UNE MATRICE DE RISQUE : POUR FAIRE QUOI ?
A RISK MATRIX: FOR WHAT USE?

Olivier CASTELLANI
SNCF – Centre d'Ingénierie du Matériel
4 allée des Gémeaux 72100 LE MANS

Jean-Marc POURCHIER
SNCF – Direction de la Sécurité Système et Projets
20 rue de Rome 75008 PARIS

Sandrine CHRUN et Jean-Marie CLOAREC
SYSTRA – Direction Systèmes de Transport
72 rue Henry Farman, 75015 PARIS

Résumé
La matrice de risque est un outil largement enseigné, présenté dans les normes FMDS de tous les secteurs et auquel la plupart des contrats font référence. Cependant, il n'y a aucune homogénéité sur la manière de l'utiliser ni sur la définition des concepts sous-jacents.
Nous expliquerons pourquoi les décisions qui concernent l'acceptation des risques dans le milieu ferroviaire sont généralement justifiées et partagées entre experts concernés, mais ne sont pas souvent fondées sur l'utilisation de cette matrice.
Nous expliquerons enfin pour quel cas l'utilisation de la matrice est pertinente (s'il y en a).

Summary
The risk matrix is a tool largely taught, presented in RAMS standards of all sectors, and to which most contracts refer. However, there is a lack of homogeneity on the way to use it, and on the definition of its underlying concepts
We will explain why the decision concerning the risk acceptance in the railway domain are generally justified and shared among concerned actors, but are not always based on the use of this matrix.
We will also explain in which case the use of a matrix is relevant (if any).

Contexte

Il est couramment admis que l'on utilise une matrice de risques pour évaluer le niveau de risque acceptable d'un système au cours d'une étude de sécurité, et par extension définir l'objectif de sécurité. Cette pratique s'applique, théoriquement, à tout type de système et de technologie. Les premières matrices sont apparues avec les normes US de la série des MIL-STD.
Dans le domaine ferroviaire, c'est l'EN 50126 qui donne les bases applicables de définition et d'utilisation de la matrice de criticité.
L'expérience tirée de plusieurs projets ferroviaires, tant nationaux qu'internationaux, montre que, quand ils y font référence, les ingénieurs ne se posent même plus la question de savoir si une matrice de criticité répond bien à leur besoin et, dans le pire cas selon nous, réutilisent des matrices qui « ont fait leur preuve » sur des projets précédents. Nous supposons d'ailleurs que cette problématique n'est pas spécifique au domaine ferroviaire.
Les auteurs ont constaté, dans leur travail au quotidien dans le domaine ferroviaire, l'emploi de cet outil sans plus de réflexion quant à son adéquation au sujet traité.

Mais si on creuse un peu la question, autrement dit si on met en doute la pertinence de la matrice dans son usage courant, on se rend compte que ce n'est pas si simple, et on en vient à s'interroger sur son utilité réelle.

Contenu de la réflexion

Il s'agit de réinterroger les concepts qui sont couramment associés à l'idée de la matrice des risques (fréquence, gravité, criticité…), de montrer que leur utilisation ne va pas de soi, et que le discours théorique sur ces concepts peut faire dévier les réflexions de l'objectif réel, et conduire à de mauvaises prises de décision. Nous allons donc décortiquer les différents items qui composent l'outil « matrice de risque », et nous interroger sur son domaine de pertinence.

Une image culinaire peut résumer notre point de vue : il est possible de disserter à l'envie sur le fait de savoir si une tomate est un fruit ou un légume, d'ailleurs les biologistes ont beaucoup d'arguments à nous proposer. Cependant, il n'est pas nécessairement utile d'avoir répondu à cette question pour cuisiner un bon gazpacho. Ce qui importe réellement, c'est de connaître les propriétés utiles au but recherché, et de s'assurer de la pertinence et de la validité des concepts employés dans le contexte du système étudié.

