pour cette application, la mise en œuvre du système est conforme aux exigences de sécurité. Le Dossier de Sécurité de l'Application doit être approuvé par la société d'exploitation ferroviaire et il convient d'y inclure

– une présentation globale du système;
– un résumé des exigences de sécurité ou la référence à ces exigences, y compris la présentation de la justification du SIL retenu pour les fonctions de sécurité dans le cadre de l'application;
– un résumé des contrôles relatifs au management de la qualité et de la sécurité adoptés au cours du cycle de vie;
– un résumé de l'évaluation de la sécurité et des tâches d'audit de sécurité;
– un résumé des tâches d'analyse de sécurité;
– une vue d'ensemble des techniques de sécurité utilisées dans le système;
– la justification de la conformité du système aux exigences de sécurité, y compris en termes de SIL, ainsi que la justification de la conformité de sa réalisation concrète pour cette application;
– un résumé des éventuelles limites et contraintes relatives à l'application.

6.9.3.4 L'exigence n° 4 de la présente phase doit être de mettre au point et de mettre en œuvre un processus d'acquisition et d'évaluation des données opérationnelles à titre de source d'un processus d'amélioration du système.

6.9.4 Eléments de sortie

6.9.4.1 Les résultats de la présente phase doivent être documentés et comprendre les hypothèses et justificatifs correspondants.

6.9.4.2 Toutes les tâches de validation de la FDMS entreprises au cours de la phase, y compris les tâches de mise en état de fonctionnement, doivent être consignées.

6.9.4.3 Le Dossier de Sécurité de l'Application doit être élaboré au cours de la présente phase.

6.9.4.4 Toutes les tâches d'acceptation entreprises au cours de la présente phase doivent être consignées.

6.9.4.5 Les éléments de sortie de la présente phase constituent un point d'entrée déterminant pour les phases suivantes du cycle de vie.

6.9.5 Vérification

6.9.5.1 Les tâches suivantes de vérification du processus doivent être effectuées dans le cadre de la présente phase:

a) l'évaluation de la pertinence des informations et, le cas échéant, des données et des autres informations statistiques, utilisées comme éléments d'entrée pour les tâches de la présente phase;

b) undertake probationary period of operation, if required, to enable the resolution of in-service system problems. Where use is made of a probationary period of operation as part of system acceptance, consideration shall be given to the need for system safety to be demonstrated prior to operation of the system in revenue earning service.

6.9.3.3 Requirement 3 of this phase shall be to prepare an Application Safety Case for the system, if not already prepared in phase 6 (item b) of 6.6.3.5), to justify that the system, as specifically applied within this application, complies with the system safety requirements. The Application Safety Case requires approval by the Railway Authority, and should include

– an overview of the system;

– a summary or reference to the safety requirements, including a consideration of the SIL justifications for safety functions within the application;

– a summary of the quality and safety management controls adopted within the life cycle;

– a summary of safety assessment and safety audit tasks;

– a summary of safety analysis tasks;

– an overview of the safety engineering techniques employed within the system;

– adequacy of compliance with safety requirements for the system, including adequacy of compliance with the SIL requirements of the application including its physical realisation within the specific application;

– a summary of any limitations and constraints applying to the application.

6.9.3.4 Requirement 4 of this phase shall be to establish and implement a process for the acquisition and assessment of operational data as an input to a system improvement process.

6.9.4 Deliverables

6.9.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.9.4.2 A record of all RAMS validation tasks undertaken within the phase, including the commissioning activity, shall be maintained.

6.9.4.3 An Application Specific Safety Case shall be produced for the system within this phase.

6.9.4.4 A record of all Acceptance Tasks undertaken within this phase shall be maintained.

6.9.4.5 The deliverables from this phase form a key input to subsequent life cycle phases.

6.9.5 Verification

6.9.5.1 The following process verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase;

b) la vérification et la validation, au moyen d'analyses et de tests, de la conformité du système installé aux exigences de FDMS. Il convient de noter que pour certains systèmes ferroviaires, l'acceptation du Dossier de Sécurité de l'Application est exigée avant les activités d'installation et de mise en état de fonctionnement;

c) la vérification de la réalisation de l'activité de mise en état de fonctionnement conformément au Plan de Mise en état de fonctionnement;

d) l'évaluation de la pertinence et de l'efficacité du système de recueil des données opérationnelles;

e) l'évaluation de la pertinence des méthodes, des outils et des techniques utilisés au cours de la présente phase;

f) l'évaluation de la compétence de l'ensemble des personnes chargées d'effectuer des tâches au cours de la présente phase.

