Sécurité des systèmes de contrôle-commande et signalisation ferroviaire: nouvelle approche d'analyse préliminaire des risques

FATEH GUENAB, JEAN-LOUIS BOULANGER, WALTER SCHON

Heudiasyc, Université de Technologie de Compiègne
Centre de Recherches de Royallieu, BP 20529, 60205 Compiègne Cedex, France

prenom.nom@hds.utc.fr

Résumé — L'analyse préliminaire des risques (APR) est une méthode qualitative de la sûreté de fonctionnement. Elle est essentiellement utilisée au stade préliminaire de la conception du système pour mieux le connaître de manière à déterminer les scénarios d'accidents potentiels, évaluer leurs probabilités d'occurrence ainsi que la gravité des conséquences résultants et proposer des solutions (mesures préventives et/ou de protection) afin de réduire le niveau de risque en terme de gravité/occurrence. L'APR a été largement utilisée dans plusieurs domaines industriels (aéronautique, militaire, chimique, ferroviaire,…) afin d'étudier la sécurité des systèmes. D'un domaine à l'autre, d'un expert à l'autre de nombreuses démarches et méthodes extrêmement différentes sont utilisées pour effectuer cette analyse. En outre, les formats représentant les résultats de l'APR sont souvent variés ainsi que la terminologie et les concepts liés aux APR.

L'objectif de ce travail, réalisé dans le cadre du projet ANR-PREDIT-SECUGUIDE[1], est de proposer une démarche et un contenu type pour une APR dans le contexte des systèmes ferroviaires en prenant en compte l'utilisation des Nouvelles Technologies de l'Information et de la Communication (NTIC).

Mots clés — Sécurité ferroviaire, Analyse Préliminaire des Risques (APR), événement redouté, accident potentiel, risque, Systèmes de contrôle-commande et signalisation, Nouvelles Technologies de l'Information et de la Communication (NTIC).

I. INTRODUCTION

La mise en sécurité des systèmes ferroviaires nécessite la maîtrise de toutes les phases du cycle de vie de ces systèmes. Les phases amont et aval du cycle de vie (Concept, Définition du Système et de ses Conditions d'Application, Acceptation du Système, Exploitation et Maintenance, Surveillance des Performances, Modification et Remise à Niveau, Retrait et Dépose) sont essentiellement de la responsabilité des exploitants et des autorités de tutelle. Les phases centrales du cycle de vie (Analyse de Risques, Exigences du Système, Allocation des Exigences, Conception et Réalisation, Fabrication, Installation, Validation du Système) sont essentiellement de la responsabilité des Industriels fournisseurs des systèmes ferroviaires. Dans le cadre d'affaires réalisées à l'export, les industriels prennent également de plus en plus de responsabilités dans les phases amont et aval. Les phases correspondant aux transferts de responsabilités entre acteurs sont évidemment cruciales.

Les normes ferroviaires actuelles ([1], [2] et [3]) ont été régulièrement révisées pour tenir compte des avancées technologiques permanentes dans le domaine des matériels électroniques et celui des techniques informatiques. Celles-ci ont un impact important sur la conception des systèmes ferroviaires. Cependant les normes n'ont pas encore bien formalisé le processus de distribution des prescriptions de sécurité du système ferroviaire sur les différents sous-systèmes, matériels et logiciels qui les supportent. En d'autres termes, si les risques sont bien identifiés et suivis au travers des démonstrations et justifications de sécurité, il reste à améliorer la démarche d'Analyse des Risques et d'Allocation des Exigences.

L'objectif de ce travail est de proposer, dans un premier temps, une démarche et un contenu type pour une APR dans le contexte des systèmes de contrôle-commande et signalisation de systèmes ferroviaires. Cette méthode intégrera l'impact des NTIC sur la sécurité en termes de risques induits par les NTIC.

