Outil d'aide à la décision basée sur l'analyse de risques

Cyril Cappi, Stella Duvenci-Langa, Fabien Létourneaux, Charlyne Toussaint, Fabrice Ardeois

Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Outil d'aide à la décision basée sur l'analyse de risques
Risk analysis decision support tool

Cyril Cappi
SNCF
1/3, avenue François Mitterand
93210 La Plaine Saint-Denis
cyril.cappi@sncf.fr

Fabien Létourneaux
SNCF
1/3, avenue François Mitterand
93210 La Plaine Saint-Denis
fabien.letourneaux@sncf.fr

Fabrice Ardeois
FRET SNCF
24, rue Villeneuve - 92583 CLICHY LA GARENNE
fabrice.ardeois@sncf.fr

Stella Duvenci-Langa
SNCF Réseau
93210 La Plaine Saint-Denis
stella.duvenci-langa@reseau.sncf.fr

Charlyne Toussaint
Polytech Angers
62 Avenue de Notre Dame du Lac,
49000 Angers
toussaint.charlyne@gmail.com

***Résumé* —Le but de cette communication est de présenter la preuve du concept faisant suite aux travaux du projet PLASA (smart PLAnning and SAfety), mené au sein du département Innovation & Recherche de la SNCF, et qui s'insère dans le cadre d'un projet européen Shift2Rail. On s'intéresse au concept d'un outil d'aide à la décision en tenant compte de l'évaluation des risques industriels dans le domaine ferroviaire. A destination des gestionnaires de la cellule de crise dans les centres opérationnels, il permet de collecter les informations nécessaires d'un incident survenu et ainsi pouvoir les aider à prendre des décisions cruciales rapidement. L'idée de réaliser un tel projet vient de la complexité du processus de prise de décision dans les centres opérationnels qui est basé principalement sur l'expérience des décisionnaires. L'autre souhait est de vouloir apporter une autre vision basée, non plus uniquement sur la ponctualité, mais également sur la prise de conscience des risques.**

Abstract*— *The purpose of this communication is to present proof of the concept following the work of the Plasa project (smart PLAnning and SAfety), carried out within the Innovation & Research department of SNCF, and which is part of a project European Shift2Rail. We are interested in the concept of a decision support tool taking into account the assessment of industrial risks in the railway sector. Aimed at managers of the crisis unit in operational centers, it makes it possible to collect the necessary information about an incident that has occurred and thus be able to help them make crucial decisions quickly. The idea to carry out such a project comes from the complexity of the decision-making process in the operational centers which is based mainly on the experience of the decision-makers. The other wish is to want to bring another vision based, not only on punctuality, but also on awareness of the risks.

Keywords—risk assessment, decision support tool, digital, human factor,

I. INTRODUCTION

Le secteur ferroviaire se caractérise par des cycles particulièrement longs. Sur le réseau ferré, les innovations récentes côtoient souvent des équipements de plusieurs dizaines d'années. La cohabitation de ces différents systèmes, basés sur des technologies radicalement différentes rend leur gestion délicate.

Dès lors, le système ferroviaire peut être qualifié de compliqué et même de complexe, les interfaces et les interactions y sont omniprésentes.

En France, la SNCF exploite plus de 15000 trains quotidiens, trains de banlieue, régionaux et à grande vitesse. Exploiter en toute sécurité avec un niveau de qualité élevé pour les clients (e.g. ponctualité, information voyageur, trains supprimés, …) devient un véritable défi. Cela nécessite de pouvoir réagir rapidement à la survenue d'un aléa, comprendre ce qu'il se passe, appréhender les risques. La prise de décision devient clé de voûte pour la résilience du système. Ainsi la recherche dans le domaine de la sécurité et de l'exploitation est cruciale, tant dans la gestion opérationnelle tant dans la conception de nouveaux systèmes.

Shift2Rail est la première initiative européenne à proposer des solutions ciblées de recherche et d'innovation (R&I). C'est en ce sens qu'en 2016, le projet PLASA (Smart Planning and Safety) est lancé. D'une part, il améliore les activités de planification des différents acteurs du système ferroviaire au moyen d'une simulation ferroviaire précise et, d'autre part, il fournit une méthodologie pour gérer la sécurité du système ferroviaire sur la base d'une évaluation des risques. C'est ce second objectif que nous présentons.

Afin d'illustrer ces travaux aboutissant à la conception d'un PoC (Proof Of Concept), nous décrivons la démarche méthodologique en deux temps : tout d'abord sous l'angle

d'un état de l'art afin d'éclairer les processus, entre analyse de risque et prise de décision, nous développons ensuite l'approche retenue :

- Par une mise en perspective entre pratique usuelle et désirable, compte tenu des moyens technologiques actuels.
- Puis au travers d'un cas d'usage traitant d'une anomalie de signalisation ferroviaire, nous explicitons les paramètres pertinents à considérer, les outils d'évaluation des risques idoines, le modèle mis en œuvre ainsi qu'un premier retour d'expérience.

Enfin nous donnons des précisions sur les choix qui ont guidé le prototypage de l'outil.

II. ETAT DE L'ART

On décrit généralement le processus de décision en quatre étapes :
1. Identifier le problème à résoudre et/ou formuler la question à laquelle répondre,
2. Identifier les choix possibles,
3. Étudier les conséquences de chacun de ces choix,
4. Sélectionner et mettre en œuvre l'un de ces choix

Les méthodes de gestion des risques tentent de répondre aux trois premières étapes, tandis que la quatrième est abordée par les théories de prise de décision.

A. Méthodes d'analyse de risque

Les différentes méthodes pour analyser les risques dans le domaine ferroviaire sont similaires à la plupart des autres domaines industriels [1]. Aujourd'hui le recours à des méthodes dites « classiques » sont d'usage.

La technique d'analyse préliminaire des risques (PHA) est une vaste étude initiale utilisée dans les premiers stades de la conception du système. Le FME (C) A, un outil de conception utilisé pour analyser systématiquement les défaillances de composants et identifier les effets résultant sur les opérations du système. L'analyse de l'arbre de défaillance (FTA) est une analyse de défaillance déductive descendante dans laquelle un état indésirable d'un système est analysé à l'aide de la logique booléenne pour combiner une série d'événements de niveau inférieur. L'analyse d'arbre d'événements (ETA) est une technique de modélisation logique ascendante pour le succès et l'échec qui explore les réponses à travers un seul événement initiateur et ouvre la voie à l'évaluation. Une étude de danger et d'opérabilité (HAZOP) est un examen structuré et systématique d'un processus complexe ou d'opérations planifiées ou existantes afin d'identifier et d'évaluer les problèmes pouvant représenter des risques pour le personnel ou l'équipement. Le modèle Bow-tie est une méthode d'évaluation des risques qui peut être utilisée pour analyser et démontrer relations causales dans les scénarios à haut risque.

