Analyse des risques d'accident dans les transports ferroviaires

Mohamed Habib Mazouni, Habib Hadj Mabrouk

Analyse des risques d'accident
dans les transports ferroviaires

Mohamed Habib MAZOUNI **Habib HADJ-MABROUK**

Email: mohamed-habib.mazouni@inrets.fr
Tel : + 33 (0) 1 47 40 72 13
Fax: + 33 (0) 1 45 47 56 06
INRETS
2, Avenue du Général Malleret-Joinville
F-94114 Arcueil Cedex France

Résumé

L'analyse préliminaire des risques(APR) permet d'identifier essentiellement les accidents potentiels liés au système et à ses interfaces afin d'évaluer leur probabilité d'occurrence ainsi que la gravité des dommages qu'ils puissent engendrer et enfin de proposer des solutions (mesures de prévention et/ou de protection) qui permettront de contrôler et réduire le niveau de risque inhérent (Gravité/Occurrence).

Bien que primordiale parmi les activités d'analyse de la sécurité, l'APR est très différemment développée et demeure mal définie. Les documents recommandés sont peu précis et s'écartent parfois des usages. Les formats de représentation des résultats de l'analyse sont souvent extrêmement variés. En outre, la terminologie et les concepts liés aux APR sont très fluctuants, voire contradictoires d'un système de transport à un autre ou d'un constructeur à un autre. Enfin, l'élaboration et l'évaluation d'une APR sont des pratiques laborieuses et fastidieuses qui ne sont pas habituellement soutenues par une stratégie formalisée. En effet, l'exhaustivité et la cohérence des analyses demeurent essentiellement fondées sur le savoir-faire, l'intelligence et l'intuition des experts du domaine.

Conformément à la réglementation en vigueur et en s'inspirant de la norme CEI 300-3-9, le présent article introduit l'analyse préliminaire des risques et définit ses cadres réglementaire et normatif.

Mots-Clés :

Analyse Préliminaire des Risques(APR), Accident Potentiel, Niveau de risque, sécurité, transports ferroviaires.

I. Introduction à l'Analyse Préliminaire des Risques

Pour construire la sécurité, il existe plusieurs analyses hiérarchisées admises par l'INRETS et réalisées par le constructeur : Analyse Préliminaire des Risques (APR), analyse de la sécurité fonctionnelle (ASF) et analyse de la sécurité du produit réalisé qui concerne l'analyse de la sécurité des logiciels (ASL) et l'analyse de la sécurité des matériels (ASM).

Une APR bénéficie d'une part de l'expérience et de l'imagination du constructeur et d'autre part du suivi en exploitation (retour d'expérience). Du fait que cette analyse est réalisée très tôt par rapport au développement d'un système, ses résultats peuvent être incomplets ou imprécis. Une APR doit être donc complétée et mise à jour jusqu'à ce que la conception du système soit assez avancée. Ceci permet de vérifier qu'à chaque accident potentiel identifié, correspond dans la conception, des fonctions, des précautions ou dispositions pour contrôler ou réduire sa fréquence d'occurrence ainsi que sa gravité. Le dossier d'APR reste ouvert pendant toute l'étude et est constamment mis à jour.

L'APR est un document fondamental dans le processus de construction de la sécurité d'un système de transport guidé. En effet, de la qualité de l'APR dépend la qualité des analyses postérieures et donc la sécurité globale du système.

I.1 interactions de l'APR avec les autres analyses de sécurité

Les résultats de l'APR permettent de définir les exigences et critères de sécurité du système à prendre en compte lors des phases de conception et de réalisation des équipements matériels et logiciels et enfin d'établir les lignes directrices des analyses de sécurité postérieures : l'Analyse de sécurité fonctionnelle, l'Analyse de Sécurité des Logiciels et l'Analyse de Sécurité des Matériels.