L'évolution de la conception des systèmes passe par l'intégration des NTIC. La principale caractéristique des NTIC est d'être des composants sur étagères (COTS). Les COTS permettent une maîtrise du coût de réalisation du système, mais en contrepartie il y a une perte de la maîtrise de leurs sécurités (voir [6]). C'est pourquoi, la démarche proposée devra prendre en compte les risques inhérents à ce type de composant. Une autre contrainte concerne la prise en compte des erreurs humaines.

Ce papier est organisé comme suit. Les abréviations utilisées sont données dans la section 2. La section 3 est consacrée aux définitions des colonnes de l'APR. Une méthodologie de mise en œuvre de l'APR est proposée dans la section 4. La section 5 est consacrée à la description des phases de la méthodologie APR présentée précédemment. La dernière section est consacrée aux conclusions et perspectives.

[1] Le projet ANR-PREDIT-SECUGUIDE est un projet financé par l'ANR (www.anr.fr) qui a débuté en janvier 2006 pour une durée de 3 ans. Le projet a pour objectif d'étudié l'impact de l'introduction des NTIC dans les systèmes ferroviaires sur la sécurité-innocuité.

II. ABREVIATIONS

APR	Analyse Préliminaire des Risques
APD	Analyse Préliminaire des Dangers
CENELEC	Organisme composé des comités électrotechniques nationaux d'une quinzaine de pays de l'Europe occidentale, membres de la Commission électrotechnique internationale (CEI). Le CEN et le CENELEC forment ensemble une institution de normalisation européenne (CEN/CENELEC) qui promulgue des normes européennes (EN)
COTS	Composants sur étagères (Components Off The Shelf)
ER	Evénement Redouté
NTIC	Nouvelles Technologies de l'Information et de la Communication
FMDS	Fiabilité, Maintenabilité, Disponibilité, Sécurité
REX	Retour d'expérience

III. DEFINITIONS DES COLONNES DE L'APR

Sachant que les résultats de l'analyse préliminaire de risques sont présentés dans un tableau à colonnes et compte tenu des différentes définitions des termes et concepts liés à l'APR nous consacrons cette section pour détailler ces concepts. En se basant sur les normes [1], [2], [3] et [4], nous proposons les définitions des colonnes d'une APR appliquée aux systèmes de contrôle-commande ferroviaires. Une normalisation des principaux concepts et de la terminologie associé s'est en effet avérée nécessaire après étude de plusieurs APR ferroviaires de provenances diverses (industriels, exploitants…), ou des incohérences importantes (utilisation d'un même mot pour un concept différent par exemple) ont pu être constatées.

- **Mode de fonctionnement** (ou mode d'utilisation, ou mode d'exploitation, ou phase ou contexte) : sachant que l'analyse de dangers et de risques est effectuée pour toutes les situations raisonnablement prévisibles, cette colonne est nécessaire. Il est par exemple inutile d'envisager un scénario « vanne bloquée fermée » pour une vanne qui doit être ouverte en permanence pour le mode de fonctionnement choisi. Ou encore envisager une mesure de couverture « les portes palières doivent être strictement fermées » pour un métro qui est en ligne, voire en station où les portes palières n'existent pas ou en mode dégradé (portes palières bloquées ouvertes)... Dans certains cas, il n'est toutefois pas obligatoire de préciser le mode de fonctionnement.
- **Entité dangereuse** (ou sous-ensemble en cause/ à l'origine) : un sous ensemble du système étudié qui est à l'origine de l'événement redouté, c'est la cause initiale du scénario étudié. La fonction en cause ou la fonction de l'entité dangereuse peut être précisée si nécessaire.
- **Evénement redouté** (ou événement causant une situation dangereuse, ou événement indésirable, ou panne, ou erreur, ou cause de défaillance) : est un événement dangereux, c'est l'événement affectant l'entité dangereuse ou la fonction en cause de l'entité dangereuse conduisant le système en une situation dangereuse.
- **Situation dangereuse** ou danger : état indésirable du système suite à l'événement redouté, pouvant conduire à un accident potentiel.
- **Dommage** ou conséquence : c'est le résultat d'un accident donné en termes de décès ou blessure physique ou une atteinte à la santé des personnes ou dégât causé aux biens ou à l'environnement.
- **Gravité:** une classification sur une échelle à plusieurs niveaux permettant d'évaluer et d'estimer les conséquences des accidents potentiels. D'après [1], le tableau (1) présente une description des niveaux types de gravité des accidents potentiels ainsi que les conséquences liées à chaque niveau de gravité. Afin d'éviter de mauvaises interprétations des termes qualitatifs, certains industriels ou exploitants utilisent des numéros pour les différents niveaux de gravité (de 1 à 4 par ordre de gravité croissante 4 = catastrophique).

