GESTION DU RISQUE ET GOUVERNANCE

Mounir SARRAJ (*), **Habib HADJ MABROUK** (**) **Ahmed MAALEL** (***)
rams@planet.tn, ,mabrouk@inrets.fr, maalel.ahmed@gmail.com

(*)Faculté de Droit et des Sciences Economiques et Politiques de Sousse, (Tunisie),
(**)INRETS, Institut National de Recherche sur les Transports et leur Sécurité, (France)
(***)Laboratoire RIADI GDL – Ecole Nationale des Sciences de l'informatique, (Tunisie)

Mots clefs :
Veille scientifique et technologique, Sûreté de fonctionnement, Sécurité, Systèmes intelligents, Gouvernance
Keywords:
Scientific and technical observation, Reliability, Safety, Systems intelligent, Gouvernance
Palabras clave:
Escudriñar científico y tecnológico, Confianza, Seguridad, Sistemas Inteligentes, Gobernabilidad

Résumé

Cet article propose une nouvelle approche méthodologique qui prend en considération la méthode d'analyse préliminaire des risques en vue de prendre d'une manière conjointe l'aspect économique et technologique rarement pris en considération au sein des entités économiques, l'originalité de cet article réside au niveau de la prise en compte de la complémentarité de ces deux aspects , la création de la valeur ne peut être omise vue qu'elle conditionne le renforcement de toute recherche visant à assurer la sûreté de fonctionnement d'un système et notamment la composante sécurité obéissant un optimum du couple sécurité/Coût dont la matérialisation n'est possible qu'a travers des systèmes d'aide à la décision dits « Systèmes intelligents ».

Introduction :

La sûreté de fonctionnement d'un système (SdF) est définit comme la qualité du service délivré par un système, qualité telle que les utilisateurs de ce service puissent placer une confiance justifiée dans le système qui le délivre [1] Son objectif est alors de connaitre et de maitriser les risques de dysfonctionnement des produits et systèmes complexes, notamment leur fiabilité en mettant en œuvre des méthodes prévisionnelles, expérimentales et opérationnelles appropriées [3]. Le terme "sûreté de fonctionnement", inventé voici trente ans pour englober plusieurs concepts, n'a pas d'équivalent exact en langue anglaise. En France, la sûreté de fonctionnement d'un système à risque s'articule autour de quatre principales composantes, à savoir : la fiabilité, la disponibilité, la maintenabilité et la sécurité. . [2]

- **La fiabilité :** aptitude d'un système à rester constamment opérationnel pendant une durée donnée.
- **La disponibilité :** aptitude d'un système à être opérationnel au moment où il est sollicité. C'est une notion importante pour un appareil de sécurité tel qu'un disjoncteur par exemple. Une disponibilité importante est compatible avec une fiabilité faible, pour peu que l'appareil puisse être réparé très rapidement.
- **La maintenabilité :** c'est l'aptitude d'un système à être remis rapidement dans un état opérationnel. Ainsi les systèmes dont les composants sont très facilement démontables peuvent bénéficier d'une meilleure maintenabilité que les autres.
- **La sécurité :** c'est l'aptitude d'un système à ne pas connaître de pannes considérées comme catastrophiques pendant une durée donnée.

En outre, l'évolution technologique a contribué à l'apparition d'autres attributs à savoir : la qualité, l'ergonomie et les facteurs humains.

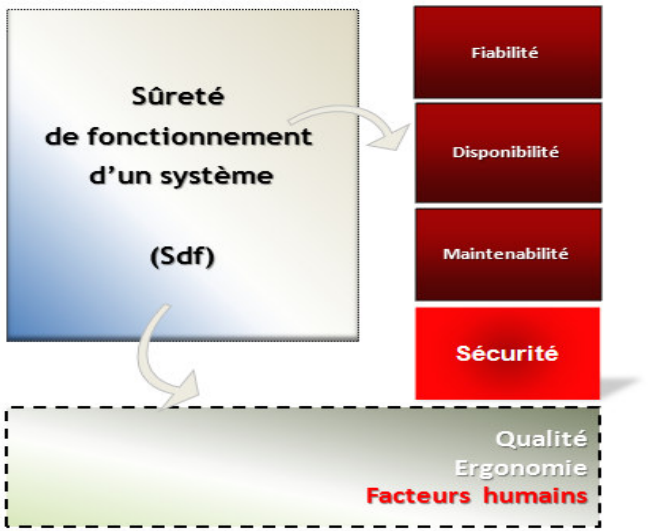

Figure 1 : Composants de base de la Sûreté de fonctionnement (SdF) (hhm)

1. La sécurité

La norme européenne CENELEC 50129 [3] définit la sécurité par « l'absence de tout niveau de risque inacceptable ». Le risque fait intervenir de manière conjointe et complémentaire deux paramètres : la probabilité d'occurrence des accidents potentiels et la Gravité des dommages engendrés par ces accidents potentiels sur l'environnement, le système et l'homme ; ainsi que leurs interactions mutuelles. On parle généralement de matrice Gravité/Occurrence pour identifier et évaluer le niveau d'acceptabilité du risque.