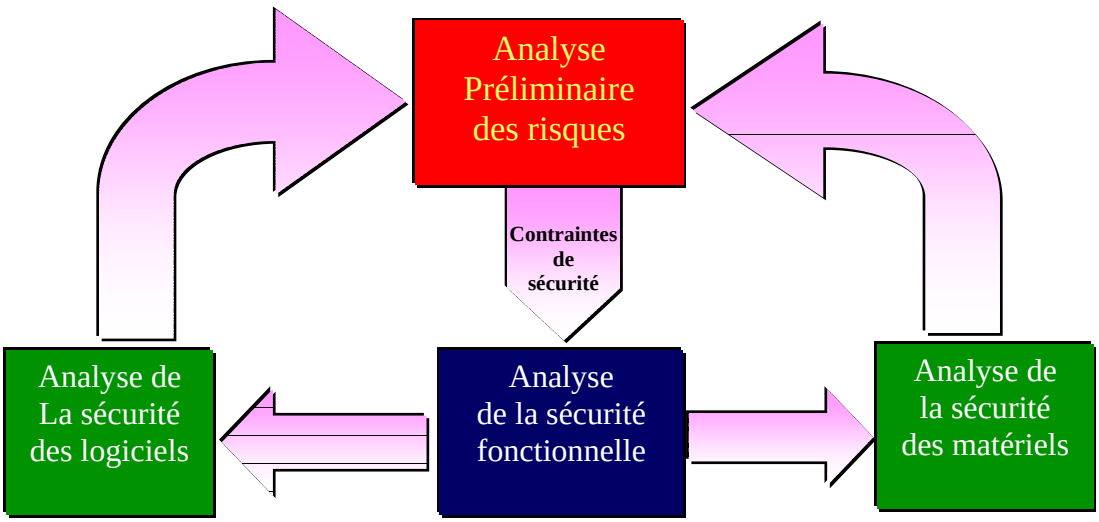

Fig.1 Interactions entre l'APR, l'ASF, l'ASM et l'ASL [Hadj-Mabrouk, 1997]

Les interactions entre les différentes analyses montrées par la figure 1 doivent se dérouler sous les contraintes suivantes : Exhaustivité en terme de cas étudiés, Cohérence des résultats obtenus et Traçabilité des correspondances entre les différentes analyses, autrement dit les résultats d'une analyse doivent être exploités facilement par les analyses situées en aval.

I.2 Place de l'APR dans la méthodologie de développement d'un système

L'ensemble des études de sécurité est réalisé parallèlement aux différentes activités du cycle de vie d'un système. L'analyse Préliminaire des Risques (APR) est considérée comme la première pièce du dossier de sécurité dans un système de transport guidé. Elle intervient très tôt dans le processus de développement du système, dès la phase de spécification du système [Hadj-Mabrouk, 1995].

En fait, il existe une synchronisation de tâches entre les activités de développement du système et les activités de construction de la sécurité.