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 grave 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

Tableau 1. Niveau de gravité des situations dangereuses

- **La probabilité d'occurrence** : la probabilité des séquences d'événements. Une évaluation qualitative [1] des probabilités est proposée dans présentée par le tableau (2).

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

Tableau 2. Fréquence d'un événement dangereux

- **Les mesures de couverture** (ou mesures de sécurité ou contraintes de sécurité ou exigences de sécurité) **:** Les moyens et actions susceptibles de réduire ou d'éliminer les

risques. Elles peuvent être des mesures préventives permettant de réduire les probabilités d'occurrences des événements dangereux (événement redouté et événement causant un accident potentiel) ou des mesures de protection en utilisant des dispositifs de protection permettant de réduire la gravité des dommages et ainsi protéger la cible (humain, système, environnement). Cette colonne peut décrire le sous-système (équipement, système,…) chargé d'assurer les mesures de sécurité (entité responsable de la réduction du risque) et sa référence.

- **Evénement causant un accident potentiel** : c'est un événement dangereux qui transforme une situation dangereuse en un accident potentiel. Il n'existe pas dans le cas des scénarios d'ordre 1. Des colonnes peuvent figurer dans l'APR, pour les séquences des événements dangereux permettant de passer d'une situation dangereuse à un accident, ceci dépend de l'ordre du scénario étudié.
- **Accident potentiel** : Un accident potentiel peut être un accident ou un incident. L'occurrence des dommages attribue l'identité accidentelle à l'accident potentiel sinon il est un incident. Sachant qu'un accident est un événement ou série d'événements inattendus conduisant au décès, à des blessures, à la perte d'un système ou d'un service, ou à des dommages sur l'environnement.

IV. METHODE PROPOSEE

Rappelons que l'objectif de l'APR est [5] :

- De déterminer les dangers et ses causes (entités dangereuses, situations dangereuses, accidents potentiels)
- D'évaluer la gravité des conséquences des situations et des accidents précédemment déterminés
- D'en déduire les moyens et les actions susceptibles d'éliminer ou de maîtriser les situations dangereuses et les accidents potentiels

La figure (1) en résume les étapes. L'identification des entités dangereuses, des situations dangereuses et des accidents potentiels repose au départ sur l'expérience et le jugement des spécialistes, aidés par des listes guide qui sont mises à jour par le retour d'expérience tout au long du cycle de vie du système.