2.1. Principes de sécurité

En Europe, on distingue trois grands principes de sécurité. En Allemagne, on applique le principe MEM (Minimum Endogenous Mortality) qui prétend qu'on continue à améliorer le niveau de sécurité si seulement si le taux de mortalité dues aux faits technologiques (exogène à l'organisme) soit inférieur au taux de mortalité endogène (dans un lieu et un espace de temps déterminé). Au Royaume-Uni, le principe est plutôt d'ordre économique. En effet, le principe ALARP (As Low As Reasonably Practibale) y appliqué exige qu'un niveau de risque est acceptable si le cout dû à la réduction du risque est disproportionné en regard du gain d'amélioration. Apparu dans le décret 30 mars 2000, GAME (Globalement Au Moins Equivalant) est le principe retenu par le comité européen. Ce principe stipule que le niveau de sécurité d'un nouveau système doit être au moins équivalent à celui d'un système comparable déjà existant et réputé sûr.

2.2. Principe GAME

Or la composante cruciale principale c'est la sécurité des systèmes sociotechniques qui est définit selon la norme européenne 50129 [3] par l'absence de tout niveau au du risque inacceptable. Le risque zéro n'existe pas mais l'objectif est de rester dans un niveau du risque acceptable [11] . conformément à la réglementation en vigueur le niveau du risque doit obéir s'aligner au principe GAME globalement au moins équivalent qui a été retenu en Europe, autrement dit lorsqu'on doit développer un système sociotechnique , la notion de globalement au moins équivalent revient à dire : lors de développement d'un système ; on exige que le niveau de risque soit globalement au moins équivalent à un système déjà homologué et certifié et réputé sure , par exemple en France on fait appel au métro parisien pour atteindre cet object en ayant recours aux statistiques des accidents du métro parisien, dans ce contexte. Néanmoins, ce principe GAME pose au moins une question qui demeure sans réponse :

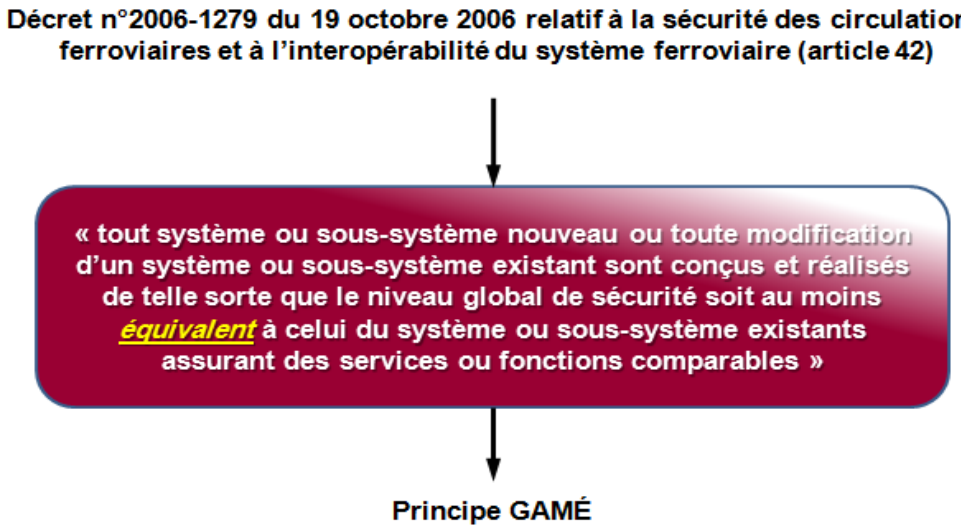

Figure 2. : Principe GAME [11]

C’est quoi un système comparable réputé sur ? Pour apporter un élément de réponse à ce problème on fait généralement appel au retour d’expérience (Rex), le paragraphe suivant sera consacré à la présentation de retour d’expérience.

2. Le retour d’expérience :

La première phase du processus de construction du retour d’expérience s’intéresse à l’énumération de toutes les anomalies rencontrées et le recueil maximal des données. La collecte concerne ainsi les données relatives essentiellement à l’opérateur humain, à son environnement interne et externe et notamment au système technique [4]. La deuxième phase, l’Analyse, répond au principe « comprendre » permet de mieux cerner les mécanismes générateurs des événements affectant la sécurité. Vient juste après la phase de stockage, la mémorisation et l’archivage des données collectées et analysées dans une base de données grâce, souvent, à un outil informatique. La phase suivante correspond à l’exploitation autrement dit l’utilisation et l’interprétation des résultats issus des différents informations dont l’objectif principal est d’extraire l’événement réellement prédictif, de prendre en considération les cas isolés et de prédire ou d’imaginer les futurs scénarios d’accidents ou événements non pris en compte. Enfin la dernière phase de recommandations qui consiste à éclairer et identifier les mesures de préventions et de protections adéquates pour limiter la reproduction d’un événement d’insécurité. Il s’agit de mieux tirer profit des enseignements de l’expérience acquise pour améliorer la sécurité