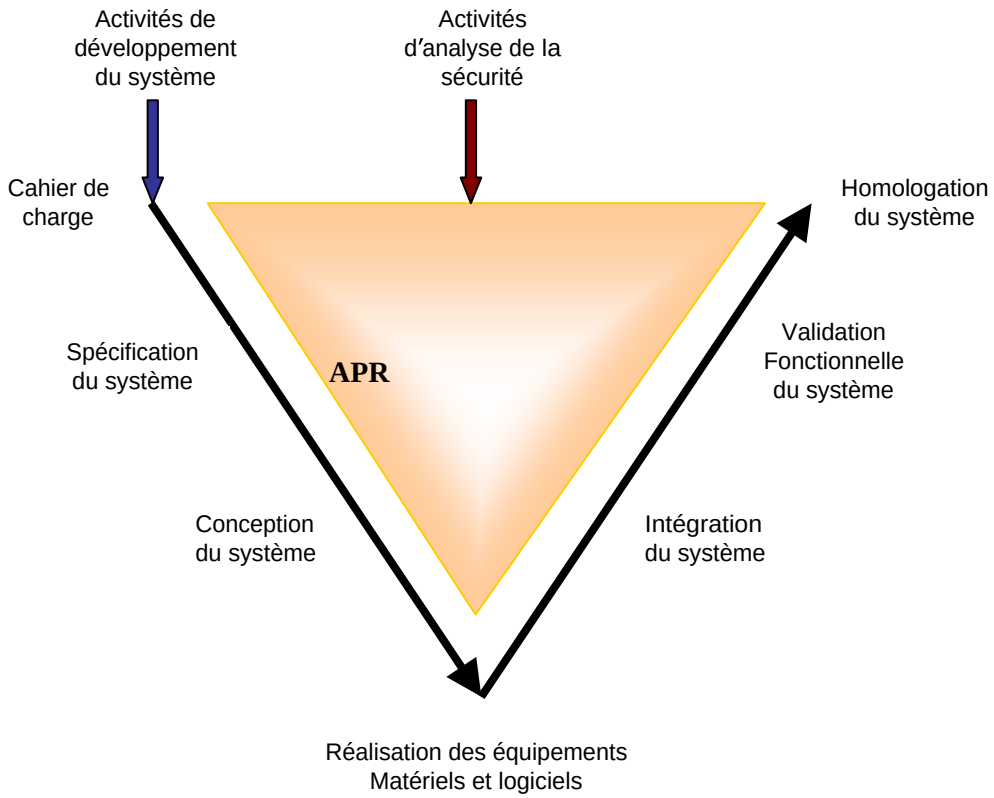

Fig.2 Place de l'APR dans la méthodologie de développement du système [Hadj-Mabrouk, 1995]

II. Cadre réglementaire de l'APR

II.1 Décret n°2000-286 du 30 mars 2000 relatif à la sécurité du réseau ferré national

Le Dossier Préliminaire de Sécurité (DPS) prend en compte les données techniques et fonctionnelles ainsi que les objectifs de sécurité énoncés au dossier de définition. La réalisation d'un nouveau système ne peut commencer qu'après que le ministre chargé des transports a approuvé ce dossier. Ce dernier peut, si nécessité, demander que soient apportés des compléments au dossier de sécurité (DS). Ce dossier est tenu à jour pendant toute la durée de l'exploitation du système considéré.

Selon l'arrêté d'application du 08 janvier 2002, le DPS précise les objectifs de sécurité poursuivis et les méthodes qui seront appliquées pour les atteindre, les méthodes de démonstration et les principes dont le respect permettra le maintien du niveau de sécurité pendant l'exploitation du système. Le DPS comporte notamment un document relatif à l'organisation du projet et s'appuie sur les résultats d'une ***Analyse Préliminaire des Risques (APR).***

L'arrêté d'application du 08 janvier 2002 précise aussi que le Dossier de sécurité (DS) a pour objet de décrire le système tel que réalisé, d'apporter la preuve du respect des mesures de sécurité exposées dans le dossier préliminaire de sécurité (DPS). Il contient les conclusions des études de sécurité réalisées et attestation de **la couverture des risques identifiés dans l'APR**, autrement dit, une démonstration de l'aptitude du système à être exploité et maintenu avec le niveau de sécurité requis.

II.2 Décret n° 2003-425 du 9 mai 2003 relatif à la sécurité des transports publics guidés

L'article 16 stipule que : « les travaux de réalisation ou de modification substantielle d'un système de transport ne peuvent être engagés qu'après l'approbation d'un dossier préliminaire de sécurité (DPS) par le préfet du département dans lequel doit être implanté le système, sans préjudice des autorisations éventuellement nécessaires au titre d'autres réglementations ».

L'article 17 précise que le dossier préliminaire de sécurité doit démontrer, à partir **d'une analyse des risques** résultant des options de conception des divers éléments constitutifs du système de transport, que les dispositions fonctionnelles, techniques, d'exploitation et de maintenance prévues pour le projet ainsi que le programme prévu d'essais et de tests, permettent d'atteindre l'objectif de sécurité tout au long de la durée de vie du système, de prévenir les différents types d'accidents étudiés et d'en réduire les conséquences, et de prendre en compte les risques naturels ou technologiques susceptibles d'affecter le système de transport».