6.9.5.2 D'éventuelles erreurs ou lacunes peuvent nécessiter la reprise de tout ou partie des activités d'une ou de plusieurs phases précédentes du cycle de vie.

6.10 Phase 10: Acceptation du système

6.10.1 Objectifs

Les objectifs de la présente phase sont

a) d'évaluer la conformité de l'ensemble combiné des sous-systèmes, des composants et des dispositifs externes de réduction du risque aux exigences globales de FDMS du système;

b) d'accepter l'entrée en service du système.

6.10.2 Eléments d'entrée

Les éléments d'entrée de la présente phase doivent comporter toutes les informations pertinentes et, le cas échéant, les données nécessaires pour satisfaire aux exigences de la phase et, notamment, les exigences système élaborées lors de la phase 4, le Plan de Vérification et de Validation et le Plan d'Acceptation élaborés lors de la phase 4 ainsi que la traçabilité des tâches de vérification et de validation assurée lors de la phase 9.

6.10.3 Exigences

6.10.3.1 L'exigence n° 1 de la présente phase doit être d'évaluer l'ensemble des tâches de vérification et de validation du système, notamment la vérification et la validation de la FDM ainsi que le Dossier de Sécurité de l'Application conformément au Plan d'Acceptation du système.

6.10.3.2 L'exigence n° 2 de la présente phase doit être, le cas échéant, l'acceptation formelle de l'entrée en service du système.

6.10.3.3 L'exigence n° 3 de la présente phase doit être de mettre à jour le Registre des Situations Dangereuses afin de consigner toute situation dangereuse résiduelle identifiée lors de la validation et de l'acceptation du système, et de s'assurer que les risques résultant d'une telle situation dangereuse sont pris en charge avec efficacité.

6.10.4 Eléments de sortie

6.10.4.1 Les résultats de la présente phase doivent être documentés et comprendre les hypothèses et justificatifs correspondants.

6.10.4.2 Toutes les tâches d'acceptation entreprises au cours de la présente phase doivent être consignées.

b) verification and validation, by analysis and test, that the installed system meets RAMS requirements. It should be noted that for some railway systems, acceptance of the Application Specific Safety Case will be required prior to installation and commissioning activities taking place;

c) verification that the commissioning activity was carried out in accordance with the Commissioning Plan;

d) assessment of the adequacy and effectiveness of the operational data collection system;

e) assessment of the adequacy of the methods, tools and techniques used within the phase;

f) assessment of the competence of all personnel undertaking tasks within the phase.

6.9.5.2 Any errors or shortfalls may require the re-application of some or all of the activities of one or more previous life cycle phases.

6.10 Phase 10: System acceptance

6.10.1 Objectives

The objectives of this phase are to

a) assess compliance of the total combination of sub-systems, components and external risk reduction measures with the overall RAMS requirements of the complete system;

b) accept the system for entry into service.

6.10.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirement, and in particular the system requirements prepared in phase 4, the Verification and Validation Plan and Acceptance Plan prepared in phase 4 and the record of verification and validation tasks prepared in phase 9.

6.10.3 Requirements

6.10.3.1 Requirement 1 of this phase shall be to assess all system verification and validation tasks, specifically the RAM verification and validation and the Application Specific Safety Case, in accordance with the System Acceptance Plan.

6.10.3.2 Requirement 2 of this phase shall be to formally accept the system for entry into service, if appropriate.

6.10.3.3 Requirement 3 of this phase shall be to review and update the Hazard Log to record any residual hazards identified during system validation or acceptance and to ensure that the risks from any such hazards are effectively managed.

6.10.4 Deliverables

6.10.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.10.4.2 A record of all acceptance tasks undertaken within the phase, shall be maintained.

6.10.4.3 Le Registre des Situations Dangereuses doit être mis à jour lors de la présente phase.

6.10.4.4 Les éléments de sortie de la présente phase constituent un point d'entrée déterminant pour les phases suivantes du cycle de vie.