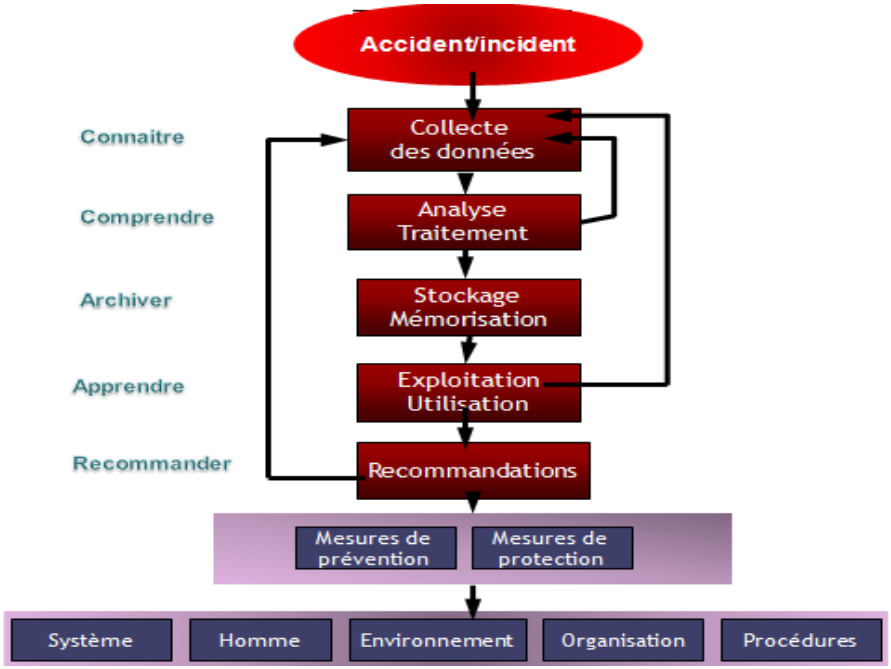

Figure 3. Articulation des différentes étapes de déroulement du Rex [4]

3. Le risque :

3.1. La notion de risque

Quel que soit la définition, la notion de risque est toujours associée aux notions de responsabilité, dommages, événements indésirables, gravité. La définition retenue est celle du Management de risques projets : «le risque est un danger ou inconvénient possible ou probable dont on peut mesurer l'occurrence et la gravité » [1].
Quel que soit l'activité ou le domaine considéré, la perte humaine, matérielle ou financière peut être perçue comme la conséquence d'un accident lui-même aboutissement d'un scénario d'accident décrit par trois événements séquentiels « présence d'un danger », «situation dangereuse ou accidentelle » et« accident » Ces trois événements doivent être considérés comme des états du système ou de son environnement. Un danger est le premier maillon d'un scénario d'accident en absence de danger, on ne peut pas identifier d'événements conduisant à des situations dangereuses. La situation dangereuse est le deuxième maillon d'un scénario d'accident, il correspond à un état instable mais irréversible. Le risque est la mesure de l'instabilité de la situation dangereuse ou menaçante et de potentialité d'accident, c'est un danger éventuel plus ou moins prévisible qui peut affecter l'issue du projet. Il ne sera possible de tous les éliminer, car le risque zéro n'existe pas. Il est néanmoins possible de diminuer les risques en choisissant des technologies plus sûres en améliorant la prévention en exigent la transparence de l'information en matière de risque.

3.2. Les différents types de risque

La classification des risques est pertinente dans la mesure où elle permet de cerner de manière précise la notion des risques. Les risques peuvent être liés à la nature ou à l'environnement. C'est notamment le cas de toutes les catastrophes dites «naturelles » : tremblement de terre, inondations, changements climatiques. Les risques peuvent être également liés plus spécifiquement à l'activité industrielle et aux nouvelles technologies. Enfin les risques peuvent aussi toucher le secteur économique et plus particulièrement dans des aspects financiers, juridiques ou sociaux. On distingue essentiellement ces principaux risques : [5]

- Les risques technologiques
- Les risques naturels
- Les risques humains
- Les risques financiers
- Les risques environnementaux

3.3. Triangle de risque :

Dans un système sociotechnique, la gestion de risque implique la prise en compte d'une manière conjointe et complémentaire de trois composantes essentiels l'environnement, l'homme et le système et l'interaction entre eux. Ces trois composantes contribuent à la génération de l'accident. [6]