1. Le diagnostic : le concept semble clair, mais il pose beaucoup de questions

1.1. La théorie est simple…

Dans le domaine ferroviaire, la référence communément acceptée en la matière est la norme EN 50126.
Les matrices de risque sont typiquement construites par une combinaison :

- D'une échelle de gravité, ex :

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

Tableau 1. Exemple de catégories de gravité utilisées dans le ferroviaire

Comme on peut le voir dans cet exemple, les classes de gravité peuvent décrire plusieurs critères à la fois (ex : ici, les aspects sécurité et disponibilité sont évoqués).
Nous donnons ci-après un autre exemple non dédié au domaine ferroviaire, qui montre également que des classes de gravité peuvent ne pas se cantonner à des conséquences en termes de blessure/mort :

Gravité	Effet de la défaillance	Objectifs	Niveau
Catastrophique	L'avion ne peut voler de façon sûre, perte de l'avion, de l'équipage ou de passagers	10^{-9}	A
Dangereux	Réduction importante des marges de sécurité ou des fonctions, augmentation importante de la charge de travail pour l'équipage, blessures sévères	10^{-7}	B
Majeur	Réduction significative des marges de sécurité ou des fonctions, augmentation de la charge de travail pour l'équipage, inconfort ou blessures possibles	10^{-5}	C
Mineur	Réduction légère des marges de sécurité ou des fonctions, augmentation de la charge de travail pour l'équipage, inconfort	10^{-3}	D

Tableau 2. Exemple de catégories de gravité utilisées dans l'aérien

Dans l'exemple ci-dessus, on peut voir que le champ de la gravité ne se limite pas uniquement aux conséquences, mais traite également d'une « réduction des marges de sécurité », c'est-à-dire par exemple de pertes de barrière (ex : redondance, système de contrôle…).

Le tableau suivant montre que parfois le découpage des classes de gravité peut être beaucoup plus (trop ?) raffiné :

Category	Harm to persons	Material damage, costs for elimination of environmental damage, extent of service interruptions
I	Malaise	< 1000 CHF
II	Light injury (single person)	1000 – 100 000 CHF
III	2..10 persons with light injuries or 1 person with serious injuries	> 100 000 – 1 Million CHF Interruption of medium size station for 1 hour
IV	2..10 persons with serious injuries or 1 fatality	> 1 Million CHF – 10 Million CHF Interruption of big node for several hours
V	2..10 fatalities	> 10 Million CHF – 100 Million CHF Interruption of big node for several days
VI	More than 10 fatalities	> 100 Million CHF Interruption of large part of network for several days

- D'une échelle de fréquence, ex :

Catégorie	Description	Ordre de grandeur
Fréquente	Situation dangereuse continuellement présente	Se produira plus d'une fois par an
Probable	Survient souvent	Se produira souvent (tous les 2 ou 3 ans) dans la vie de l'engin
Occasionnelle	Survient à plusieurs reprises	Se produira quelques fois (<10) dans la vie de l'engin
Rare	Se produit à un moment du cycle de vie du système	Se produira une fois dans la vie de l'engin
Improbable	Peut exceptionnellement se produire	Se produira une fois dans la vie du **parc**
Invraisemblable	Ne se produira à priori pas	Ne doit pas se produire dans la vie du **parc**

Tableau 3. Exemple de catégories de fréquence

Comme on peut le voir dans cet exemple, donner des ordres de grandeur correspondant aux classes définies permet de donner une échelle de valeur qu'il est plus facile de partager.

En l'absence des ordres de grandeurs, les termes utilisés dans les descriptions des catégories de fréquences peuvent être comprises de manières différentes en fonction des personnes et des projets.

- D'un critère d'acceptabilité du risque, ex :

Inacceptable	Inacceptable, doit être éliminé
Indésirable	Acceptable uniquement si la réduction du risque est impossible, et avec accord du client
Acceptable	Acceptable moyennant un contrôle approprié et l'accord du client
Négligeable	Acceptable sans nécessité d'accord du client

Tableau 4. Exemple de catégories d'acceptabilité

Ces trois données sont alors combinées pour construire une matrice, qui attribue une classe d'acceptabilité à chaque couple [gravité ; fréquence], ex :

	A Fréquent	B Probable	C Occasionnel	D Rare	E Improbable	F Invraisemblable
IV Catastrophique	Inacceptable	Inacceptable	Inacceptable	Indésirable	Indésirable	Acceptable
III Critique	Inacceptable	Inacceptable	Indésirable	Indésirable	Acceptable	Négligeable
II Marginal	Inacceptable	Indésirable	Indésirable	Acceptable	Négligeable	Négligeable
I Insignifiant	Indésirable	Acceptable	Acceptable	Négligeable	Négligeable	Négligeable

Tableau 5. Exemple de matrice de risque

1.2. …mais la pratique est problématique :

Ce qui a été évoqué ci-dessus semble simple, mais amène pourtant beaucoup de questions épineuses.
En effet, nous avons constaté, au cours de différentes études, qu'il existait une grande disparité quant à la définition d'une matrice de risque.
Le mieux étant de l'illustrer par les exemples suivants en s'intéressant, dans un premier temps, uniquement à l'échelle de fréquence.