6.10.5 Vérification

6.10.5.1 Les tâches de vérification suivantes doivent être effectuées lors de la présente phase:

a) l'évaluation de la pertinence des informations et, le cas échéant, des données et des autres informations statistiques, utilisées comme éléments d'entrée pour les tâches de la présente phase;

b) l'acceptation, au moyen d'analyses et de tests, de la conformité du système aux exigences de FDMS, y compris aux exigences de coût global;

c) la vérification de la conformité de l'acceptation au Plan d'Acceptation;

d) l'évaluation de la mise à jour du Plan de Sécurité pour s'assurer qu'il demeure applicable;

e) l'évaluation de l'efficacité de la prise en charge de toute situation dangereuse résiduelle;

f) l'évaluation de la pertinence et de l'exhaustivité du Dossier de Sécurité de l'Application;

g) l'évaluation de la pertinence des méthodes, des outils et des techniques utilisés au cours de la présente phase;

h) l'évaluation de la compétence de l'ensemble des personnes chargées d'effectuer des tâches au cours de la présente phase.

6.10.5.2 D'éventuelles erreurs ou lacunes peuvent nécessiter la reprise de tout ou partie des activités d'une ou de plusieurs phases précédentes du cycle de vie.

6.11 Phase 11: Exploitation et maintenance

6.11.1 Objectifs

Les objectifs de la présente phase sont d'assurer l'exploitation (dans les limites spécifiées), la maintenance et la logistique de l'ensemble combiné des sous-systèmes, des composants et des dispositifs externes de réduction du risque de manière à assurer la continuité de la conformité aux exigences de FDMS du système.

6.11.2 Eléments d'entrée

Les éléments d'entrée de la présente phase doivent comporter toutes les informations pertinentes et, le cas échéant, les données nécessaires pour satisfaire aux exigences de la phase et, notamment, les procédures d'exploitation et de maintenance élaborées lors de la phase 6.

6.11.3 Exigences

6.11.3.1 L'exigence n° 1 de la présente phase doit être de contrôler la réalisation du système et de mettre en œuvre les procédures d'exploitation et de maintenance, en particulier du point de vue des performances du système et des questions liées au coût global.

6.11.3.2 L'exigence n° 2 de la présente phase doit être d'assurer la conformité du système aux exigences de FDMS tout au long de la présente phase:

a) par la mise à jour régulière des procédures d'exploitation et de maintenance;

b) par la mise à jour régulière des documents de formation;

6.10.4.3 An updated Hazard Log shall be produced within this phase.

6.10.4.4 The deliverables from this phase form a key input to subsequent life cycle phases.

6.10.5 Verification

6.10.5.1 The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase;

b) acceptance, by analysis and test, that the system meets the RAMS requirements, including life cycle cost requirements;

c) verification that the acceptance activity was carried out in accordance with the Acceptance Plan;

d) assessment of the continued applicability of the revised Safety Plan;

e) assessment to ensure that any residual hazards are being managed effectively;

f) assessment of the adequacy and completeness of the application specific safety case;

g) assessment of the adequacy of the methods, tools and techniques used within the phase;

h) assessment of the competence of all personnel undertaking tasks within the phase.

6.10.5.2 Any errors or shortfalls may require the re-application of some or all of the activities of one or more previous life cycle phases.

6.11 Phase 11: Operation and maintenance

6.11.1 Objectives

The objective of this phase shall be to operate (within specified limits), maintain and support the total combination of sub-systems, components and external risk reduction measures such that compliance with system RAMS requirements is maintained.

6.11.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data necessary to meet the requirement, and in particular the operation and maintenance procedures prepared in phase 6.

6.11.3 Requirements

6.11.3.1 Requirement 1 of this phase shall be to monitor implementation of the system and to implement the operation and maintenance procedures, particularly with regard to system performance and life cycle cost issues.

6.11.3.2 Requirement 2 of this phase shall be to assure compliance with system RAMS requirements throughout this phase by

a) regular review and update of operation and maintenance procedures;

b) regular review of system training documentation;

c) par la mise à jour régulière du Registre des Situations Dangereuses et du Dossier de Sécurité;

d) par un soutien logistique efficace, comportant les pièces de rechange, les outils, les instruments d'étalonnage, le personnel compétent et la maintenance fondée sur la FDMS;

e) par la maintenance du Système de Signalement, d'Analyse et de Correction des Défaillances (SSACD).

6.11.4 Eléments de sortie

6.11.4.1 Toutes les tâches de FDMS entreprises au cours de la phase doivent être consignées ainsi que les éventuels hypothèses et justificatifs correspondants.