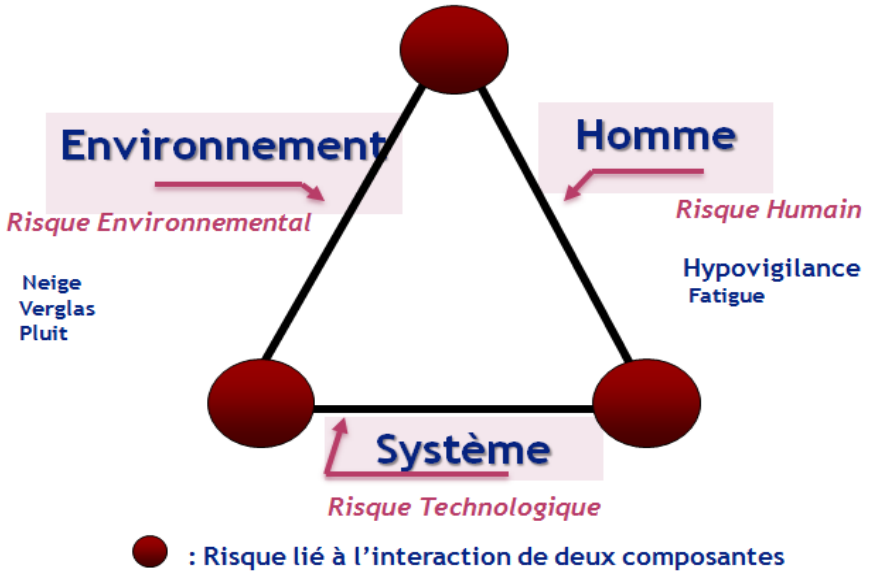

Figure 4. Triangle de risque [6]

4.2 Matrice gravite/ occurrence :

4.2.1 Niveau de probabilité de l'accident potentiel

Les normes en matière de sécurité des transports tentent à définir l'ensemble des niveaux de probabilité d'occurrence sans prendre en compte le type d'analyse de sécurité dans lequel ces niveaux seront employés. Elles visent à proposer une échelle quantitative pour des probabilités dont la quantification est énormément complexe. Néanmoins, la norme EN 50126 [7] propose des probabilités quantitatives, d'où la probabilité d'occurrence d'un événement peut être :

- ***Fréquent (A) :*** surviendra probablement souvent. Le risque de concrétisation du danger sera continuellement présent. **($P > 10^{-3}$)**
- ***Probable (B) :*** surviendra plusieurs fois. Le danger se concrétisera fréquemment.
($10^{-3} > P > 10^{-4}$)
- ***Occasionnel (C) :*** surviendra probablement plusieurs fois au cours de la vie de système. Le danger se concrétisera plusieurs fois. **($10^{-4} > P > 10^{-5}$)**
- ***Rare (D) :*** surviendra probablement au cours de la vie du système. On peut raisonnablement s'attendre à la concrétisation de ce danger. **($10^{-5} > P > 10^{-7}$)**
- ***Improbable (E) :*** peu probable mais possible. On peut admettre que ce danger se concrétisera exceptionnellement. **($10^{-7} > P > 10^{-9}$)**
- ***Hautement improbable :*** Extrêmement improbable. On peut admettre que ce danger ne se concrétisera pas. **($10^{-9} > P$)**

3.3.2. Niveau de gravité des dommages engendrés par l'accident potentiel

Les normes classifient les niveaux de gravité des dommages engendrés par l'accident potentiel sur trois niveaux : selon les dommages aux personnes, au système et à l'environnement. Considérant les conséquences sur les personnes, la norme EN 50126[7] propose quatre niveaux de gravité des dommages :

- ***Catastrophique :*** plusieurs blessés graves ou plusieurs morts.
- ***Grave :*** un blessé grave ou un mort
- ***Signifiant :*** un blessé léger
- ***Insignifiant :*** ni blessé, ni mort.

A noter que cette norme différencie les dommages dus à des accidents individuels de ceux qui résultent d'accidents collectifs.

3.3.3. Niveau de risque

Généralement, il existe une confusion entre le risque et le niveau de risque. En effet, le niveau de risque identifie la combinaison du niveau de probabilité d'occurrence de l'accident potentiel ainsi que le niveau de gravité des dommages engendrés par cet accident potentiel ; d'où plusieurs classifications apparaissent. La norme EN 50126 [7] identifie 4 niveaux de risque :

- ***Risques intolérables :*** doivent être éliminés
- ***Risques non souhaitables :*** « ne peuvent être acceptés, avec l'accord du Responsable Sécurité, que si l'on ne peut pas réduire le risque »
- ***Risques tolérables :*** « acceptables, avec l'accord du Responsable Sécurité, et moyennant des précautions appropriées »
- ***Risques négligeables :*** « acceptables, avec l'accord du Responsable Sécurité »

A partir de ces définitions, les différentes normes recommandent la mise en place d'une matrice gravité/occurrence pour évaluer le risque ; d'où la matrice suivante identifiée par la même norme en vigueur :

		Niveau de gravité des dommages			
		Catastrophique	Grave	Signifiant	Insignifiant
Niveau de probabilité d'occurrence de l'accident potentiel	Fréquent				
	Probable				
	Occasionnel				
	Rare				
	Improbable				
	Hautement improbable				

Risque intolérable
Risque non souhaitable
Risque tolérable
Risque négligeable

Figure 5 Matrice gravité/occurrence [10,11]

La figure suivante présente les principaux termes retenus ainsi que l'articulation des paramètres descriptifs d'une analyse préliminaire des risques.