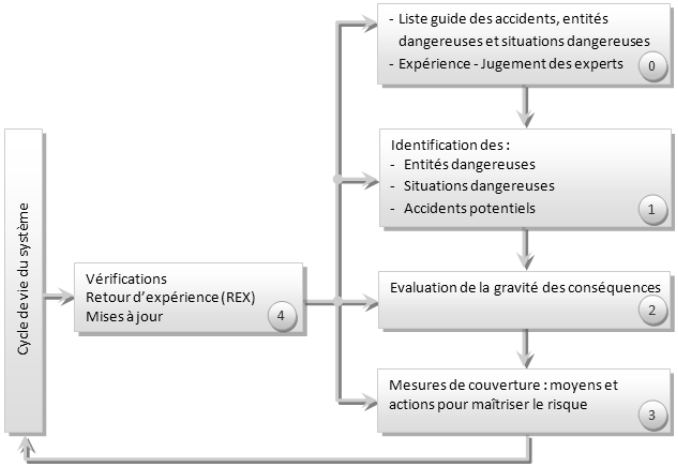

Figure 1. Les étapes de l'APR

L'APR est le plus souvent considérée comme une démarche inductive (depuis les événements redoutés vers les accidents potentiels), cependant certains acteurs la considèrent déductive. Une manière déductive ou inductive ne concerne pas la démarche générale décrite par la figure (1) mais uniquement l'étape (1) : identification des entités dangereuses, situations dangereuses et accidents potentiels. Lors de cette étape, certains experts déterminent les accidents potentiels par induction en partant des entités dangereuses (événements redoutés), d'autres experts utilisent une méthode déductive partant depuis les accidents potentiels pour déterminer les événements dangereux. Quand nous disposons d'une liste complète de tous les accidents potentiels (respectivement événements redoutés) la démarche déductive (respectivement inductive) toute seule est valable et conduit à des résultats acceptables couvrant tous les scénarios possibles. En revanche pour un système possédant un nombre important de scénarios et dans le cas où nous ne disposons pas de listes complètes des accidents potentiels (respectivement événements redoutés), utiliser la démarche déductive (respectivement inductive) seule n'est pas efficace. Dans ces cas, on risque de ne pas prendre en compte les accidents (respectivement événements redoutés) non cités dans la liste générique. Pour avoir des résultats complets, il faut utiliser une démarche déductive/inductive.

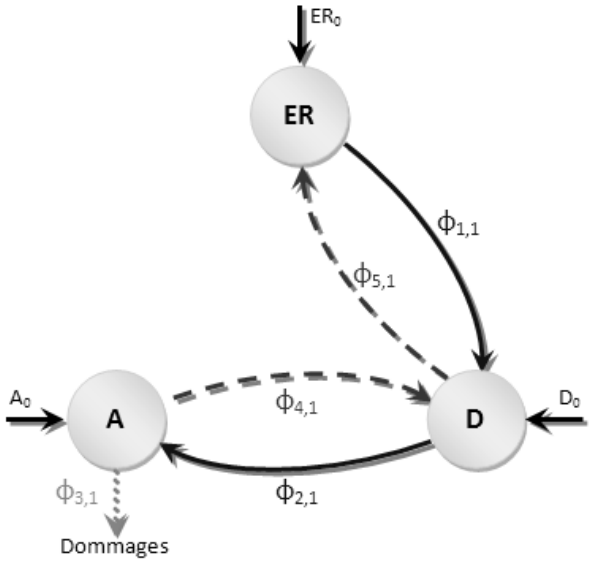

Figure 2. Démarche d'identification des événements redoutés, des dangers, des accidents potentiels et des dommages

La figure (2) représente l'étape (1) de l'APR de la figure (1).

- **ER_0**, **D_0** et **A_0** sont les listes préliminaires (initiales) des événements redoutés, des dangers et des accidents potentiels respectivement. Elles sont définies à partir des listes génériques analysées par des experts, ces derniers peuvent supprimer des scénarios incohérents ou rajouter autres scénarios manquants. Nous considérons que nous disposons de ces listes à l'issu de l'étape d'initialisation (étape (0) de figure (1)).
- **ER**, **D** et **A** représentent les listes des événements redoutés, des dangers et des accidents potentiels respectivement. Au début de l'analyse elles sont initialisées à **ER_0**, **D_0** et **A_0** et elles contiennent les listes définitives à la fin de l'analyse.
- La démarche contient plusieurs phases cycliques : deux phases inductives (ligne continue), deux autres déductives (ligne discontinue) et une phase pour générer la liste des

dommages engendrés par les accidents potentiels (ligne en pointillé). Les phases sont notées $\phi_{i,j}$:

Où l'indice « *i* » indique le numéro de phase et l'indice « *j* » indique le cycle en cours. i.e. $\phi_{4,1}$ est la 4ème phase du cycle 1.