Ces méthodes, en fonction de leur représentation, sont très utiles dans le dialogue, la communication et plus globalement dans des compréhensions partagées, essentielles dans le processus décisionnel. Ces différentes méthodes sont complémentaires. Parfois, vous pouvez lier les sorties de certains d'entre elles aux entrées des autres. Selon le système que vous souhaitez analyser, vous devez choisir la méthode la plus adaptée. Cela pourrait être un avantage car vous pouvez choisir la plus efficace mais cela pourrait être un inconvénient si vous ne connaissez pas la méthode que vous devez choisir. Le principal inconvénient de ces méthodes est que les facteurs externes sont rarement pris en compte. Par ailleurs, les facteurs organisationnels, humains et sociaux ne sont guère modélisés dans de telles méthodes. La sortie dépend, dans de nombreux cas, de l'analyste. L'exhaustivité ne peut être abordée pendant la phase d'enquête. Habituellement, seulement les causes et conséquences les plus importantes sont étudiées.

Ces méthodes concernent un système cohérent et simple. Il est très difficile d'analyser un système complexe où tous les éléments sont liés et on ne maîtrise pas les interactions, ni les conséquences. Le raisonnement causal n'est plus linéaire et la modélisation d'un tel événement ou scénario est quasi impossible.

Enfin, ces méthodes ne tiennent pas compte des critères éventuels des managers et, la plupart du temps, il est très difficile de transformer l'analyse des risques et les conclusions de l'évaluation en décisions. Les théories sur la prise de décision complètent en ce sens la dimension organisationnelle, sociologique et humaine dans les prises de décision.

Au vu des limites des méthodes classiques, les méthodes à base de modèle (e.g. MBSA) voient peu à peu le jour dans le domaine du transport guidé. Prometteuses, par leur capacité à répondre à l'enjeu de cette complexité, les modèles d'ingénierie complexe (i.e. MBSE) restent toutefois encore trop rares dans le domaine du ferroviaire pour nous permettre de les exploiter. Dès lors, il nous parait difficile d'aborder l'outil d'aide à la décision sous l'angle de ces techniques [2], d'où un choix des plus traditionnels.

B. Prise de décision

Au carrefour du management, de la sociologie des organisations et des sciences politiques, la prise de décision est devenue l'objet d'une quasi discipline à partir des années 50. Plusieurs modèles se sont développés : le modèle rationnel, politique, cognitif…Ils ont tous en commun de mettre en avant le fait que les processus de prise de décision ne sont en aucune façon neutre et objectif.

Processus de prise de décision

La prise de décision est un processus cognitif complexe, différent de la réaction instinctive et immédiate, visant à la sélection d'un type d'action parmi différentes alternatives. Ce processus est théoriquement basé sur des critères de choix, et sur une analyse des enjeux et des options et conduit à un choix final. Cependant, plusieurs recherches montrent que dans certaines situations critiques et urgentes, les experts, influencés par les émotions, peuvent privilégier leur intuition (Klein, 1999) [3]. C'est ce qu'on appelle l'intelligence émotionnelle (Damasio, 1995) [4], un nouveau champ d'étude en train de se développer pour permettre la résilience des organisations.

Herbert Simon (1957) [5], à l'origine des recherches sur le processus de décision, aboutit à la théorie sur la rationalité limitée. Cette théorie part du principe qu'il est impossible aux acteurs de maximiser leur « utilité » car :

- Il est difficile de traiter l'incertitude,
- L'information disponible est imparfaite,
- Les acteurs ont des capacités de traitement de l'information limitées,
- Les acteurs sont en situations d'interdépendance stratégique.

Ainsi, la décision ne sera pas « parfaite », elle sera juste satisfaisante. « Un agent recherche, non pas l'action qui donne le meilleur résultat dans des conditions données, mais une action qui conduit à un résultat jugé satisfaisant, relativement à un certain niveau d'aspiration ».

Niveaux organisationnels et modes de décisions

- Décider seul : La décision ne dépend que de soi et peut être rapidement prise, mais la décision personnelle risque d'être subjective sous l'influence des facteurs personnels (âge, culture, état psychologique…)
- Décider en groupe : les décisions par consensus ou à la majorité, intègrent les avis des membres d'un groupe [6].
- Décider par délégation : la responsabilité de la prise de décision est donnée à un individu ou à un groupe, au nom de toute l'équipe.

L'objectif de l'étude ci-dessous s'inscrit dans le « décider seul » en s'appuyant sur la conception d'un outil d'aide à la décision simple, basée sur des techniques dites « classiques » d'analyse des risques, sans remettre en cause le processus de décision qui demeure inchangé, celui des processus opérationnels de l'entreprise.

III. APPROCHE

A. Vers une objectivation de la prise de décision

Le projet PLASA part du constat que les opérateurs en charge des circulations ferroviaires doivent prendre des décisions critiques et rapides en cas d'incident générant des conditions de trafic dégradées sur le réseau ferré. Aujourd'hui, les prises de décisions sont principalement basées sur le respect des référentiels et sur des outils de simulation proposant des scénarios optimaux vis-à-vis du retour à un trafic nominal. Mais elles s'appuient également fortement sur l'expérience préalable de l'opérateur notamment lorsque différentes alternatives sont possibles.

Cependant ces différentes options n'ont pas toutes le même impact sécurité lorsqu'on élargit le champ à l'ensemble de l'environnement ferroviaire intégrant ainsi des facteurs difficilement maitrisables (météo, travaux, comportements des passagers en particulier). Eclairer la prise de décision nécessite donc d'une part une approche holistique de la situation et d'autre part, la fourniture d'éléments factuels permettant d'évaluer les facteurs clés régissant celle-ci.

Les technologies IOT (internet des objets) associées aux ressources du Big data et de l'intelligence artificielle (IA) permettent d'envisager une réponse moyen-long terme à cette problématique, en assurant une surveillance constante des assets et en développant des modèles prédictifs. Cette approche est notamment développée dans le cadre du projet complémentaire à PLASA dans Shift2Rail : GoSafeRail [7]. En outre, aujourd'hui l'exemple du Data mining [8] répond à cette volonté d'allier des outils analytiques puissants à l'analyse de données massives. Ils permettent aux utilisateurs d'analyser les données sous l'angle du prisme sécurité. Le Data Mining repose sur des algorithmes complexes et sophistiqués permettant de segmenter les données et d'évaluer les probabilités futures. Ces technologies associées aux méthodes MBSA seront gages d'une plus grande cohérence et précision, en limitant l'effet simplification de l'évaluation aux risques et des calculs afférents.