6.11.4.2 La documentation du système doit être, au besoin, mise à jour au cours de la présente phase.

6.11.4.3 Les éléments de sortie de la présente phase constituent un point d'entrée déterminant pour les phases suivantes du cycle de vie.

6.11.5 Vérification

Les tâches de vérification suivantes doivent être effectuées au cours de la présente phase:

a) l'évaluation de la pertinence des informations et, le cas échéant, des données et autres informations statistiques, utilisées comme éléments d'entrée pour les tâches de la présente phase;

b) la vérification de la conformité des modifications portant sur des éléments de soutien, aux exigences de FDMS du système et aux exigences de coût global;

c) l'évaluation de la pertinence des méthodes, des outils et des techniques utilisés au cours de la présente phase;

d) l'évaluation de la compétence de l'ensemble des personnes chargées d'effectuer des tâches au cours de la présente phase.

6.12 Phase 12: Surveillance des performances du système

6.12.1 Objectifs

L'objectif de la présente phase est de maintenir le niveau de confiance dans les performances de FDMS du système.

6.12.2 Eléments d'entrée

Les éléments d'entrée de la présente phase doivent comporter toutes les informations pertinentes et, le cas échéant, les données nécessaires pour satisfaire aux exigences de la phase et, notamment, les exigences de FDMS du système et les données de soutien au système.

6.12.3 Exigences

6.12.3.1 L'exigence n° 1 de la présente phase doit être l'établissement, la mise en œuvre et la révision régulière du processus suivant:

– la collecte des statistiques relatives aux performances d'exploitation et à la FDMS;

– l'acquisition, l'analyse et l'évaluation des données relatives aux performances et à la FDMS;

– la vérification de la pérennité de la validité des hypothèses figurant dans le dossier de sécurité.

c) regular review and update of Hazard Log and Safety Case;

d) effective logistic support, including spare parts, tools, calibration, competent staff, RAMS focused maintenance;

e) maintenance of the Failure Reporting Analysis and Corrective Action System (FRACAS).

6.11.4 Deliverables

6.11.4.1 A record of all RAMS tasks undertaken within the phase shall be maintained, along with any assumptions and justifications made during the phase.

6.11.4.2 System documentation shall be updated, as appropriate, within this phase.

6.11.4.3 The deliverables from this phase form a key input to subsequent life cycle phases.

6.11.5 Verification

The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase;

b) verification that changes in support arrangements are consistent with system RAMS requirements and life cycle cost requirements;

c) assessment of the adequacy of the methods, tools and techniques used within the phase;

d) assessment of the competence of all personnel undertaking tasks within the phase.

6.12 Phase 12: Performance monitoring

6.12.1 Objectives

The objective of this phase shall be to maintain confidence in the RAMS performance of the system.

6.12.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data necessary to meet the requirement, particularly system RAMS requirements and system support data.

6.12.3 Requirements

6.12.3.1 Requirement 1 of this phase shall be to establish, implement and regularly review a process for

– the collection of operational performance and RAMS statistics;

– the acquisition, analysis and evaluation of performance and RAMS data;

– checking that the assumptions made in the safety case remain valid.

6.12.3.2 L'exigence n° 2 de la présente phase doit être d'analyser les données et les statistiques relatives aux performances et à la FDMS afin d'en tirer

– de nouvelles procédures d'exploitation et de maintenance;

– des modifications du soutien logistique du système.

6.12.4 Eléments de sortie

6.12.4.1 Toutes les tâches de surveillance des performances entreprises au cours de la présente phase doivent être consignées ainsi que les éventuels hypothèses et justificatifs élaborés au cours de la présente phase.

6.12.4.2 La documentation de soutien du système est, au besoin, mise à jour au cours de la présente phase.

6.12.4.3 Les éléments de sortie de la présente phase constituent un point d'entrée déterminant pour les phases suivantes du cycle de vie.

6.12.5 Vérification

Les tâches suivantes de vérification du processus doivent être effectuées au cours de la présente phase:

a) l'évaluation de la pertinence des informations et, le cas échéant, des données et autres informations statistiques, utilisées comme éléments d'entrée pour les tâches de la présente phase;

b) la vérification de la conformité des modifications portant sur des éléments de soutien, aux exigences de FDMS du système et aux exigences de coût global;

c) l'évaluation de la pertinence des méthodes, des outils et des techniques utilisés au cours de la présente phase;

d) l'évaluation de la compétence de l'ensemble des personnes chargées d'effectuer des tâches au cours de la présente phase.