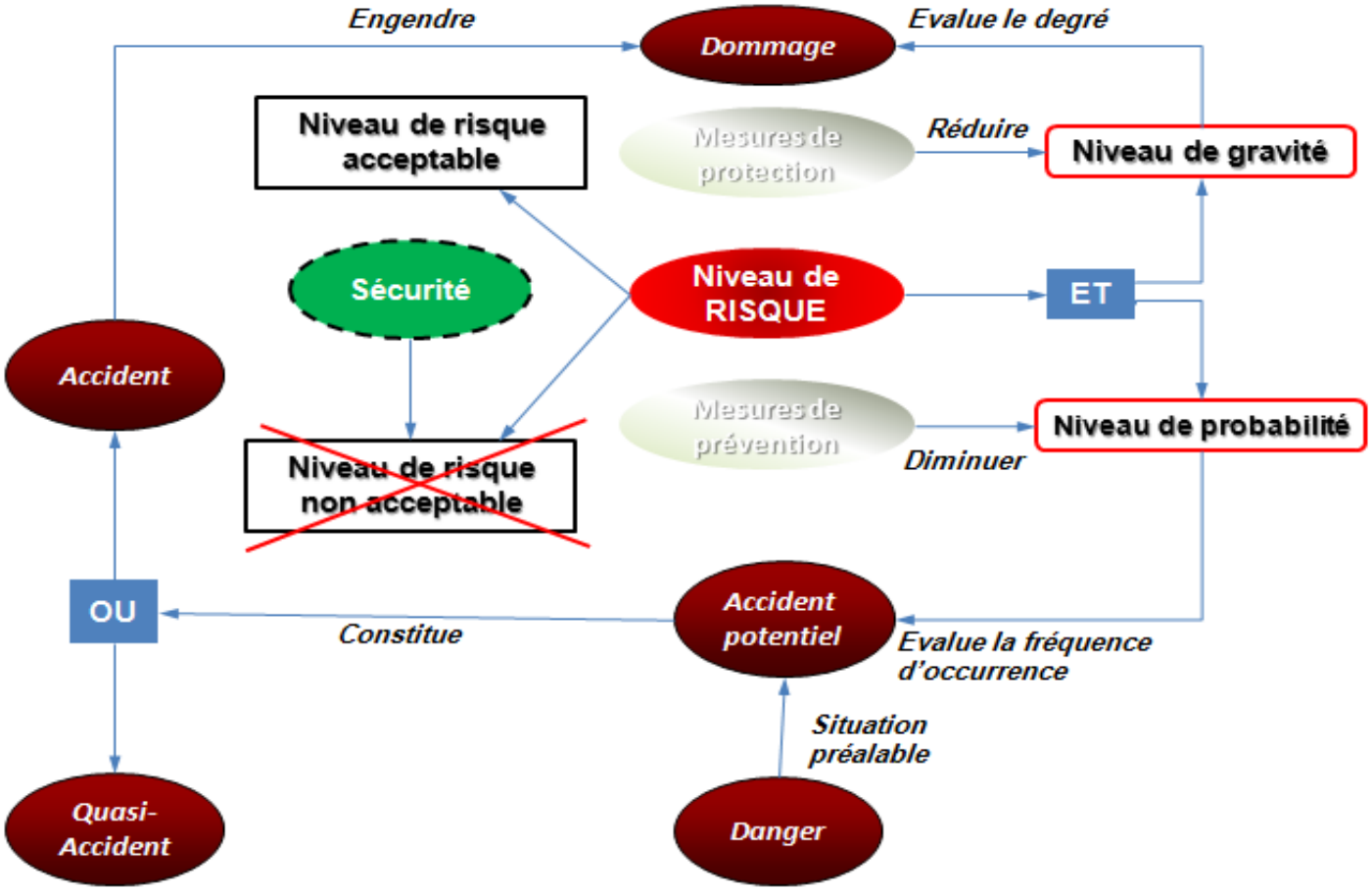

Figure 6. Articulation des principaux paramètres descriptifs d'une APR [10]

En se basant sur la terminologie précédemment évoquée, la méthode d'Analyse Préliminaire des Risques (APR) proposée fait intervenir, généralement, les étapes suivantes :

- Identifier la liste des accidents potentiels

- Identifier la liste des dangers, des dommages, des éléments dangereux y associés
- Evaluer le niveau de risque en identifiant le niveau de gravité ainsi que le niveau de probabilité associé à l'accident potentiel.
- Proposer les mesures de protection (pour atténuer la gravité des dommages provoquées par un accident potentiel) et de prévention (minimiser ou annuler la probabilité d'un accident potentiel).
- Identifier les contraintes et les critères de sécurité qui doivent être imposé sur l'ensemble des études de sécurité situé en aval.