Bien que prometteuses ces approches requièrent toutefois un déploiement long et coûteux de capteurs et de capacité de traitements qui ne sera pas effectif rapidement sur l'ensemble du réseau. Cela implique également une transformation profonde des métiers (organisation, compétences).

Il est donc nécessaire de développer également des approches intermédiaires, plus "rustiques", se basant sur les seuls éléments disponibles à date et privilégiant la présentation consolidée des informations, sous une forme adaptée et interprétable sur le terrain. L'ambition est de proposer une évolution sans rupture, reprenant les schémas actuels de la prise de décision tout en améliorant ce processus par la fourniture d'un tableau de bord composé d'informations prétraitées utiles, objectives et fiabilisées. Les mécanismes de traitement sous-jacents de l'information restent imparfaits dans un premier temps, car issus d'analyses a priori et non exhaustives de données incomplètes ainsi que de dire d'experts et de retour d'expérience. Ceci étant, l'outil se base sur une sélection attentive des risques, des bases statistiques. Nécessairement, en focalisant sur les risques majeurs nous nous privons de l'appréhension des risques mineurs. Mais considérons, que cela contribue à renforcer la place de l'homme dans la boucle, avec un maintien nécessaire des compétences, une sensibilité aux risques et une culture de sécurité

Cependant, cette approche intermédiaire constitue un socle sur lequel peuvent se capitaliser le savoir-faire et les nouvelles connaissances. Elle peut également évoluer et construire un pont vers l'approche long-terme basée sur la technologie (IOT, Big data, IA).

B. Paramètres à considérer (interprétable par l'homme)

La première étape d'une évaluation des risques consiste à déterminer comment exprimer les exigences de sécurité [9]. Un système peut être considéré, ou pas, comme acceptable en termes de sécurité sur la base des paramètres et des valeurs qui sont choisis pour l'évaluer. Par conséquent, l'évaluation des risques dépendra de ces choix.
Ci-dessous sont listés les paramètres de sécurité les plus courants issus de notre expérience. L'un de ces paramètres, ou une combinaison de ceux-ci, sera utilisé dans les évaluations des risques :

- Nombre équivalent de victimes : chaque blessure dans un accident est convertie en nombre de victimes,
- Coût : toutes les victimes se voient attribuer un coût et les solutions sont comparées sur la base du coût total,
- Disponibilité du système, lorsque la disponibilité d'un système est fortement liée à la sécurité,
- Temps disponible pour mettre en œuvre la mesure, pour les systèmes déjà en service.

Afin de les utiliser, comme données d'entrée de l'outil d'aide à la prise de décision, il conviendra de leur donner un caractère interprétable.

C. Description du cas d'usage

Il s'agit d'une extinction d'un signal lumineux de cantonnement (utilisé pour assurer l'espace entre les trains), sur un secteur de gare, en proche banlieue ouest parisienne.

Ici le risque majeur pourrait être le franchissement dudit signal, engendrant par exemple une collision avec un autre train. Ainsi dans telle situation, le preneur de décision peut choisir de continuer d'exploiter les trains par la voie considérée avec des mesures de réduction du risque, ou bien dévoyer les trains sur une voie contigüe exempte de toute anomalie figure 1. Chaque alternative, supportée par l'application de procédures issues de référentiel de sécurité, garantit la résilience du système. Mais les textes de prescription considèrent rarement l'angle du cas le plus défavorable, y préférant celui le plus probable. Ainsi du point de vue de la durée d'exposition au risque : une considération d'une maintenance rapide sous 2 heures (90% des cas) est gage de sécurité. Au contraire, si l'avarie perdure, le facteur d'exposition pourrait augmenter la probabilité d'apparition du risque sécurité.

Figure 1 : Schéma simplifié de la gare

Notons qu'un dispositif de sécurité technique (KVB Contrôle de Vitesse par Balise) supervise la vitesse du train. En revanche le respect de l'arrêt en amont du signal éteint, son identification et l'application des procédures de franchissement reposent intégralement sur des opérateurs humains. Il convient de quantifier les probabilités de la fiabilité des barrières humaines.

D. Evaluation des risques

Notre approche s'intéresse au principe retenu d'un processus standardisé, figure 2, pour tous les cas d'usage, tout en laissant latitude sur les outils d'évaluation des risques à mettre en œuvre,ceux-là même décrits dans le Chapitre état de l'art (Cf. Chp II A).

Ce processus commence par la collecte des principales caractéristiques du cas traité. Ensuite, les scénarios pertinents et leurs risques associés doivent être identifiés. La troisième étape consiste à analyser les dits risques, en déterminant leurs causes et leurs conséquences et les probabilités d'occurrence. Enfin, l'évaluation des risques détermine, de manière qualitative et/ou quantitative, la gravité et autorise le calcul de données de sorties qui matérialisent les exigences de sécurité : ces données alimentent alors le modèle de décision [10].

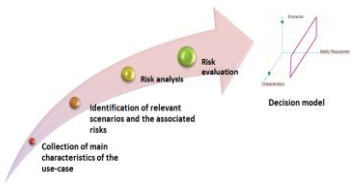


Figure 2 : Processus d'évaluation des risques

L'analyse a été réalisée d'un point de vue opérationnel pendant le cycle de vie du composant lors d'une panne (signal éteint). La figure 3 reproduit la méthode, composée de 5 étapes principales, en parallèle le processus qui conduit au modèle de décision.

Dans cet incident, en raison de la nature inductive de l'analyse (signal éteint), un modèle d'analyse d'arbre d'événement a été sélectionné par des experts pour effectuer l'analyse figure 4. Les facteurs causaux sont quant à eux identifiés par la méthode déductive avec le modèle d'analyse d'arbre de défaillance figure 5.

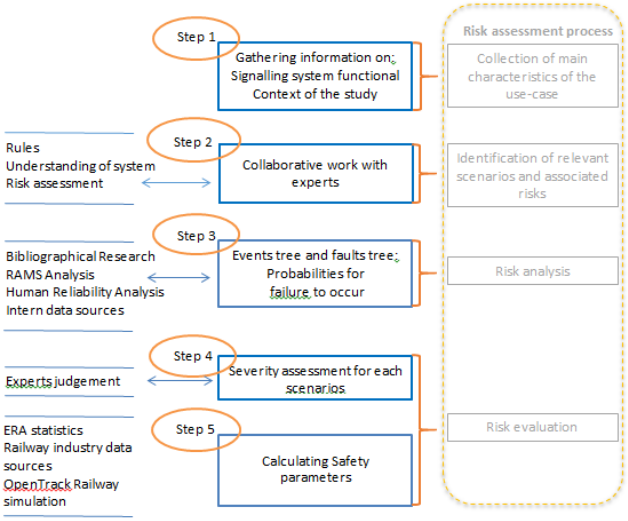


Figure 3: Méthode d'évaluation des risques

La détermination des occurrences et des probabilités d'occurrences de défauts a été quantifiée à partir de données internes en termes de fiabilité, de disponibilité des composants du système. Puis elles ont été affectées dans les arbres d'évènement et défaillance.