- Les cycles commencent par l'index 1 (j > 0), autrement dit, le premier cycle de cette étape correspond à « j = 1 ».
- Au début d'un cycle « *j* », les ensembles des événements redoutés, des dangers et des accidents potentiels sont indexés par « *j-1* », $\mathbf{ER_{j-1}}$, $\mathbf{D_{j-1}}$ et $\mathbf{A_{j-1}}$. Par exemple qu'au début du cycle 1 les listes **ER**, **D** et **A** sont égales à $\mathbf{ER_0}$, $\mathbf{D_0}$ et $\mathbf{A_0}$ respectivement.

V. DEMARCHES DE LA METHODE

Dans ce paragraphe nous allons présenter les différentes phases de la méthode APR présentée dans le paragraphe précédent.

Au début du cycle 1, les listes des événements redoutés, des dangers et des accidents potentiels sont initialisées à $\mathbf{ER_0}$, $\mathbf{D_0}$ et $\mathbf{A_0}$ et représentées par la figure suivante :

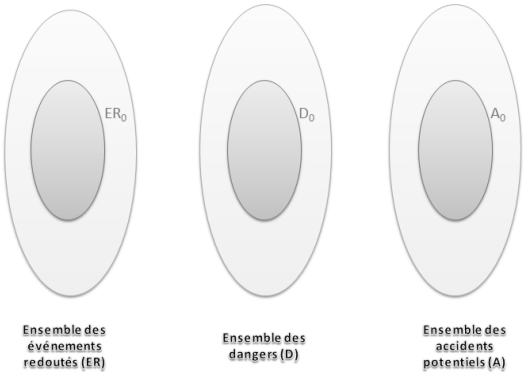

Figure 3. Les listes ER, D et A au début du cycle 1

La phase 1 permet de déterminer les dangers à partir des événements redoutés (phase inductive).

Lors de cette phase, la liste $\mathbf{ER_0}$ peut générer une liste de dangers correspond à :

- Une partie de la liste préliminaire notée $\mathbf{D_0^{'}} \subseteq \mathbf{D_0}$. On note par $\mathbf{D_0^{''}}$ la partie restante de la liste préliminaire $\mathbf{D_0}$.
- **Et** une nouvelle liste de dangers notée $\mathbf{D_0^{'n}}$ qui est ajoutée à la liste préliminaire.

A l'issue de cette phase, la nouvelle liste des dangers est $\mathbf{D_0} \cup \mathbf{D_0^{'n}}$ ou $\mathbf{D_0^{'}} \cup \mathbf{D_0^{''}} \cup \mathbf{D_0^{'n}}$. La seule sous-liste de dangers qui n'a pas de correspondance dans la liste des événements redoutés est $\mathbf{D_0^{''}}$.

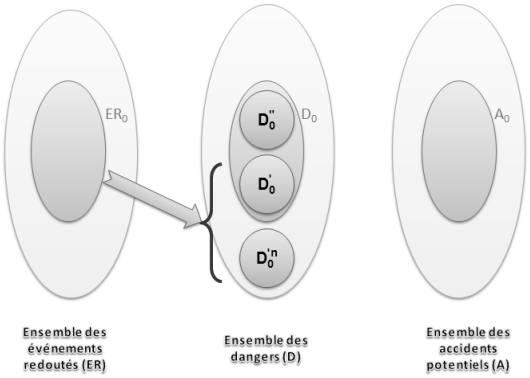

Figure 4. Phase 1

La phase 2 permet de déterminer les accidents potentiels à partir des dangers (phase inductive).

Lors de cette phase, la liste des dangers issue de la phase précédente $\mathbf{D_0} \cup \mathbf{D_0^{'n}}$ permet de générer une liste d'accidents potentiels correspond à :

- Une partie de la liste préliminaire notée $\mathbf{A_0^{'}} \subseteq \mathbf{A_0}$. Notons $\mathbf{A_0^{''}}$ par la partie restante de la liste préliminaire des accidents.
- Et une nouvelle liste d'accidents notée $\mathbf{A_0^{'n}}$, elle est ajoutée à la liste préliminaire.