4. Complémentarité du risque économique et du risque technologique :

De point de vue économique, le niveau du risque prend en considération à la fois l'aspect économique et technique. Malheureusement dans une entreprise, les spécialiste de sécurité parlent et essayent de minimiser les risque technique or les concepts techniques et économique ne peuvent pas être dans en aucun cas traité d'une manière séparé, en effet en fonction de ces caractéristiques, des opportunités des menaces, des coûts de la rentabilité, un bon système de la gouvernance doit trouver un optimum permettant d'obtenir le meilleur rapport cout/sécurité. La sécurité qui coute cher devient une menace et induit à l'insécurité ce qui nous pousse à dire que la sécurité reste une composante crucial à manipuler avec prudence. Cependant la composante sécurité reste une condition primordiale compte à une bonne gouvernance. [8]

5. Proposition d'une nouvelle approche d'analyse du risque économique et technologique :

Pour apporter un élément de réponse, notre approche repose essentiellement sur une méthode d'analyse de sécurité nommé l'analyse préliminaire des risques APR suggéré par plusieurs réglementations nationales et européennes. Comme son nom l'indique elle est préliminaire, quelque soit le système, il est indispensable de se doter d'une méthode d'analyse des risques.
La méthode développée s'articule autour de trois étapes complémentaires et itératives. A partir des accidents potentiels, la première étape permet de déterminer par induction la liste des dommages que pourrait causer un accident et par déduction la liste des dangers qui peuvent se manifester dans le système. La deuxième étape utilise les dangers précédents pour identifier par déduction la liste des éléments dangereux et, par induction, celle des accidents potentiels. Etablir à nouveau la liste des accidents potentiels à partir des dangers permet éventuellement d'engendrer de nouveaux accidents potentiels non considérés lors de la première étape. Dans ce cas, la première étape de l'analyse doit être reprise en vue d'enrichir la liste des dangers précédemment déduite. Il s'agit en fait d'une action de vérification qui permet d'accroître davantage la liste initiale des accidents potentiels. La troisième étape de l'analyse consiste, à induire des dangers, à partir des éléments dangereux déduits lors de la deuxième étape. Le catalogue des dangers établi à l'issue de cette troisième analyse est confronté à celui qui est déduit lors de la première étape de l'analyse à partir des accidents potentiels. L'invention de nouveaux dangers impose de recommencer la deuxième étape d'analyse et éventuellement la première. Ce processus de contrôle itératif permet d'assurer la complétude et de tendre ainsi vers l'exhaustivité de l'analyse préliminaire de risques (APR). La figure 7 schématise les différentes étapes impliquées dans le processus d'analyse de risque que nous préconisons [9] et [10].