6.13 Phase 13: Modification et remise à niveau

6.13.1 Objectifs

L'objectif de la présente phase doit être de contrôler les tâches de modification et de remise à niveau du système pour assurer le maintien de ses exigences en termes de FDMS.

6.13.2 Eléments d'entrée

Les éléments d'entrée de cette phase doivent comporter toutes les informations pertinentes et, le cas échéant, les données nécessaires pour satisfaire aux exigences de la présente phase.

6.13.3 Exigences

6.13.3.1 L'exigence n° 1 de la présente phase doit être d'établir un Plan de Sécurité.

6.13.3.2 L'exigence n° 2 de la présente phase doit être l'établissement, la mise en œuvre et la révision régulière du processus de contrôle des modifications et des remises à niveau du système en termes de FDMS, qui comporte notamment

– le contrôle fondé sur l'utilisation obligatoire d'un modèle de cycle de vie adapté à l'ensemble des tâches de modification et de remise à niveau;

– l'établissement obligatoire d'une procédure de vérification, de validation et d'acceptation des performances de FDMS après modification et remise à niveau;

6.12.3.2 Requirement 2 of this phase shall be to analyse performance and RAMS data and statistics to influence

– new operating and maintenance procedures;
– changes in logistic support for the system.

6.12.4 Deliverables

6.12.4.1 A record of all performance monitoring tasks undertaken within the phase shall be maintained, along with any assumptions and justifications made during the phase.

6.12.4.2 System support documentation may be updated within this phase.

6.12.4.3 The deliverables from this phase form a key input to subsequent life cycle phases.

6.12.5 Verification

The following process verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase;
b) verification that changes in support arrangements are consistent with system RAMS requirements and life cycle cost requirements;
c) assessment of the adequacy of the methods, tools and techniques used within the phase;
d) assessment of the competence of all personnel undertaking tasks within the phase.

6.13 Phase 13: Modification and retrofit

6.13.1 Objectives

The objective of this phase shall be to control system modification and retrofit tasks to maintain system RAMS requirements.

6.13.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data, necessary to meet the requirement.

6.13.3 Requirements

6.1.13.1 Requirement 1 of this phase shall be to establish a Safety Plan.

6.13.3.2 Requirement 2 of this phase shall be to establish, implement and regularly review a process to control system modification and retrofit, in the context of RAMS, including:

– control through the mandatory use of an appropriate life cycle model for all modification and retrofitting tasks;
– a requirement to establish a procedure for verifying, validating and accepting the RAMS performance of the system following modification and retrofit;

– l'analyse obligatoire des motifs de la modification;
– la réalisation d'une analyse d'impact de la modification sur la FDMS, y compris en termes de coût global;
– la programmation obligatoire de la réalisation de la modification et de son acceptation;
– la consignation obligatoire des tâches de modification et de remise à niveau;
– la mise à jour obligatoire de l'ensemble de la documentation concernée du système.

6.13.4 Eléments de sortie

6.13.4.1 Le principal élément de sortie de la présente phase est un système modifié et validé.

6.13.4.2 Les résultats de la présente phase doivent être documentés et comprendre les hypothèses et justificatifs correspondants.

6.13.4.3 Toutes les tâches de vérification, de validation et d'acceptation entreprises au cours de la phase doivent être consignées.

6.13.4.4 Il convient de mettre à jour le Registre des Situations Dangereuses au cours de la présente phase.

6.13.4.5 La présente phase doit donner lieu à la mise à jour du Dossier de Sécurité de l'Application.

6.13.4.6 Il convient de mettre à jour, au besoin, tous les documents relatifs à la FDM.

6.13.4.7 Les éléments de sortie de la présente phase constituent un point d'entrée déterminant pour les phases suivantes du cycle de vie.