En ce sens et pour répondre au besoin de quantifier les barrières humaines omniprésentes la méthode HEART [11] a été choisie, ou plus précisément une déclinaison "ferroviaire" de cette méthode développée par le Rail Safety and Stard Board (RSSB) [12]. Les deux éléments clés de l'évaluation de la fiabilité des tâches ferroviaires sont les GTT de types « tâches génériques » et les EPC « conditions de production d'erreurs ». Il existe huit types de tâches génériques : chaque GTT vise à fournir une description générique d'une tâche et une estimation de la probabilité d'erreur humaine associée. Les conditions de production d'erreurs (EPC) sont des facteurs qui devraient influencer négativement les performances humaines et qui sont utilisées pour adapter plus étroitement la tâche générique à la tâche réelle évaluée. Ces EPC sont pondérés par un facteur de proportion d'effet évalué (APOA) à dire d'expert.

Cette méthode calcule de la probabilité d'erreur humaine à l'aide de la formule:

Human Error Probability HEP = GTT × A1 × A2 ×…. × An

GTT = la probabilité d'erreur humaine associée à un GTT
A = Affect calculée pour chaque EPC

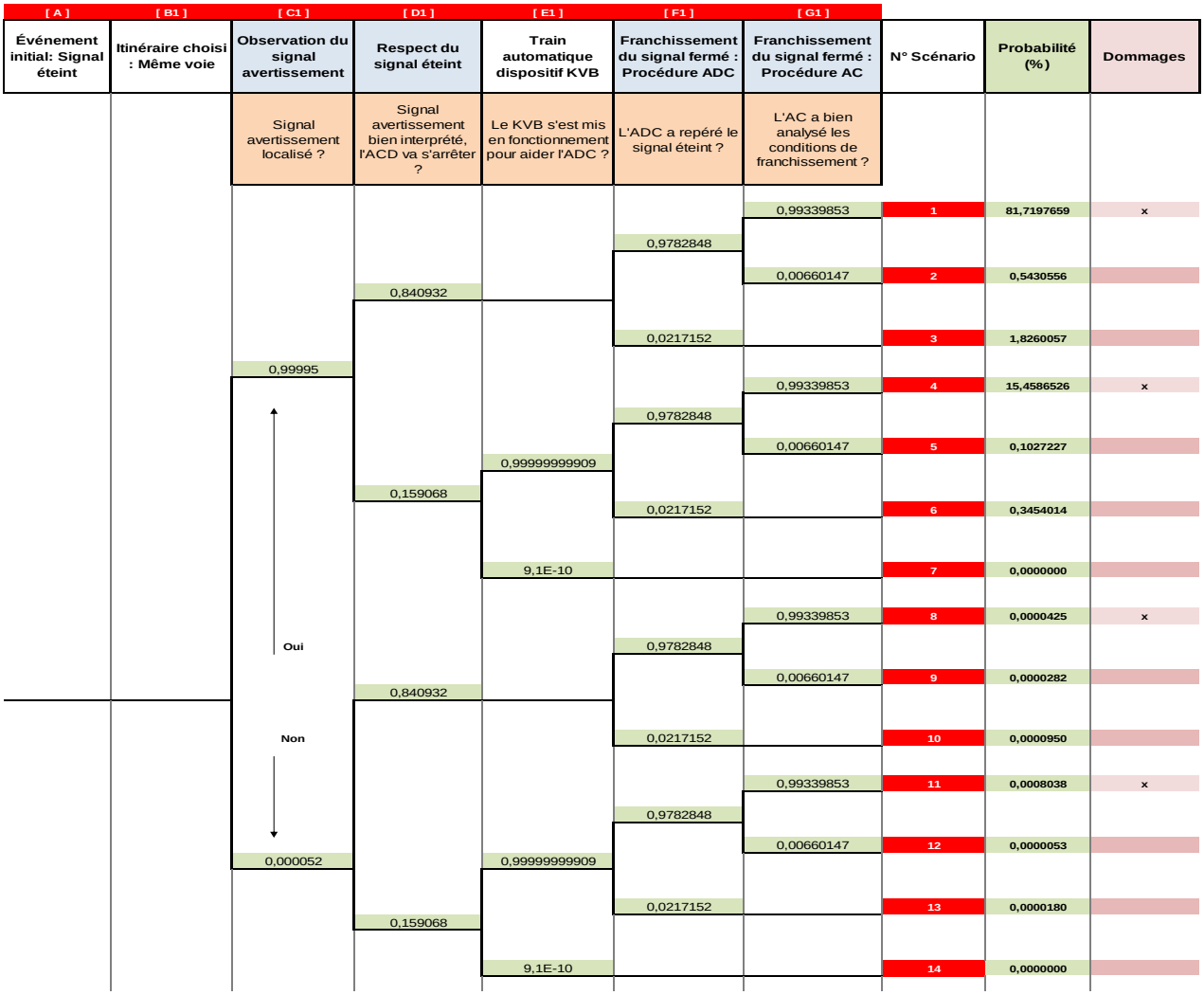


Figure 4 ETA extrait arbre d'évènement signal éteint

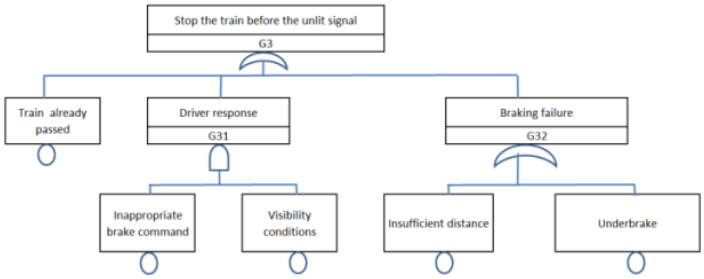


Figure 5 exemple arbre de défaillance

Les résultats obtenus pour la quantification de la fiabilité humaine des opérateurs intervenants sont également transposés dans les arbres d'évènement et défaillance (figure 4 et 5).