Le texte évoque une analyse des risques, mais ne précise pas s'il s'agit d'une APR. Néanmoins ceci est dit implicitement par la précision « une analyse des risques résultant des options de conception ».

II.3 Arrêté du 8 janvier 2002 pris pour l'application du décret n° 2000-286 du 30 mars 2000 relatif à la sécurité du réseau ferré national

Cet arrêté d'application précise en annexe 2 qu'une APR devrait contenir les documents suivants :

- Description du fonctionnement du système ;
- Identification des événements redoutés liés à la sécurité du système ;
- Evaluation et classement des risques associés ;
- Liste des mesures de prévention et de protection à mettre en oeuvre pour réduire ces risques;
- Guide pour les études de sécurité détaillées ultérieures;
- Proposition d'allocation des objectifs de sécurité entre les composants du système ;
- Cadre de référence pour la validation du projet ;
- Cadre de référence pour l'élaboration de la documentation du projet.

L'annexe 3 précise les documents contenus dans un DPS :

- Plan d'organisation du projet et de management de la sécurité ;
- Présentation et justification des objectifs de sécurité ;
- Présentation générale du système et de son environnement ;
- Description fonctionnelle et structurelle du système et de son environnement ;
- Identification des composants de sécurité ;
- Documents de référence : textes réglementaires, documents normatifs ;
- Liste des spécifications techniques et fonctionnelles du système de référence ;
- Liste des spécifications techniques et fonctionnelles du système en projet ;
- Liste des constituants possédant déjà des certificats ;
- Présentation et justification des écarts éventuels avec le système de référence ;
- Résultats de l'**Analyse Préliminaire des Risques** ;
- Justification des compétences de l'organisme ou service technique indépendant ;
- Plan d'évaluation ;
- Présentation détaillée des aspects novateurs du système ;
- Présentation et justification des études et vérifications de sécurité ;
- Présentation et justification des études de démonstration de la sécurité ;
- Liste des documents intéressant la sécurité et la qualité à produire par le constructeur ;
- Définition et programme prévisionnel des tests et essais ;
- Principes d'exploitation et de maintenance envisagés.

L'annexe 4, précise les documents contenus dans un DS :

- Documents descriptifs du système réalisé ;
- Liste des composants de sécurité ;
- Attestation du respect des méthodes de travail et des référentiels présentés dans le dossier préliminaire de sécurité (DPS) ;
- Présentation et justification des écarts éventuels ;
- **Objectifs de sécurité ;**
- Attestation, par la Société nationale des chemins de fer français(SNCF), de la conformité de la réalisation aux engagements pris dans le dossier préliminaire de sécurité et, le cas échéant, aux prescriptions énoncées dans l'acte d'approbation de ce dossier ;
- Rapport de l'organisme ou service technique indépendant (OSTI) ;
- Conclusions des études de sécurité réalisées et attestation de **la couverture des risques identifiés dans l'APR** ;
- Résultats des tests et essais ;
- Plan de documentation et de gestion des modifications ;
- Principes suivis pour la sélection, la formation et l'habilitation des personnels ;
- Liste des règlements et consignes d'exploitation ;
- Présentation et justification des principes de maintenance : liste des documents de référence ;
- Présentation de l'organisation de l'exploitation en couvrant notamment les aspects : suivi de l'évolution du niveau de sécurité, statistiques, retour d'expérience, inspections, contrôles et audits ;
- Plan d'intervention et de sécurité.

III. Cadre normatif de l'APR

Cette partie tire profit et s'inspire de la norme CEI 300-3-9 [CEI, 1995] relative à la gestion de la sûreté de fonctionnement et plus précisément de la 3éme partie présentant le processus d'analyse des risques.