Projet		→	1/2 semaines	↔	1/mois	↔	1/an	↔	1/10 ans	↔	1/100 ans	↔	1/1 000 ans	↔	1/10 000 ans	↔	1/100 000 ans	↔	1/1 000 000 ans	←
TR 50126	1	FQ		FQ		PRB		OCC		IMP		INC								
TGV 1	2	CON		VFQ		FQ		PRB		OCC		UL		VUL		REM		IMP		INC
TGV 2	9	FQ		FQ		PRB		OCC		REM		REM		IMP		IMP		INC		
TGV 3	12	FQ		FQ		PRB		OCC		REM		REM		IMP		IMP		INC		
Métro 1	3	FQ		FQ		FQ		PRB		OCC		REM		IMP		VUL				
Métro 2	4	VFQ		FQ		PRB		OCC		REM		UL		IMP		INC				
Métro 3	7	FQ		PRB		PRB		OCC		OCC		REM		REM		IMP		IMP		INC
RER	5	FQ		FQ		PRB		OCC		REM		IMP								
Tramway 1	6	FQ		PRB		OCC		OCC		OCC		REM		REM		IMP				
Tramway 2	8	FQ		FQ		PRB		OCC		REM		REM		IMP		IMP		INC		
Tramway 3	10	FQ		FQ		PRB		OCC		REM		REM		IMP		IMP		INC		
Tramway 4	11	FQ		FQ		PRB		OCC		REM		REM		IMP		IMP		INC		
Tramway 5	13	FQ		FQ		FQ		PRB		OCC		OCC		IMP		IMP		IMP		INC
Tramway 6	14	FQ		FQ		FQ		FQ		PRB		OCC		REM		IMP		INC		
Proba horaire					1,00E-03		1,00E-04		1,00E-05		1,00E-06		1,00E-07		1,00E-08		1,00E-09			

Tableau 6. comparaison de critères d'acceptabilité de risque entre différents projets

Si on regarde la classe de fréquence située entre 1 défaillance par an et 1 défaillance tous les 10 ans, on constate que les interprétations de cette classe sont : occasionnelle (OCC), probable (PRB) et fréquent (FQ). Si on regarde les systèmes :

- TGV : la classe est soit PRB pour TGV1, soit OCC pour TGV2 et TGV3,
- Metro : la classe est soit PRB pour METRO1, soit OCC pour METRO2 et METRO3,
- Tramway : on va de FQ pour Tramway 6, à PRB pour Tramway 5, jusqu'à OCC pour Tramway 1 à 4

Si on regarde maintenant, tous systèmes confondus, pour la classe de fréquence située entre 1 défaillance tous les 100 ans et 1 défaillance tous les 1000 ans, on va naviguer de OCC à UL (Unlikely) en passant par REM et IMP.

Enfin, si on essaye de rebâtir la matrice de risque, on va arriver à des matrices différentes. Exemple :

	FQ	PRB	OCC	REM	IMP	INC
CAT						
CRIT						
MARG						
INS						

METRO 3

	FQ	PRB	OCC	REM	IMP	INC
CAT						
CRIT						
MARG						
INS						

Tramway 6

Tableau 7. comparaison entre 2 matrices de risque de différents projets

Même si les différences ne sont fondamentales, on voit qu'on risque de ne pas prendre la même décision suivant où on se trouve.
Exemples :

- Pour le couple (CRIT, PRB), le critère d'acceptabilité est « inacceptable » pour METRO3 quand il est « indésirable » pour Tramway 6
- Pour le couple (CRIT, INC), le critère d'acceptabilité est « acceptable » pour METRO3 quand il est « négligeable » pour Tramway 6.

Il en résulte qu'un manque de réflexion approfondie sur la définition des différents critères d'acceptabilité sous-tendant la matrice de risque, conduira à des matrices différentes et donc des décisions également différentes selon les projets, ce sans que l'on se soit réellement posé la question de la « normalité » de cette disparité.