A titre d'exemple, voici la tâche de détection du signal éteint :

Description de la tâche:

Le conducteur risque de ne pas détecter le signal éteint. Il a effectué des phases de décélération, dans la zone d'approche (début du quai de gare) à une vitesse <30km / h et le signal situé à la fin du quai est éteint. L'horaire prévoit un arrêt régulier dans la gare. Pendant l'arrêt, avec le pic de trafic et la perturbation, le quai est bondé. A l'arrêt, quelques passagers demandent des informations au conducteur.

Évaluation de la fiabilité de la tâche ferroviaire:

L'identification d'un signal éteint nécessite de diagnostiquer un signal qui n'a pas d'indication dédiée, comme une lumière verte, jaune ou rouge. Le GTT R7 est donc sélectionné "Identification de situation nécessitant une interprétation des schémas d'alarme / d'indication". La description inclut le potentiel de charge de travail supplémentaire EPC R7 car le conducteur gère la conduite du train (conditions de reprises de marche) tout en informant les passagers, ce qui pourrait conduire plus directement à

des effets de type distraction. L'expérience et la formation du conducteur à la gestion de ces situations sont évaluées pour conduire à une proportion d'effet évaluée (APOA) à 0,1. Il n'est pas inclus dans la description, mais il y a aussi un faible bruit de signal en raison des conditions de visibilité (nuit / jour) pendant la tâche, l'EPC 'Un faible rapport signal-bruit' est appliqué avec une plage de valeurs d'effet (APOA) sur l'EPC [0,1 le jour - 0,4 la nuit].

GTT	EPC	MA	APOA
R7. Identification de la situation nécessitant une interprétation des modèles d'alarme / indication	T7. Conflit entre l'objectif long termes et court terme	2.5	0.1
	Ln1. Faible rapport signal/bruit	10	Nuit : 0.4 Jour : 0.1

Calcul:
Les valeurs HEP varient de 1,5.10-1 à 3.10-1.
Toutes les valeurs sont reflétées dans l'arbre de défaillance de la figure 4 avec une analyse de sensibilité en termes de conséquences dans l'arbre des événements.

La gravité quant à elle, a été estimée par le jugement d'experts. L'identification des risques met en exergue le risque de collision ou de déraillement. Les conséquences pouvant être la mort d'une ou plusieurs personnes et des blessures graves. Pour déterminer les exigences de sécurité, nous avons utilisé les statistiques de l'UEAR (European Union Agency for Railway), la simulation avec le logiciel Open Track pour les impacts de ponctualité, régularité relatifs à la disponibilité du système.

E. Modèle global

Dans le domaine ferroviaire, la prise de décision pour l'exploitation d'un système est basée sur l'évaluation et la comparaison de scénarii.
Afin d'établir les différents scénarii, nous devons connaître les conditions initiales du système. Il s'agit de prendre en compte des éléments de contexte (i.e. des éléments invariables comme le plan de voies, le type de matériel roulant, la localisation ...) mais aussi des éléments variables (i.e. la disponibilité du service de maintenance, les heures creuses et de pointe, jour / nuit, la météo ...) figure 6. Ces éléments seront désignés "caractéristiques". Le système peut donc être défini par la forme suivante:

$$\text{Système} = \sum \text{Caractéristiques}$$

Caractéristiques : éléments de contexte et éléments variables qui décrivent le système et affectent la séquence d'événements.

La méthode des scénarii peut être énoncée comme une approche synthétique qui, d'une part, simule, étape par étape et de manière plausible et cohérente, une séquence d'événements conduisant un système à une situation future et qui, d'autre part, en présente une vue d'ensemble.

F. Enseignements tirés

Le procédé utilisé est plutôt "classique" dans le domaine de l'analyse des risques avec l'utilisation d'arbres de défaillance,

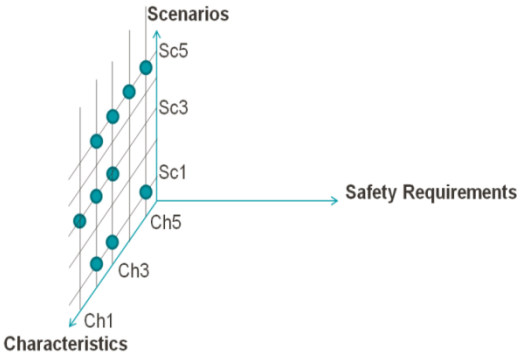


Figure 6 : Lien entre caractéristiques et scénarii

L'outil d'aide à la décision comprend le scénario à évaluer et la manière dont les caractéristiques d'un scénario affectent les exigences de sécurité (C.f. Chap III -B) figure 7. Le modèle est ainsi défini comme les relations entre : les informations disponibles sur le scénario, les événements variables (i.e. sources potentielles d'un impact sur le scénario) et les exigences que nous voulons évaluer.

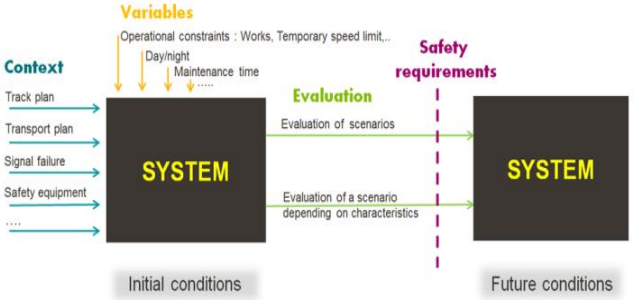


Figure 7 : Concept d'outil d'aide à la décision

Lorsque cette relation est basée sur des paramètres sur lesquels le concepteur de système ou bien le décideur peut agir le modèle devient un support à la décision qui prend en charge le choix de la meilleure solution optimisée pour la satisfaction des exigences.
Ainsi, l'outil d'aide à la décision se veut être un programme offrant une échelle de représentation de l'évaluation à deux niveaux.
Le premier niveau est appelé "macro vision". Dans cet affichage, l'utilisateur trouve tous les scénarii configurés à partir des caractéristiques du système initial (c'est-à-dire des éléments contextuels immuables et des éléments variables). Les éléments variables prennent par défaut une valeur statique. Chaque scénario est évalué en fonction des exigences de sécurité.
Dans sa version appelée "micro vision", le programme affiche un scénario unique préalablement sélectionné par l'utilisateur. L'interface permet de modifier les éléments variables (e.g. jour ou nuit, trafic, etc…), par une valeur dynamique. Pour chaque incrément, l'évaluation est automatiquement recalculée et le programme affiche les données à jour des exigences de sécurité. De cette façon, le décideur peut également simuler l'impact de l'évolution des caractéristiques variables du système sur les exigences.
d'arbres d'événements. Ces outils sont fréquemment utilisés dans les études de conception. Ainsi, dans une évaluation des risques dite «opérationnelle», nous pouvons gagner un temps

précieux en ayant accès aux études de sécurité FDMS (Fiabilité, Disponibilité, Maintenabilité, Sécurité).