Cette norme recommande qu'une analyse des risques soit effectuée conformément à une séquence de six étapes :

1. Définition du domaine d'application ;
2. Identification des dangers et évaluation initiale des conséquences ;
3. Estimation du risque ;

4. Vérification ;
5. Documentation ;
6. Mise à jour de l'analyse.

III.1 Définition du domaine d'application

La première démarche de l'APR selon la norme concerne la description de l'emploi prévu du dispositif. Cette étape a pour but de fournir une base pour l'identification des dangers. D'un point de vue générique il est conseillé dans cette étape de fournir les éléments suivants :

- Description des raisons et problèmes qui ont donné lieu à l'APR ;
- Définition du système et une description de ses interfaces ;
- Description des aspects sécuritaires, techniques, environnementaux, légaux, organisationnels et humains concernant l'activité et le problème à analyser ;
- Définition des hypothèses et contraintes régissant l'analyse ;
- Identification des décisions à prendre, du résultat requis de l'étude ainsi que des décisionnaires.

III.2 Identification des dangers et évaluation initiale des conséquences

Il est nécessaire d'identifier les dangers qui engendrent un risque dans le système ainsi que les formes qu'ils pourraient prendre. Il faut donc énoncer clairement les dangers constatés y compris ceux qui sont apparus lors d'accidents précédents, et ce selon les procédés du retour d'expérience.

III.3 Estimation du risque

Il est important d'effectuer une évaluation initiale de l'importance des dangers sur la base d'une analyse des conséquences des accidents potentiels qui leur sont associés, ainsi que d'un examen des causes premières. Cette évaluation donnera lieu à l'une des actions suivantes :

- Mesures correctives prises pour éliminer, réduire ou contrôler le risque.
- Arrêt de l'analyse à ce niveau si le niveau de risque est acceptable.
- Poursuite de l'estimation du risque après avoir pris les mesures nécessaires.

L'estimation des risques doit examiner les événements ou les circonstances initiales, la séquence d'événements concernée, d'éventuelles circonstances atténuantes ainsi que la nature et la fréquence des conséquences délétères possibles des dangers identifiés pour obtenir une mesure du niveau des risques à analyser. Les mesures prises pourraient concerner les risques encourus par les personnes, les biens ou l'environnement [CEI, 1995].

Dans le cas d'une analyse préliminaire des risques cette définition doit être formulée comme suit :

« L'estimation du niveau de risque doit examiner les événements ou les circonstances initiales, la séquence d'événements concernée, d'éventuelles circonstances atténuantes ainsi que la nature et la fréquence des accidents potentiels identifiés(Accident/Incident) pour obtenir une mesure de leur niveau de risque. Les mesures prises pourraient concerner les risques encourus par les personnes, les biens ou l'environnement »

Notons que les méthodes utilisées pour l'estimation des risques sont souvent quantitatives. Une classification comparative, quantitative ou qualitative des risques peut aussi être intéressante.

III.3.1 Analyse de fréquence :

L'analyse de fréquence sert à estimer la probabilité d'occurrence des accidents potentiels préalablement identifiés. Plusieurs approches peuvent répondre à ceci, les plus pertinentes sont celles-ci :

- Le retour d'expérience
- La déduction des fréquences au moyen de techniques analytiques
- L'utilisation d'avis d'experts

Ces trois approches peuvent être croisées, c'est-à-dire adoptées en même temps. Par exemple, appliquer les deux premières séparément, et puis réguler les résultats à l'aide d'avis d'experts.

III.3.2 Analyse des conséquences

L'analyse des conséquences sert à estimer l'impact sur l'humain, le système et l'environnement en cas d'occurrence d'un accident potentiel.

L'analyse des conséquences doit impérativement :

- Décrire toutes les conséquences des événements indésirables.
- Tenir compte à la fois des effets immédiats et de ceux qui peuvent apparaître après un certain temps surtout en ce qui concerne les nuisances à l'environnement.
- Tenir compte des conséquences secondaires, telles que celles en rapport avec des équipements et systèmes adjacents.