6.13.5 Vérification

Les tâches suivantes de vérification du processus suivantes doivent être effectuées au cours de la présente phase:

a) l'évaluation de la pertinence des informations et, le cas échéant, des données et autres informations statistiques, utilisées comme éléments d'entrée pour les tâches de la présente phase;
b) la vérification et la validation de la conformité des éventuels changements ou modifications apportés au système aux exigences de FDMS et de coût global;
c) l'évaluation de la pertinence et de l'exhaustivité des modifications apportées à la documentation du système et, en particulier, aux documents du Dossier de Sécurité;
d) l'évaluation de la pertinence des méthodes, des outils et des techniques utilisés au cours de la présente phase;
e) l'évaluation de la compétence de l'ensemble des personnes chargées d'effectuer des tâches au cours de la présente phase.

6.14 Phase 14: Retrait du service et dépose

6.14.1 Objectifs

L'objectif de la présente phase est de contrôler les tâches de retrait du service et de dépose du système.

– a requirement to analyse the reasons for the change;
– a requirement to carry out a RAMS impact analysis of the change, including the impact on life cycle cost requirements;
– a requirement to plan the implementation and subsequent acceptance of the change;
– a requirement to record modification and retrofit tasks;
– a requirement to update all affected system documentation.

6.13.4 Deliverables

6.13.4.1 The key deliverable from this phase is a validated, modified system.

6.13.4.2 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.13.4.3 A record of all verification, validation and acceptance tasks undertaken within the phase, shall be maintained.

6.13.4.4 An updated Hazard Log should be produced within this phase.

6.13.4.5 An updated Application Safety Case shall be produced within this phase.

6.13.4.6 All RAM related documents should be reviewed and updated where necessary.

6.13.4.7 The deliverables from this phase form a key input to subsequent life cycle phases.

6.13.5 Verification

The following process verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase;
b) verify and validate that any changes or modifications to the system are consistent with the RAMS requirements for the system and life cycle cost requirements;
c) assessment of the adequacy and completeness of any amended system documentation, in particular, any system safety case documents;
d) assessment of the adequacy of the methods, tools and techniques used within the phase;
e) assessment of the competence of all personnel undertaking tasks within the phase.

6.14 Phase 14: Decommissioning and disposal

6.14.1 Objectives

The objective of this phase shall be to control system decommissioning and disposal tasks.

6.14.2 Eléments d'entrée

Les éléments d'entrées de la présente phase doivent comporter toutes les informations pertinentes et, le cas échéant, les données nécessaires pour satisfaire aux exigences de la phase.

6.14.3 Exigences

6.14.3.1 L'exigence n° 1 de la présente phase doit être

a) de définir l'impact du retrait du service et de la dépose sur tout autre système ou élément externe en relation avec le système à retirer du service;

b) de programmer le retrait du service, qui comporte notamment l'établissement de procédures concernant:

   – la mise hors service en sécurité du système et de tout autre élément externe associé;

   – le démontage en sécurité du système et de tout autre élément externe associé;

   – l'assurance que tout autre système ou élément externe concerné par le retrait du service du système reste conforme aux exigences de FDMS.

6.14.3.2 L'exigence n° 2 de la présente phase doit être de fournir une analyse des performances relatives au cycle de vie de la FDMS, y compris celle du coût global; cette analyse sera utilisée comme élément d'entrée des systèmes futurs.

6.14.4 Eléments de sortie

6.14.4.1 Les résultats de la présente phase doivent être documentés et comprendre les hypothèses et justificatifs correspondants.

6.14.4.2 Toutes les tâches de retrait du service et de dépose entreprises au cours de la présente phase doivent être consignées.

6.14.4.3 Il convient de mettre à jour le Registre des Situations Dangereuses au cours de la présente phase.

6.14.4.4 Il convient d'établir le Plan de Sécurité traitant des tâches de retrait du service et de dépose et de le clore après achèvement des travaux.

6.14.4.5 Le Dossier de Sécurité de l'Application est au besoin mis à jour au cours de la présente phase.

6.14.4.6 La documentation montrant que les systèmes associés concernés restent conformes aux exigences de FDMS au cours des tâches de retrait du service et de dépose est, au besoin, mise à jour.

6.14.5 Vérification

Les tâches suivantes de vérification du processus doivent être effectuées au cours de la présente phase:

a) l'évaluation de la pertinence des informations et, le cas échéant, des données et autres informations statistiques, utilisées comme éléments d'entrée pour les tâches de la présente phase;

b) l'évaluation de la pertinence de toute la documentation des systèmes concernés par les opérations de retrait du service et de dépose;

c) l'évaluation de la pertinence des méthodes, des outils et des techniques utilisés au cours de la présente phase;

d) l'évaluation de la compétence de l'ensemble des personnes chargées d'effectuer des tâches au cours de la présente phase.