La méthode RSSB [12] permet de quantifier la fiabilité humaine pour les cas d'usage où les barrières techniques font défaut. L'approche est accessible et peut être facilement mise en œuvre pour les responsables opérationnels ou les ingénieurs d'études.

L'ETA est au cœur de l'outil d'aide à la décision. Néanmoins de par sa complexité (i.e. la grande taille des ETA le rende non ergonomique) il reste peu ou prou interprétable pour un décideur, un concepteur. Les résultats de l'ETA, notamment les probabilités d'occurrence et la sévérité peuvent venir alimenter la source de données multicritères d'un outil d'aide à la décision, sous réserve de les fournir sous une forme intelligible. Enfin, les données ETA peuvent initialement être collectées et alimentées manuellement, puis tendre vers l'automatisation dans le futur avec la technologie du Big Data.

L'outil d'aide à la décision met en évidence des risques facilement identifiables et d'autres qui le sont moins (e.g. dévoyer le train fait apparaitre de nouveaux risques, comme le heurt par un train dû à la traversée des voies par les clients lors d'un changement de quai). Lors d'une situation perturbée, le décideur doit agir rapidement et l'outil peut lui fournir immédiatement une vision globale de la situation. Il peut alors, sur la base de sa propre expérience, enrichir l'analyse et décider de la solution appropriée. En complément l'outil permet d'améliorer sa prise de conscience des risques du système ferroviaire et contribue ainsi à développer des compétences.

Concernant la détermination des gravités, les outils de simulation facilitent parfois la quantification des exigences de sécurité (e.g. disponibilité). Quant à la question des dommages humains, relativement peu de données sont disponibles. La piste des outils de simulation des accidents ferroviaires, des chutes de voyageurs, pourrait enrichir la quantification. Une autre voie serait de porter aux autorités de régulation l'intérêt de constituer dès à présent une base de recueil de statistiques plus exhaustive que l'existant.

Cette approche nécessite au préalable de réunir la triple expertise : métier, méthode, mathématiques/statistiques. Un engagement collectif de plusieurs séances de travail est inévitable.

IV. OUTIL

A. Cahier des Charges de l'outil

Définir les principaux attributs du PoC est l'étape majeure de sa conception. C'est un moyen d'obtenir une première orientation. Les exigences retenues sont les suivantes :

Attributs fonctionnels :

- L'outil doit proposer les différents **itinéraires possibles** selon l'incident sélectionné et sa localisation ;
- L'outil doit évaluer et quantifier les **risques humains** liés à chaque itinéraire ;
- L'outil doit évaluer et quantifier l'**impact ponctualité** lié à chaque itinéraire ;
- L'outil doit permettre à l'utilisateur de faire varier le **temps de maintenance** ;

Attributs non-fonctionnels :

- **Utilisabilité** – L'outil doit être simple et souple d'utilisation et de prise en main ;
- **Fiabilité** – L'outil doit donner des résultats fiables et cohérents ;
- **Robustesse** – L'outil doit donner des résultats justes et fournir des valeurs réalistes par défaut aux données d'entrée du modèle. Il doit être capable de s'adapter aux divers niveaux de renseignement des données d'entrée par les utilisateurs ;
- **Modificabilité** – L'outil doit être modifiable afin de pouvoir être étoffé ;
- **Testabilité** – L'outil doit être facile à tester.

Ces deux listes sont non-exhaustives et sont issues de choix d'expérience et d'attentes des utilisateurs afin de ne pas rendre trop complexe ce premier prototype.

B. Développement

La partie calculatoire du PoC s'est déroulée en deux grandes parties :
- Analyse des risques,
- Recherche et consolidation des données.

• *Analyse des risques*

Par rapport à cet incident, 4 scénarii sont envisageables :
(1) Continuer d'exploiter par la même voie avec le signal éteint,
(2) Dévoyer par une autre voie, ne demandant aucun changement de quai,
(3) Dévoyer par une autre voie, demandant un changement de quai,
(4) Dévoyer par une autre voie et supprimer l'arrêt à Sartrouville.

Un arbre d'événement a été décliné pour chaque scénario. Les arbres donnent donc les probabilités de succès et d'échec de chaque scénario. Tous les événements se sont vus être attribués des probabilités issues des études FDMS pour les barrières techniques et celles calculées par le biais de la méthodologie RSSB présentée précédemment.

- *Variabilité des données*

Pour aller plus loin dans la prédiction, la volonté est d'intégrer une certaine variabilité sur les données. Une sensibilité liée aux éléments variables (affluence trafic, fatigue des agents, météo, etc…). En faisant varier certains paramètres, l'objectif est de pouvoir au maximum se rapprocher un peu plus de la réalité. Quelques exemples sont donnés ci-dessous.

Définition des facteurs :

- Facteur d'exposition

Affecter un facteur d'exposition aux probabilités finales de succès, données par les arbres d'événements, est un moyen de modéliser la durée d'exposition, en d'autres termes, le temps de maintenance. En effet, celui-ci a un fort impact sur la probabilité d'erreur. Ce facteur a donc été modélisé par la loi exponentielle dont la formule est la suivante :

$$y = e^{-0.006*t}$$

Exemple :

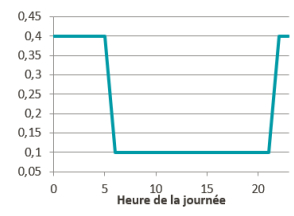
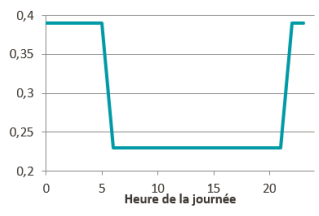
Temps de maintenance (en heure)	*0*	*1*	*10*	*30*
Probabilité de commettre une erreur (en %)	*2.0*	*2.6*	*7.7*	*18.2*

- Autres facteurs

- Visibilité

Selon le moment de la journée, qu'il fasse jour ou nuit, la probabilité de ne pas discerner le signal éteint évolue. Estimer la proportion de l'effet APOA pour l'EPC et in fine sur le HEP, qui sera une valeur comprise entre 0,1 (représentant un petit effet) et 1 (représentant le plein effet) maximum, repose sur le jugement de l'analyste. Nous considérons ici la sensilibilté de ce facteur de visibilité en fonction de l'heure.