III.4 Vérification

Cette étape est nécessaire à la confirmation de l'intégrité de l'APR, elle permet de s'assurer que les objectifs de sécurité énoncés sont atteignables. Dans un premier temps il faudrait s'assurer que le domaine d'application convient à ces objectifs. Les hypothèses critiques seront révisées afin de s'assurer qu'elles sont crédibles.

Les méthodes, les modèles et les données utilisées peuvent faire l'objet d'une appréciation. Les résultats de l'APR sont à leur tour revus avec la plus grande attention afin de s'assurer de leur conformité et surtout du fait qu'ils ne seraient pas affectés par la manière dont les données sont formatées.

Lorsque des expériences pratiques pertinentes sont disponibles, la vérification peut être effectuée en comparant les résultats de l'APR à des observations directes en se référant aux mécanismes du retour d'expérience.

III.5 Documentation

Le document final relatif à l'APR doit rapporter en détail le processus d'analyse. La portée du rapport dépendra des objectifs de l'analyse. Sauf pour des APR très simples, il convient normalement que la documentation comporte les sections suivantes :

- Les objectifs de l'analyse
- Les limites, hypothèses et la justification des hypothèses
- La description des parties pertinentes du système
- La méthodologie d'analyse
- Les données exploitées et leurs sources
- Les résultats d'identification des dangers
- Les résultats d'estimation du risque

III.6 Mise à jour

Si l'APR est prescrite pour appuyer un processus continu de gestion des risques, il convient qu'elle soit itérative et auto constructive et qu'elle soit réalisée et documentée de façon qu'elle puisse être maintenue pendant tout le cycle en vie du système. Le dossier d'APR reste ouvert pendant tout ce cycle, ainsi de nombreuses nouvelles informations sont éventuellement rajoutées ou modifiées au fur et à mesure.

Conclusion

L'APR est très diversement pratiquée et demeure assez mal définie. Les approches des constructeurs vis-à-vis de l'analyse préliminaire des risques (APR) sont très diverses, les choix de représentation sont variés et les terminologies imprécises ou même parfois contradictoires. Ces derniers suivent chacun sa propre méthodologie avec un vocabulaire, une terminologie et un savoir-faire qui lui sont propres.

La nature générique de la norme rend le processus recommandé difficilement adoptable pour élaborer une APR. L'identification directe du danger sans identifier au préalable l'élément dangereux l'engendrant relève d'une bonne maîtrise du système étudié. Cependant la programmation de l'APR tôt dans le processus de construction du système, et plus précisément entre la phase de spécification et la phase de conception, renvoie cette possibilité. Désormais, les données sur le système à ce stade prématuré de la conception sont incomplètes voire même incertaines.

La deuxième étape selon la norme, en l'occurrence " Identification du danger et évaluation initiale des conséquences" montre que le processus proposé correspond plus à une Analyse de dangers (Hazard Analysis) qu'à une analyse des risques (Risk Analysis).

VILLEMEUR définit l'Analyse Préliminaire des Risques (APR) comme une simple extension de l'Analyse Préliminaire des Dangers (APD): « L'APD est appelée APR lorsqu'elle est complétée par une évaluation des risques » [VILLEMEUR, 1988]. Ça n'est pas vraiment le cas si l'on considère premièrement qu'un risque est associé à un accident potentiel donné, et que deuxièmement un accident potentiel peut être le résultat de plusieurs sources potentielles de dommage et pas forcement d'une seule. Donc l'estimation du risque concerne un ensemble de phénomènes dangereux susceptibles de donner lieu à un accident ou un incident. Théoriquement cet ensemble est infini, néanmoins on se contente souvent d'un sous-ensemble majorant contenant les phénomènes dangereux les plus énergiques.