Il reste maintenant à savoir comment cet outil s'utilise, et devrait être utilisé.

2. On ne peut faire l'économie de réinterroger les concepts de base

2.1. Concept de la gravité

Afin de déterminer un objectif généralement de sécurité associé à chaque évènement redouté identifié, il y a lieu d'établir en premier lieu des classes de gravité qui soient adaptées au contexte du projet et au but recherché, et suffisamment claires afin que le classement ne soit pas problématique (ex : évènement qui pourrait être classé dans 2 classes à la fois).

2.1.1. Les classes de gravité sont à adapter en fonction du contexte du projet et du but recherché

La conception doit-elle être validée en terme de sécurité, fiabilité, disponibilité, … voire une combinaison de ces grandeurs ? Dans ce cadre, une même classe de gravité peut couvrir plusieurs de ces dimensions. Ainsi par exemple : la conception est-elle équivalente entre une défaillance amenant à un accident catastrophique, donc plusieurs morts, et une défaillance amenant l'impossibilité d'utiliser le système pendant une journée ?
Il est alors important de s'assurer de la cohérence entre ces différentes dimensions. Les classes de gravité servent surtout à classer du plus « grave » au moins « grave » les évènements redoutés identifiés. Il faudrait donc d'abord regrouper ces évènements de manière à identifier des groupes dont les conséquences sont de même nature, puis définir textuellement ces classes de gravité. Par exemple, quelle que soit la définition des classes qui sera retenue in fine, les experts savent intuitivement qu'il faudra placer la « collision » et « l'ouverture intempestive d'une seule porte » dans deux classes différentes.

Indépendamment de l'utilisation ou non d'une matrice, il est particulièrement important d'adapter la définition des classes de gravité à la phase concernée. En effet, en conception, on ne peut qu'imaginer les conséquences potentielles d'une défaillance. On pourrait certes se référer aux statistiques d'accidents antérieurs, mais il peut être dangereux d'en tirer des conclusions trop fines. En effet, ces statistiques portent par définition sur des systèmes pour lesquels protections et barrières sont déjà en place. Utiliser de manière « aveugle » celles-ci conduit à des raccourcis du genre de :

- « il n'y a pas de morts lors des déraillements, donc l'accident n'est pas à classer en catastrophique » → c'est oublier que beaucoup de trains ont des bogies inter-caisse qui permettent justement de fortement diminuer l'impact d'un déraillement. C'est oublier également plus récemment le désastre de Brétigny.
- « il n'y a jamais plus d'un mort lors d'une collision frontale, donc la sécurité peut être baissée » → c'est oublier que le fait qu'il n'y ait pas de mort provient justement des équipements de sécurité existant ainsi que de la sécurité passive en place (sans cela, nous avons par exemple l'accident de Melun, 1913, 40 morts).

Le concept de « gravité » diffère selon qu'on est en phase de conception d'un système nouveau ou modifié ou d'analyse statistique des performances d'un système existant :
Lors des analyses statistiques, il est pertinent de différencier « blessés graves » et « morts », ce n'est pas le cas en conception.
En effet, comment est-il possible d'être sûr qu'un accident comme un déraillement provoquera un ou plusieurs blessé(s) grave(s), mais aucun mort ? D'autant plus qu'un blessé grave peut mourir des séquelles de ses blessures.
Cela peut se résumer de la manière suivante : est-il possible en conception de considérer qu'une défaillance ne peut pas provoquer de morts, mais par contre des blessés graves ? Notre réponse à cette question est « c'est impossible », c'est pourquoi en phase de conception nous ne faisons pas de différence entre blessé grave (donc mort potentiel si non traité médicalement à temps) et mort (blessé grave qui n'a « pas eu de chance »).

2.1.2. La frontière entre les classes doit être claire

Hésiter entre plusieurs classes peut avoir des conséquences lourdes sur la conception qui en découle.
De ce point de vue, il peut être dangereux de faire se chevaucher des définitions (ex : catastrophique = plusieurs morts, critique = un mort ou plusieurs blessés graves, …). Pour exemple, en utilisant le Tableau 5. Exemple de matrice de risque présenté ci-dessus : si l'on a situé un risque dans la case « rare ; insignifiant », il suffit d'avoir mésestimé la gravité ou la fréquence pour passer de la zone « négligeable » à « acceptable ». Pire encore, si l'on a mésestimé à la fois la fréquence et la gravité, le risque aurait même dû être jugé « indésirable ». Pour un seul risque, on peut donc hésiter entre 3 classes d'acceptabilité si les frontières sont mal définies !