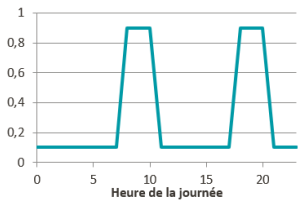
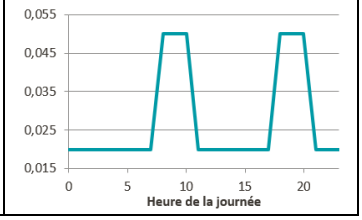
EPC : « Ln1. Un faible ratio signal/bruit »

Variation de l'APOA	***Variation de l'HEP***
Description : Variation de l'APOA en fonction du moment de la journée	Description : Probabilité que le conducteur ne localise pas le signal en fonction du moment de la journée
	

- Affluence du trafic

Selon le moment de la journée, que ce soit l'heure de pointe ou non, le risque d'erreur dans l'application des procédures (documents d'application, mémento, etc..) est différent. En effet, les périodes de pointes engendrent du point de vue système un nombre plus important de circulations, et du point de vue humain, davantage de stress et pression de régularité pour les opérateurs. La courbe de représentation de ce paramètre est présentée ci-après.

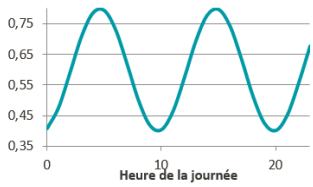
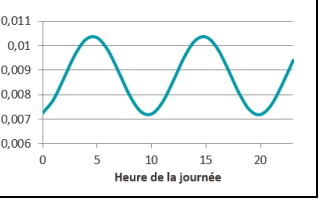
EPC : « T6. Peu ou pas de vérification de la sortie »

Variation de l'APOA	***Variation de l'HEP***
Description : Variation de l'APOA en fonction du moment de la journée	*Description : Probabilité qu'un voyageur traverse les rails en fonction du moment de la journée*
	

- Fatigue du conducteur

Selon le moment de la journée, le niveau de fatigue du conducteur n'est pas le même et donc la probabilité d'erreur peut se voir être impactée. Ce facteur est modélisé en se basant sur l'horloge circadienne du sommeil prouvée scientifiquement.

EPC : « T6. Peu ou pas de vérification de la sortie »

Variation de l'APOA	***Variation de l'HEP***
Description : Variation de l'APOA en fonction du moment de la journée	Description : Probabilité que l'agent de circulation fasse une erreur lors de la procédure en fonction du moment de la journée
	

Ainsi basés sur l'heure réelle de l'incident, tous ces facteurs prennent en compte le facteur humain et permettent la variation automatique des probabilités d'occurrences dans l'arbre d'évènement. Ils permettent aussi la prédictibilité d'évolution des indicateurs des exigences de sécurité si d'aventures l'anomalie venait à perdurer.

- *KVB (Dispositif technique)*

Pour quantifier la fiabilité de cet équipement, les études FMDS réalisées par la SNCF ont été utilisées.

$$\lambda = 1.3e - 10$$

$$R(t) = e^{-\lambda t}$$

- *Prédiction de l'évolution du trafic*

Afin de quantifier l'impact ponctualité engendré par un incident, des simulations ont été réalisées grâce au logiciel Open Track. En effet, sa fonctionnalité principale permet d'effectuer des simulations micros en y renseignant de nombreux détails comme l'infrastructure, le matériel, etc.

L'impact ponctualité va donc différer selon plusieurs paramètres comme la durée de l'incident, le chemin exploité, etc. Le *Tableau 1* reprend la moyenne des résultats des simulations dans le cas où le conducteur continue d'exploiter par la voie où le signal est éteint.

Durée de maintenance	Retard engendré
2 heures	1600 s/train
4 heures	3200 s/train
8 heures	6200 s/train
Supérieure à 24 heures	20 000 s/train

Tableau 1 - Retards engendrés

C. Interface Homme-Machine (IHM)

La conception de l'IHM du PoC, conformément au modèle, est divisée en deux vues principales :

- Vue macro : Tous les scénarii sont affichés simultanément,
- Vue micro : Le scénario préalablement choisi est affiché.

Une vue supplémentaire a été ajoutée afin de collecter les données nécessaires.

- Fenêtre n°1 :

Cette première fenêtre s'affiche à l'ouverture de l'interface avec pour objectif la collecte des principales informations liées à l'incident qui est survenu. Du type Localisation/Sens de circulation/Heure & nature d'incident/Temps de maintenance estimé.

- Fenêtre n°2 :

Cette deuxième fenêtre correspond à la vue macro figure 8. Dans le cadre noir, une animation représente graphiquement et explicitement, à la suite, tous les scénarii possibles. Ces mêmes scénarii sont repris dans le tableau situé sur la partie droite de la fenêtre. Celui-ci donne des indications sur le niveau de risques et de retards. Ces niveaux sont représentés sous forme de couleurs :

- Vert : Risques et retards faibles, voire inexistants
- Orange : Risques et retards moyens
- Rouge : Risques et retards importants

De plus, une barre de défilement a été installée, de manière à donner à l'utilisateur une première vue rapide sur le scénario considéré comme le plus risqué et celui le plus robuste, c'est-à-dire qui engendre le moins de retard. Enfin, il est possible, en cliquant sur un des scénarii du tableau, d'accéder à la 3ème et dernière fenêtre associée au scénario préalablement choisi.

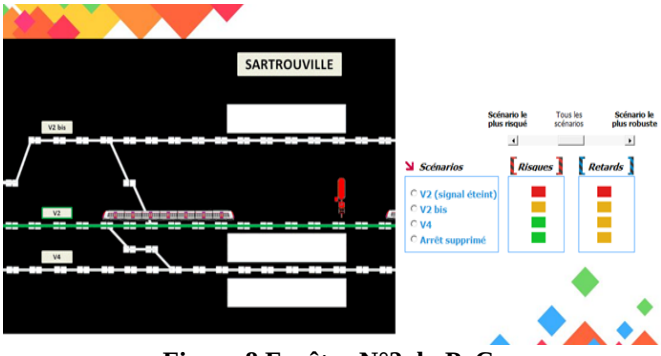


Figure 8 Fenêtre N°2 du PoC

- Fenêtre n°3 :

Cette dernière, considérée comme la plus importante de l'outil, représente la vue micro de chacun des scénarii. Au centre de la fenêtre, se trouve, une animation qui, correspond au scénario choisi. Les représentations graphiques mettent en lumière le risque encouru (e.g. traversée des voies par les clients, franchissement du signal éteint,..) de sorte à capter l'attention de l'utilisateur, à renforcer sa prise de conscience. Des éléments ont été insérés de manière à donner le contrôle à l'utilisateur pour qu'il puisse, lui-même, tester et simuler des situations différentes :

- Il peut modifier la durée de maintenance,
- Il peut activer ou non le plan de transport adapté (situation dégradée),

Après avoir déterminé tous les paramètres, le gestionnaire peut avoir en temps réel les résultats liés aux risques, au retard et à la fin prévisionnelle de l'incident. Deux colonnes présentent en juxtaposition les résultats estimés initialement et ceux prédits par la simulation. Des logo « i » information, permettent l'obtention d'informations supplémentaires. Dans le cas des risques, par exemple, les informations de compréhension indiquées sont liées à la méthodologie des calculs, mais également à la prévention des risques.