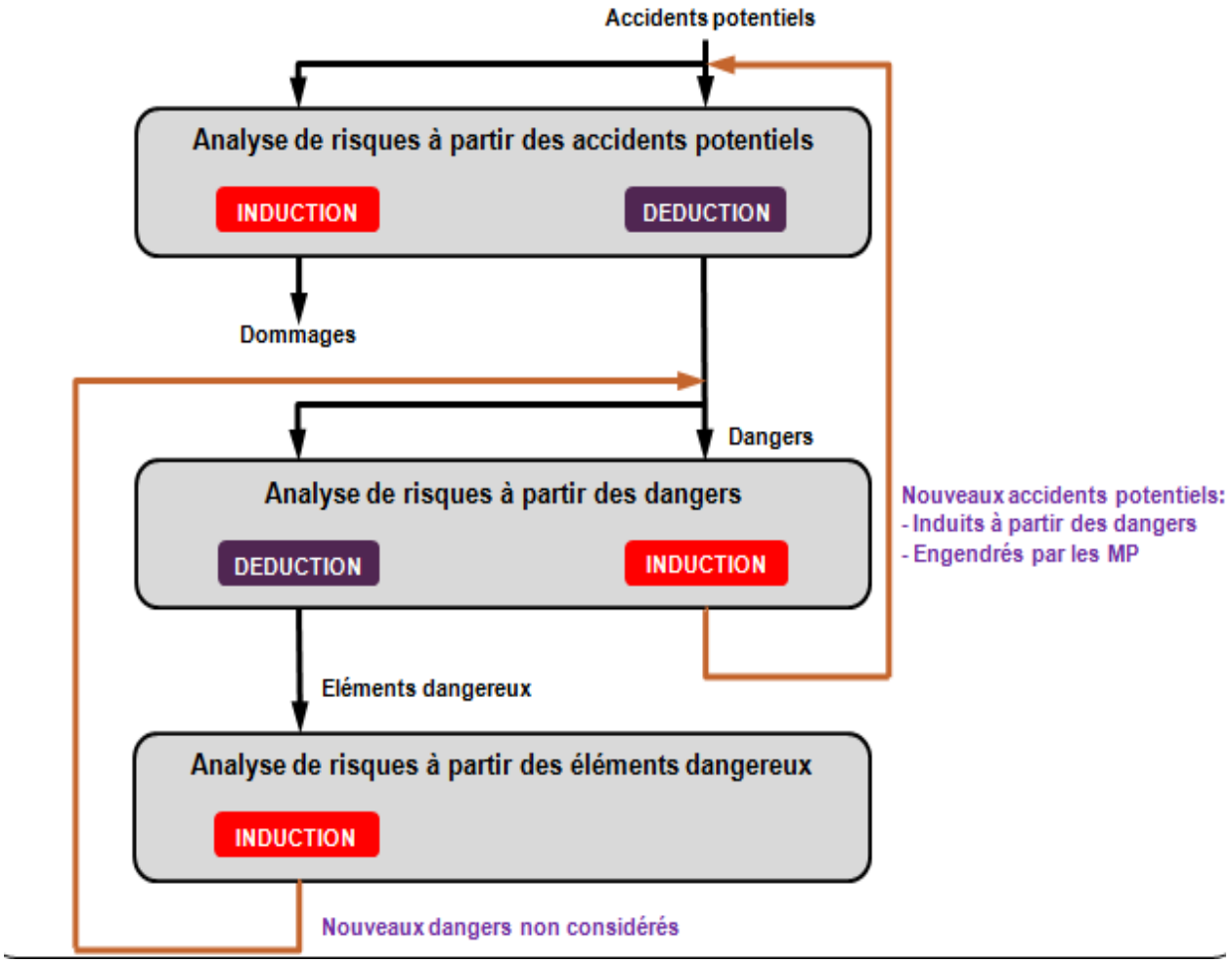

Figure 7 Principe général de la méthode d'APR [9,11]

Face à l'évolution technologique, tous les organismes et structures de recherche spécialisés, se sont rendus compte de la nécessité d'intégrer de nouveaux concepts comme la qualité, le facteur humain et l'ergonomie. La composante principale, voir même cruciale pour tout système industriel à risque, demeure toujours la sécurité. Selon la norme européenne CENELEC 50129 [3], la sécurité est définie *« par l'absence de tout niveau de risque inacceptable »*.

Cette approche elle va imposer des contraintes et des critères de sécurité sur l'ensemble des méthodes d'analyse de sécurité situé en aval.

Cette approche devient bénéfique que si elle prend en considération tous les aspects de l'entreprise et notamment économique, à noter que l'amélioration de la sécurité suppose un investissement provenant de la création de la valeur. la dite création des valeur de nos jours en stagnation voir en régression vue la conjoncture et la structure économique actuelle , de ce fait l'amélioration de la sécurité par le biais de la création de la valeur disponible actuellement n'est possible qu'a travers un système d'aide à la décision en ayant recours à l'intelligence artificielle qui de nos jours avec l'évolution technique et technologique présente l'une des solutions les moins couteuses qui a fait ses preuves dans plusieurs domaine en Europe et dans le monde entier. Tel que la comptabilité intégré la numérisation de la documentation qui minimise les risque de pertes voire même de la disparition d'archive vitale pour toute base de données nécessaire à l'analyse à l'audit et à la prévision de la sûreté de fonctionnement SdF et notamment la composante sécurité que si elle génère une valeur ajoutée , faire de la sécurité pour la sécurité ne présente aucun intérêt aucun sens si cela ne dégage pas une rentabilité supplémentaire permettant le financement de recherche tout en dégageant un profit. Cette approche nécessite un travail collégial basé sur une coopération permanente entre le pôle financier et le pôle technique.

7 Etude de faisabilité d'un outil d'aide à la prévention des risques dans un système sociotechnique

La majorité de travaux dans ce domaine se penchent sur l'utilisation des terminologies et des formalismes classique avec des outils conventionnels, peu d'intérêt est accordé pour les phases en aval notamment celle d'exploitation. La démarche de prévention des risques est généralement limitée à une exploitation quantitative générant des rapports statistiques. Il s'agit donc pour nous de proposer un moyen pour exploiter de manière qualitative ces connaissances pour éviter que les scénarios ne se reproduisent dans le futur. Une solution informatique conventionnelle n'a aucun intérêt, c'est à ce niveau que le recours aux techniques d'Intelligence Artificielle (IA) n s'avère plus approprié. En effet, le but d'IA est de simuler ou de mimer les activités intellectuelles humaines [11]. L'évolution des recherches menées dans cette voie résulte aux systèmes experts (SE) ou Systèmes à Base de Connaissances (SBC) .Ils permettent de modéliser le raisonnement humain, d'en faciliter l'acquisition, la modification et la mise à jour et de produire des explications sur la façon dont sont obtenus les résultats d'une expertise. En effet, le système expert reçoit des faits de l'utilisateur et envoie l'expertise dans le retour. Habituellement, un SE se présente comme l'association d'une Base de Connaissance, d'un moteur d'inférence et d'une Interface Homme-Machine.

- La base de connaissances modélise la connaissance d'un domaine considéré. Elle est généralement constituée par :
  - Une base de fait : représente la mémoire du travail du système expert. Elle détient les informations établies par l'utilisateur ou déduites par le moteur d'inférence.
  - Une base de règles : constitue le savoir-faire sur le domaine et indique les actions à prendre lorsqu'on est face à une situation donnée.
- Le moteur d'inférence : est la partie créative du SE. A partir des règles et des faits détenus dans la base de connaissances, et mettant en œuvre des mécanismes inductifs et préventifs, il engendre de nouveaux faits afin de réaliser la résolution effective du système.