A l'issue de cette phase, la nouvelle liste des accidents est $\mathbf{A_0} \cup \mathbf{A_0^{'n}}$ ou $\mathbf{A_0^{'}} \cup \mathbf{A_0^{''}} \cup \mathbf{A_0^{'n}}$.

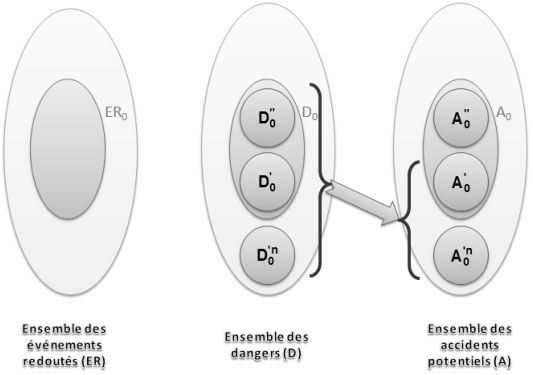

Figure 5. Phase 2

La phase 3 sert à identifier les dommages à partir de la liste des accidents obtenue à l'issue de la phase précédente ($\mathbf{A_0^{'}} \cup \mathbf{A_0^{''}} \cup \mathbf{A_0^{'n}}$). On la note $\mathbf{DOM_1}$.

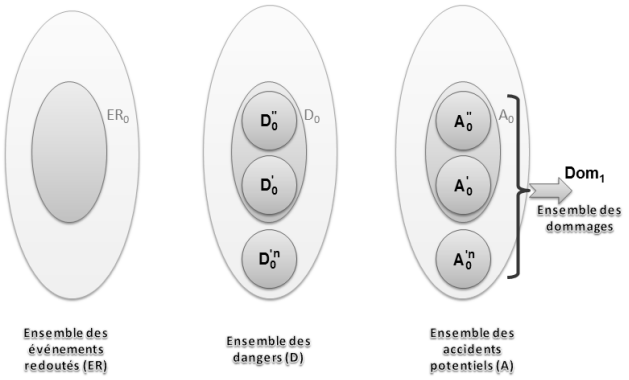

Figure 6. Phase 3

La phase 4 : Sachant que la seule sous-liste des accidents potentiels qui n'a pas de correspondance dans la liste des dangers est $\mathbf{A_0^{''}}$. Cette phase permet de déterminer les dangers possibles à partir de la sous-liste $\mathbf{A_0^{''}}$ (phase déductive). Notons par $\mathbf{D_0^{''n}}$ la nouvelle liste de dangers obtenue.

A l'issue de cette phase, la nouvelle liste des dangers est $\mathbf{D_0 \cup D_0^{'n} \cup D_0^{''n}}$ ou $\mathbf{D_0^{'} \cup D_0^{''} \cup D_0^{'n} \cup D_0^{''n}}$.

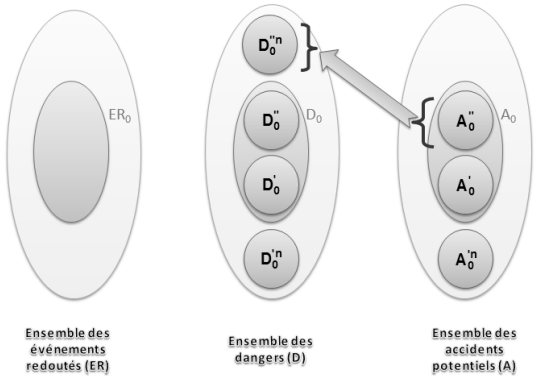

Figure 7. Phase 4

La phase 5 : Cette phase permet de déterminer la liste des événements redoutés à partir des dangers (phase déductive). La sous-liste des dangers qui n'a pas de correspondance dans la liste des événements redoutés est $\mathbf{D_0^{''} \cup D_0^{''n}}$. On note par $\mathbf{ER_0^{'n}}$ la liste des événements redoutés obtenue à l'issue de cette phase et qui correspond à la liste des dangers $\mathbf{D_0^{''} \cup D_0^{''n}}$.