Dans l'analyse de dangers, on se contente seulement d'identifier les dangers et proposer les mesures nécessaires pour les atténuer. Le concept de « danger » qui est devenu plus tard « phénomène dangereux » est défini comme étant **une source potentielle de dommage**. Dans une analyse des risques préliminaire, on ne se contente pas d'identifier les éventuelles sources susceptibles de causer des préjudices humains, matériels ou environnementaux, mais d'aller plus loin avec la motivation de traquer le risque que représentent les éléments dangereux et d'identifier ou même imaginer les différents scénarios d'accidents potentiels, de leur associer une gravité de dommage et une probabilité d'occurrence.

Dans une Europe ferroviaire qui se veut tenante de méthodes, d'indicateurs et d'objectifs de sécurité communs, il est primordial de définir et arrêter un processus d'APR type fondé sur un langage commun facilitant la coopération en matière d'APR au niveau national et puis au niveau européen.

Nous estimons que la divergence autour des définitions et des concepts de base est très importante. La notion de danger est confondue à celle de risque qui se fait confondre elle-même au niveau de risque. Cette dernière notion est quasi-absente des manuels de maîtrise des risques ou des dossiers d'APR que nous avons étudiés. Par conséquent on parle de risque acceptable au lieu de niveau de risque acceptable, tandis que l'acceptabilité des risques est définie en fonction de l'appartenance de la variable risque à une zone de criticité donnée. Cela revient à dire que le mot risque est un attribut, et que la qualification de son niveau représente une instance donnée.

Actuellement, Nos travaux de recherches s'orientent vers l'amélioration de la pratique de l'APR en remédiant aux lacunes suscitées.

Bibliographie

[CEI, 1995] « Gestion de la sûreté de fonctionnement »
[CEI 300-3-9, première édition 1995]

[ISO/CEI, 1999] « Aspects liés à la sécurité – principes directeurs pour les inclure dans les normes »
[Guide ISO/CEI 51, édition 1999]

[ISO 14971, 2000] « Application de la gestion des risques aux dispositifs médicaux»
[ISO 14971, première édition 2000]

[LIEVENS, 1976] « Sécurité des systèmes »
[C. LIEVENS, 1976]
Edition Cépaduès

[PERROW, 1984] « Normal accident – living with High-Risk technologies »
[C. PERROW, 1984]
BASIC BOOKS, HARPER TORCHBOOKS

[VILLEMEUR, 1988] « Sûreté de fonctionnement des systèmes industriels »
[A. VILLEMEUR, 1988]
Edition Eyrolles

[DESROCHES, 1992] « Une approche optimale de construction de la sécurité d'un système 'la démarche sécuritaire ' »
[A. DESROCHES, 1992]
Institut Européen de Cindyniques, Acte du colloque CANNES 1992

[CENELEC, 1994] « Principes directeurs pour inclure dans les normes les aspects liés à la sécurité»
[CEN - CENELEC, 1994]
MEMORANDUM N°9, Edition N°1

[Hadj-Mabrouk, 1995] « La maîtrise des risques dans le domaine des automatismes des systèmes de transports guidés »
[H. Hadj-Mabrouk, 1995]
Recherche transports sécurité N°49

[Hadj-Mabrouk, 1997] « Projet SAPRISTI : proposition d'une méthode et d'une maquette d'aide à d'élaboration et à la capitalisation des analyses préliminaires de risques »
[H. Hadj-Mabrouk, 1997]

[MOHR, 2002] « Preliminary Hazard Analysis»
[R-R.Mohr, 5th Edition, 2002]

[GONZALES, 1993] « The enginneering of knowledge-based systems, Theory and practice »
[A-J. GONZALES, D-D. DANKEL, 1993]
Prentice Hall, Englewood Cliffs, New Jersey

[TOURIGNY, 1998] « Systèmes d'aide à l'étude de la sécurité routière - Vers des outils hybrides, ouverts et intelligents »
[N. TOURIGNY, 1998]