En matière de sécurité il est prudent, en cas de doute entre plusieurs classes de gravité, de retenir la plus élevée, mais cela peut engendrer des surcoûts par rapport au résultat qui aurait été obtenu avec une analyse plus fine. Cela renforce la nécessité d'avoir une frontière adaptée aux circonstances et la plus claire possible afin d'empêcher ce type de doutes.

2.2. Concept de fréquence

Le concept de « fréquence » (nature mathématique, unité, caractère qualitatif ou quantitatif…) **dépend de la nature du système étudié**. Il peut être exprimé par exemple avec un taux de défaillance (par heure, par sollicitation, par cycle, par unité de distance parcourue, par mission…), avec une probabilité sans dimension, de façon qualitative (par exemple : concept de « SIL » pour le système programmés)…

Nous ne nous étendrons pas sur les chausse-trappes résultant d'une mauvaise compréhension de concepts mathématiques parfois subtils (par exemple : confusion quant à l'utilisation et la combinaison de taux, de probabilités, ou autres dans un arbre de défaillance, …), ou d'une application en dehors de leur domaine de pertinence (par exemple utilisation à tort de fréquences pour des défaillances systématiques, pour le facteur humain…). Il faut cependant rappeler la nécessité d'assurer la compatibilité des différentes approches lors de l'intégration de sous-systèmes de nature technologique différente dans un système de plus haut niveau.

De même que pour le concept de gravité il ne faut pas assimiler les fréquences des défaillances techniques aux statistiques des accidents, puisque ces statistiques portent par définition sur des systèmes pour lesquels protections et barrières sont déjà en place. Utiliser de manière « aveugle » celles-ci pourraient amener à des raccourcis.

Il faut aussi éviter le raccourci « c'est très rare, donc ce n'est pas grave » (sic), puisque c'est bien pour cela que les critères d'acceptabilité ont été mis en place.

En phase amont de la conception, dans le cas d'un système complexe, définir une fréquence d'un évènement redouté a-t-il un sens ?
En effet, si on ne connait pas l'architecture du système, comment définir la probabilité d'occurrence de l'évènement redouté ?
Si on se sert du REX d'un autre projet, ce REX tient déjà compte des barrières de sécurité en place qui servent à minimiser l'occurrence et/ou la gravité potentielle de l'évènement redouté, donc les valeurs issues du REX ne sont pas pertinentes pour un système en phase de conception, où ces barrières peuvent ne pas exister ou être différentes.
De plus, les technologies utilisées pour un système complexe mettent en jeu des fréquences qui ne sont pas comparables. L'électronique ne défaille pas comme de la mécanique. Un système mécanique peut fonctionner longtemps en mode dégradé sans pour autant être considéré comme en panne : la fréquence de la panne est donc difficile à appréhender. De même, qu'en est-il des systèmes combinant des technologies différentes (relais électropneumatique, électromécanique, …).
Les fréquences définies n'ont donc de sens qu'au niveau de la défaillance technique qui engendre directement (sans défaillance supplémentaire) l'accident potentiel.

2.3. Concept d'acceptabilité

Selon la norme EN 50126, un des objectifs est de décider, si un couple (gravité des conséquences / fréquence) associé à un risque est acceptable en l'état, ou bien dans quelle mesure des mesures de couverture du risque doivent être prises. Il faut affirmer clairement que la frontière entre les différentes zones découle d'un choix « politique », d'un ressenti du public… Elle ne découle pas d'un raisonnement rationnel d'ingénieur ; il est donc normal qu'elle puisse différer en fonction du contexte (géographique, économique, politique, …).

En toute logique, **c'est l'Etat, garant de l'ordre public, qui doit fixer les critères d'acceptabilité des risques**. Dans le ferroviaire, un certain nombre de textes règlementaires, issus du droit français et européen, poursuivent cet objectif. On notera en passant que ces objectifs, portant sur la modification de systèmes existants ou sur conception de nouveaux systèmes, ne sont pas nécessairement atteints par des systèmes existants anciens qui sont pourtant réputés tout à fait acceptables.