D. Pros and cons

- Plugin sur outils existant (gestion trafic)

A l'instar du projet PLASA dans sa partie Planning, nombreux sont les projets de recherche et développement de logiciel de gestion et optimisation de la fluidité d'exploitation des réseaux ferroviaires. Dans notre approche nous avons considéré les exigences de sécurité en intégrant les risques industriels, et aussi ceux de disponibilité. Il ne nous parait pas pertinent de créer un outil supplémentaire pour gérer la balance entre sécurité et disponibilité. Aussi, nous préférons inscrire ce PoC sous une future brique technologique qui serait implémentable dans les logiciels de gestion d'exploitation. Pour l'exploitant ferroviaire, il s'agit de produire en sécurité, et cela nous semble une opportunité, le fait de présenter les risques de sécurité dans ces interfaces. Au-delà du gain économique de développement, nous y voyons une manière de renforcer la conscience des risques, pour des managers de plus en plus éloignés du terrain.

Pour autant, d'un point de vue éthique la représentation des données dans l'outil à destination des managers, nécessite une prise de recul. Pour la sécurité industrielle, afficher des KPIs de dommages (e.g. nombres de morts, blessés graves, …) nous semble inadapté. Nous y préférons la représentation

du risque par la simulation, moins anxiogène et certainement bénéfique au regard de la prise de conscience. Pour ce qui concerne la disponibilité, le fait de s'intégrer dans un outil de gestion de l'exploitation du trafic en favorise l'explicitation.

Au-delà du domaine d'utilisation de l'outil, qu'il soit du niveau concepteur ou opérationnel, le PoC se révèle être un excellent vecteur de communication. L'évaluation des risques souvent absconse en dehors des experts en sûreté de fonctionnement, transposée sous la forme d'un outil simple devient alors un support de réflexion. : certains y devinant d'autres champs d'application possibles.

Si le lien entre évaluation des risques et outil d'aide à la décision est établi, reste à en définir les modalités, les standards pour consolider durablement les interactions entre ces deux processus.

V. Conclusion

Le concept d'un outil d'aide à la décision basé sur des évaluations des risques a été développé dans le cadre du projet européen PLASA sous l'initiative Shift2Rail. La SNCF sur la base de ces travaux a réalisé une preuve du concept sous la forme d'un PoC.

Les méthodes d'évaluation des risques appliquées sont des méthodes usuelles dans le domaine FMDS. Leur exhaustivité permet la souplesse nécessaire pour couvrir les nombreux cas d'usages ferroviaires. Un des critères de succès est d'associer des groupes pluridisciplinaires, que ce soit des experts métiers, facteurs-humains et de la sureté de fonctionnement.
L'existence de méthodes de quantification de fiabilité humaine offre une opportunité dans un domaine tel que le ferroviaire encore très peu automatisé avec une forte dépendance aux barrières humaines. Néanmoins la prise en compte des différents facteurs d'influence (environnement, interfaces,…) nécessite d'explorer des méthodes de quantification de deuxième (e.g. CREAM (Cognitive Reliability and Error Analysis Method) voire troisième niveaux (e.g. BORA Barrier- and Operational Risk Analysis). Il s'agit aussi et surtout de s'assurer que les résultats obtenus soient cohérents et corroborés par les analyses de retours d'expérience.
C'est un travail incrémental au long court, qui permettra à terme de bénéficier d'une base socle pour développer des solutions automatisées intégrant les nouvelles technologies comme l'intelligence artificielle, l'IoT, le big data. Dès lors le prospectif prendra tout son essor, et les puissances de calculs permettront d'offrir aux preneurs de décisions une réactivité quasi temps-réel.
Si les technologies liées à l'intelligence artificielle permettront la surveillance constante et un traitement prédictif des plus précis, il revient à l'Homme de continuer à évaluer les risques et à imaginer les IHM intelligibles. Cette démarche qui se veut intermédiaire, low tech, permet dès aujourd'hui de mettre à profit les approches de sureté de fonctionnement, de gestion des risques auprès des managers, qu'ils soient concepteurs ou opérationnels.

Acknowledgment

Les auteurs expriment leur reconnaissance à l'entreprise commune Shift2Rail pour le financement du projet PLASA (GA 730814) relatif aux travaux présentés ici.

Cette contribution reflete le point de vue des auteurs et ne reflete pas necessairement le point de vue ou la politique de l'entreprise commune Shift2Rail ou de la Commission europeenne.

Nous tenons à remercier Polytech Angers l'école d'ingénieurs de l'Université d'Angers avec qui nous avons développé au travers d'un stage le PoC, ainsi que les experts Synapses SNCF du cluster sécurité système et du cluster optimisation des ressources d'exploitation qui ont contribué activement à la production de ce projet.

References

[1] WP4.1 Deliverable - State of the art of risk assessment methods and presentation of the selected methods - 31/01/2017

[2] Anthony Legendre - Ingénierie système et Sûreté de fonctionnement : Méthodologie de synchronisation des modèles d'architecture système et d'analyse de risques – 15/12/2017

[3] Klein, G. 1999. « Sources of power: how people make decisions", The MIT Press - 1999

[4] Damasio, A. « L'erreur de Descartes : la raison des émotions », Paris, Odile Jacob - 1995

[5] Herbert A. Simon, Models of man : social and rational : mathematical essays on rational human behavior in a social setting, New-York, Wiley - 1957

[6] D. Anzieu, J.Y. Martin, La dynamique des groupes restreints, PUF - 1986

[7] Project Gosafe Rail : Global safety Management Framework for Rail Operations, Shift2Rail ID:730817 (http://www.gosaferail.eu/)

[8] Bhattacharjee and Al. - An artificial neural network-based ensemble model for credit risk assessment and deployment as a graphical user interface – 2017

[9] WP4.2 Deliverable - Requirements to conduct a risk assessment study on the complete railway system - 31/11/2017

[10] WP4.3 Deliverable - Examples of safety management based on risk assessment – 30/09/2018

[11] Williams, J.C - HEART – The Human Error Assessment and Reduction Technique - 1985.

[12] Huw, G. - RSSB - Railway Action Reliability Assessment user manual - 06/2012.