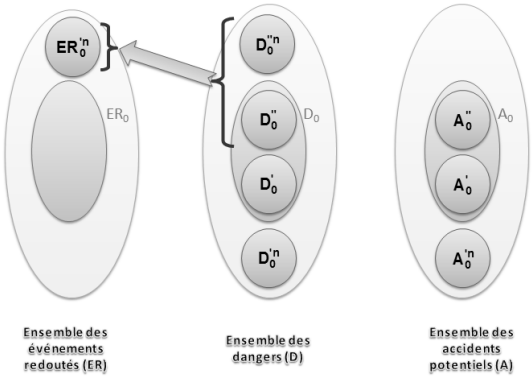

Figure 8. Phase 5

A la fin du cycle 1, les listes **ER**, **D** et **A** sont données comme suit :

$$\mathbf{ER_1 = ER_0 \cup ER_0^{'n}}$$

$$\mathbf{D_1 = D_0 \cup D_0^{'n} \cup D_0^{''n} = D_0^{'} \cup D_0^{''} \cup D_0^{'n} \cup D_0^{''n}}$$

$$\mathbf{A_1 = A_0 \cup A_0^{'n} = A_0^{'} \cup A_0^{''} \cup A_0^{'n}}$$

A partir de ces nouvelles listes, on refait un nouveau cycle avec les mêmes phases décrites. Une condition nécessaire et suffisante pour arrêter l'analyse si au cours d'un cycle quelconque définis par l'indice $j = f$:

- La phase $\phi_{1,f}$ ne génère plus de nouveau danger.

Et

- La phase $\phi_{2,f}$ ne génère plus de nouvel accident potentiel.

D'une autre manière :

- $\mathbf{D_{f-1}^{'n}} = \emptyset$ et $\mathbf{A_{f-1}^{'n}} = \emptyset$. (par exemple, au cours du cycle **1**, on arrête l'analyse si les deux listes $\mathbf{D_0^{'n}} = \emptyset$ et $\mathbf{A_0^{'n}} = \emptyset$).

Notons que l'analyse peut être commencée en partant des accidents potentiels pour arriver aux événements redoutés (sens inverse du cycle). Ceci en inversant l'ordre des phases de la façon suivante : on commence par les phases 4 et 3, la phase 5, ensuite la phase 1 et on finit par la phase 2

VI. CONCLUSION

Dans ce papier, nous avons présenté une méthode d'analyse préliminaire des risques (APR) dans le contexte des systèmes ferroviaires. Dans un premier temps, les définitions des termes utilisés dans une APR sont présentées. Ensuite nous avons proposé une méthode APR utilisant les deux approches déductive et inductive. Nos perspectives de recherche s'articulent au tour de deux points :

– Proposer un contenu type de l'analyse préliminaire des risques et développer une méthode d'analyse pour ce qui est des aspects contrôle commande et signalisation (aspects NTIC) de systèmes ferroviaires.

– Formaliser les liens entre les fonctionnalités et/ou techniques relevant des NTIC et l'APR type, dans le but d'identifier les nouveaux risques induits par les NTIC ainsi que les mesures de sécurité à prendre.

VII. REFERENCES

[1] **EN 50126 :** « Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) ». CENELEC. Septembre 1999.

[2] **EN 50128 :** « Applications ferroviaires – Systèmes de signalisation, de télécommunications et de traitement – Logiciels pour système de commande et de protection ferroviaire ».

[3] **EN50129 :** « Applications ferroviaires – Systèmes de signalisation, de télécommunications et de traitement – Systèmes électroniques de sécurité pour la signalisation ».

[4] **EN 61508-4 :** «Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité. Partie 4 : définitions et abréviations.»,

[5] A. Villemeur, « Sûreté de fonctionnement des systèmes industriels : fiabilité-facteurs humains informatisation », 1988, EYROLLES.

[6] J.L. Boulanger et W. Schön, « Référence systems and standards for safety assessment of railway applications », ESREL 2007, Stavanger, Norway, pages 2609-2613.