On a vu, en 1.1, tableau 3, qu'il est possible de définir différents niveaux d'acceptabilité (ex : « inacceptable », « indésirable », « acceptable », « négligeable ») qui correspondraient à différents niveaux de gestion des risques. Cette multiplication de niveaux entraîne de nombreuses questions, dont les suivantes :

- Combien de classes d'acceptabilité faut-il ? Ne peut-on se contenter de deux classes « Inacceptable » / « Acceptable » ?
- Lorsqu'un objectif est associé à une gravité, à quelle niveau d'acceptabilité doit-il être associé ?
- Pour une gravité donnée, faut-il fixer un objectif différent pour chacun des niveaux d'acceptabilité ?

Cette différenciation entre niveaux d'acceptabilité introduit donc une complexité certaine. On pourrait évacuer ces questions en ne retenant que deux niveaux, considérant que, puisqu'il s'agit de prendre une décision, il serait dans la majorité des cas plus simple de n'avoir qu'une frontière unique entre l'acceptable et l'inacceptable : Si un risque est jugé « inacceptable », on conçoit alors des mesures de couverture du risque d'où il découle un déplacement de ce risque dans le plan gravité/fréquence, puis on vérifie si le risque est rentré dans la zone « acceptable » après prise en compte de ces mesures. L'acceptation d'un risque doit être partagée par toutes les parties prenantes : autorités, client, concepteur, …

Notons que les cadres règlementaires français et européen ne s'embarrassent généralement pas de subtilités : Soit le système est conforme aux exigences de la règlementation (référentiels à respecter, objectifs à démontrer, …), soit il ne l'est pas. En cas de demande de dérogation, l'autorité compétente (ex : l'Etablissement Public de Sécurité Ferroviaire pour le ferroviaire) considère qu'une fois la dérogation accordée le système est devenu conforme à la règlementation (tant que les conditions auxquelles cette dérogation a été accordée restent valables bien entendu). Lorsqu'un niveau d'acceptabilité est lié à la viabilité économique du projet, l'acceptation du risque revient à une demande de dérogation tel qu'expliqué ci-dessus.

Lorsque la matrice est utilisée pour communiquer entre un client et un fournisseur dans le cadre d'un contrat, il est dangereux de définir une classe d'acceptabilité où aucun accord du client n'est recherché (par exemple, la classe « négligeable » du tableau 4 ci-dessus au §1.1) car il s'agit alors de « quitte ou double » : le risque ne sera évalué par le client qu'à la fin du projet alors que la conception est figée, tout désaccord à ce stade sera alors extrêmement coûteux. Cette classe amène souvent des raccourcis du genre « oui ça sera largement bon, donc pas besoin de travailler sur le sujet », ex : cette fonction est classique, mais on n'a pas vérifié si les contraintes du contrat sont les mêmes que pour les conceptions existantes (ex : température polaire, CEM, milieu salin, …).

2.4. Niveau d'application de la matrice

Il est courant de définir une matrice dans un contrat sans expliciter le niveau auquel cette matrice doit s'appliquer.
Une matrice peut en effet théoriquement s'appliquer à maints niveaux : composant, sous-système, grand sous-système tel que « porte », système train, système ferroviaire dans son ensemble. On peut y placer aussi des évènements externes (feu, tremblement de terre, conditions météo extrêmes,

Le jeu consiste ensuite à gérer les rapports entre ces différents niveaux d'analyse et à s'assurer de leur compatibilité, étant entendu que l'acceptabilité ne doit se décider que sur le système global :

- L'« acceptation » d'un risque au niveau d'un composant ne signifie en aucun cas son acceptation au niveau train (ex : la défaillance du composant ne peut pas provoquer de mort, mais pour autant il intervient dans le système porte, et ce dernier peut en cas de défaillance provoquer des accidents mortels).
- En revanche, entre une application « grand sous-système » et une application train, la différence est souvent négligeable.

Afin d'assurer la complétude de l'étude et d'éviter de disserter sur de faux problèmes, un bon moyen est de retenir comme niveau d'application du critère d'acceptation le niveau le plus bas où l'évènement redouté considéré peut amener directement à l'accident sans défaillance supplémentaire. Ainsi par exemple : l'ouverture d'une porte en ligne entraîne la chute de voyageur, l'absence de détection incendie entraîne la morts en cas d'incendie, sachant que l'incendie n'est pas une « défaillance technique ».