- Un moteur d'inférence peut fonctionner en chaînage avant ou en chaînage arrière

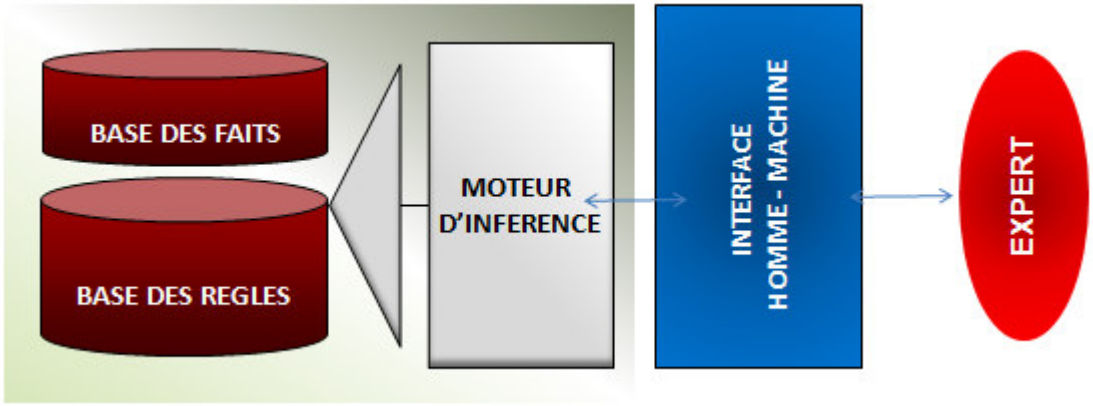

Figure 8 Architecture fonctionnelle de l'outil d'aide à la prévention des risques envisagé

8 Conclusion

La finance demeure l'élément clé de toute recherche, évolution technique et ou technologique, en outre l'élément financier représente aussi l'aboutissement de l'ensemble des éléments de recherche. Le meilleur exemple étant l'actuelle crise financière qui a paralysé les sorts technologique qu'on a vécu durant les 30 dernières années .Il y'on a des méthodes des techniques et des moyens qui peuvent être d'apport indéniables et bénéfique pour apporter un élément de réponse à la problématique soulevé Néanmoins ,la sureté de fonctionnement est plus précisément la composante sécurité demeure toujours la clé de voute de la réussite de tout système socioéconomique à risque.

Bibliographie

[1] BOULANGER J-L., *« Expression et validation des propriétés de sécurité logique et physique pour les systèmes informatiques critiques ». Thèse de Doctorat de l'Université de Technologie Compiègne. 23 Mai 2006.*

[2] INTERSECTION, LE MAGAZINE SCHNEIDER ELECTRIC DE L'ENSEIGNEMENT TECHNOLOGIQUE ET PROFESSIONNEL, *La Sûreté de Fonctionnement (SdF), Novembre 2004, p4.*

[3] NORME CENELEC EN 50 129 : *Application ferroviaire – Systèmes de signalisation, de télécommunications et de traitement è Systèmes électroniques de sécurité pour la signalisation.*

[4] MAALEL,A, HADJ-MABROUK,H, 2010, *Contribution of case based reasoning (CBR) in the exploitation of return of experience. "Application to accident scenarii in rail transport", SIIE'2010, 3rd International Conference on Information Systems and Economic Intelligence, 18-20 february 2010, Sousse, Tunisia, IEEE, 8p*

[5] BAHRI S, HADJ MABROUK *L'intégration de la sécurité dans les systèmes technologiques de l'information et de la communication.* ^{5th} *International Conference:* ***S****ciences of* ***E****lectronic,* ***T****echnologies of* ***I****nformation and* ***T****elecommunications March 22-26, 2009 – TUNISIA*

[6] CHERTUN'2008, *Première Journées d'études des chercheurs Tunisiens dans la sécurité des transports ferroviaires. Le 25 Avril 2008, Sousse, ACTE de la journée, p17.*

[7] Norme CENELEC EN 50 126: *Application ferroviaire – Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS).*

[8] HADJ-MABROUK,H, 2008, *Méthode originale d'analyse des risques technologiques, Symposium "maintenance et maîtrise des risques", mai 2008, Oran, Algérie, 12p*

[9] HADJ-MABROUK H. *« Méthode d'analyse préliminaire des risques dans les transports ferroviaires ». 15ème congrès de maîtrise des risques et de Sûreté de fonctionnement, Lille-France, 10-12 Octobre 2006.*

[10] ELMABROUK,A, HAMDAOUI,F, HADJ-MABROUK,H, 2009, *Intégration de la Sécurité dans les Autoroutes de la mer, SETIT, 5th International Conference, Sciences of Electronic, Technologies of Information and Telecommunications, mars 2009, Hammamet, Tunisie, IEEE, 11p*

[11] HADJ-MABROUK H. *« Méthode d'analyse préliminaire des risques dans les transports ferroviaires* ». 15ème congrès de maîtrise des risques et de Sûreté de fonctionnement, Lille-France, 10-12 Octobre 2006.