6.14.2 Inputs

The input to this phase shall include all relevant information, and where appropriate, data necessary to meet the requirement.

6.14.3 Requirements

6.14.3.1 Requirement 1 of this phase shall be to

a) establish the impact of decommissioning and disposal on any system or external facility associated with the system to be de-commissioned;

b) plan the decommissioning, including the establishment of procedures for:

- the safe closing down of the system and any associated external facility;
- the safe dismantling of the system and any associated external facility;
- the continued assurance of compliance with RAMS requirements of any systems or external facility affected by the decommissioning of the system.

6.14.3.2 Requirement 2 of this phase shall be to provide an analysis of RAMS life cycle performance for input to future systems, including life cycle costings.

6.14.4 Deliverables

6.14.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.14.4.2 A record of all de-commissioning and disposal tasks undertaken within the phase, shall be maintained.

6.14.4.3 An updated Hazard Log should be produced within this phase.

6.14.4.4 A Safety Plan should be established to address the de-commissioning and disposal tasks and closed out following completion of the work.

6.14.4.5 A revised Application Safety Case may be produced within this phase.

6.14.4.6 Updated documentation may be produced covering the continued compliance with RAMS requirements of affected associated systems during the decommissioning and disposal tasks.

6.14.5 Verification

The following process verification tasks shall be undertaken within this phase:

a) the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase shall be assessed;

b) assessment of the adequacy of any documentation for systems affected by decommissioning and disposal activities;

c) assessment of the adequacy of the methods, tools and techniques used within the phase;

d) assessment of the competence of all personnel undertaking tasks within the phase.

Annexe A
(informative)

Exemple de spécification des exigences de FDMS

A.1 Généralités

Afin de faciliter l'application de cette norme, la présente annexe donne un exemple de spécification des exigences de FDMS pour des systèmes ferroviaires. Il est fait référence aux figures 8 et 9 de cette norme ainsi qu'aux phases correspondantes du cycle de vie dont le détail figure à l'article 6,en illustrant cette présentation par le matériel roulant.

A.2 Présentation générale

La structure de base et le contenu d'une spécification des exigences de FDMS, dans le cadre des exigences globales du système, peuvent être présentés sous la forme suivante.

1. **Identification du projet**
   - 1.1 Identification du projet
   - 1.2 Eléments de sortie et délais
   - 1.3 Organisation du projet et management de la FDMS
2. **Description générale du système**
   - 2.1 Description technique du système
   - 2.2 Application spécifique et exploitation:

     exemple pour le matériel roulant:
     - exploitation de trains à grande vitesse;
     - composition des trains;
     - profil de mission;
     - localisation géographique;
     - horaires des trains et tolérances;
     - scénarios d'exploitation;
     - principes de sécurité;
     - considérations liées au facteur humain.
   - 2.3 Description technique des sous-systèmes:

     exemple pour le matériel roulant:
     - système d'alimentation;
     - système de freinage;
     - système de traction;
     - ventilation;
     - système de protection;
     - système de contrôle-commande;
     - système de communication;
     - chauffage.

Annex A
(informative)

Outline of RAMS specification – example

A.1 General

In order to facilitate the application of this standard, a principal outline of a RAMS specification for railway systems is presented in this annex. This outline example relates to figure 8 and figure 9 of this standard and the corresponding descriptions of the life cycle phases detailed in clause 6, using rolling-stock as an example to provide supporting detail within the outline.

A.2 Outline

The basic structure and contents of a RAMS specification, part of the overall system requirements, may accord with the following outline.

1. **Project identification**
   - 1.1 Identify project
   - 1.2 Deliverables and deadlines
   - 1.3 Project organisation and RAMS management
2. **General system description**
   - 2.1 Technical description of system
   - 2.2 Specific application and operation:

     example for rolling stock:
     - high speed train operation;
     - train compositions;
     - mission profile;
     - geographical location;
     - train schedule and tolerances;
     - operation scenarios;
     - safety principles;
     - human factor considerations.
   - 2.3 Technical description of sub-systems:

     example for rolling stock:
     - energy supply system;
     - brake system;
     - propulsion system;
     - ventilation;
     - protection system;
     - control system;
     - communication system;
     - heating.