3. La matrice est-elle utilisée là où c'est pertinent ?

3.1. A quoi sert cette matrice ?

La matrice de risque n'est, au fond, qu'un moyen d'afficher des choix politiques en matière d'acceptation des risques. On peut dans ce cadre distinguer trois utilisations classiques mais pas forcément pertinentes :

- Déterminer un objectif à appliquer pour chacun des évènements redoutés identifiés (et donc influer sur la conception)
- Vérifier qu'une conception est bien conforme à un objectif déterminé au préalable (et donc valider des choix de conception). Notons que cet objectif peut être exprimé sous une forme non quantitative (ex : nombre de défaillances indépendantes, maintenance associée, …).
- Présenter sous une forme graphique des données de retour d'expérience.

Nous allons dans les paragraphes suivants évaluer l'adéquation de l'outil matrice pour ces 3 utilisations classiques.

3.1.1. Détermination d'un objectif

Le principe est de partir de la liste des évènements redoutés qui ont été identifiés (ex : par l'intermédiaire d'une Analyse Préliminaire de Risques).
Il s'agit alors de déterminer pour chacun de ces évènements redoutés (de sécurité, de fiabilité…) l'objectif à y associer, en fonction de la gravité potentielle de ses conséquences. Cet objectif sera par la suite décliné en termes de conception, par une architecture (allocations de fiabilité, nécessité ou non de redondance, de système de contrôle, type(s) de technologie(s) utilisée(s)…), et un choix de composants, avec bien entendu un coût associé.

La question qui se pose alors est « pourquoi utiliser une matrice pour cela ? ». En effet, puisque le but est d'associer un objectif de sécurité, en fonction de la gravité des conséquences potentielles de l'évènement redouté considéré, on pourrait se contenter d'un tableau qui met en face de chaque classe de gravité une fréquence maximale acceptable.

C'est pourquoi, pour répondre à ce besoin, il suffirait d'associer un objectif à chaque classe de gravité. Le formalisme d'une matrice n'est pas absolument nécessaire pour cela.

3.1.2. Validation d'une conception

Il s'agit d'évaluer la conception choisie. Cela peut se faire :

- Soit en phase de préconception, il s'agit alors d'un avis d'expert afin de déterminer si l'on est « bien parti » avec cette conception.
- Soit en phase de validation, lorsque la conception est « figée », afin de confirmer que la solution choisie répond bien au besoin.

En phase de validation, le but est de comparer le résultat calculé de la dite conception à un objectif prédéterminé (associé à la gravité potentielle de l'évènement redouté étudié). La matrice n'est alors pas spécialement utile puisque la question est essentiellement de savoir si l'objectif prédéterminé est atteint ou non (par exemple : un taux de défaillance est inférieur ou non à une valeur fixée, avec un niveau de confiance donné).

Les questions intéressantes qui découlent de cette analyse sont généralement partagées par les experts, mais elles ne requièrent pas forcément l'utilisation d'une matrice pour être résolues, ce sont les suivantes :

- Si le système étudié obtient des résultats largement meilleurs que l'objectif, quelles en sont les conclusions à tirer ? Doit-on reconcevoir pour moins cher ? Une communication au client est-elle nécessaire ? Peut-on relâcher la maintenance initialement prévue ? …
- Si le système étudié obtient-il des résultats légèrement moins bons que l'objectif, que faut-il faire ? Reconcevoir le système ? ça reste acceptable mais renforcer la maintenance ? Rajouter des contraintes d'exploitation ? …

La matrice peut toutefois être intéressante si l'on a besoin d'une vision globale ; elle permet de placer les uns par rapport aux autres les risques identifiés et traités lors de la conception, afin d'éclairer les décisions à prendre quant à la nature d'éventuelles actions de re-conception à consentir (prévention, protection…).

3.1.3. Représentation graphique des données du REX

Le principe est d'évaluer la gravité en termes de gravité potentielle (ex : déraillement = gravité IV) de chacun des évènements redoutés qui sont suivis dans le cadre du retour d'expérience, comme cela serait fait dans les 2 cas précédents, mais par contre utiliser la fréquence observée dans l'exploitation réelle : en fonction du nombre de défaillances connues qui auraient pu amener à l'accident étudié. Les classes d'acceptabilité seront alors par exemple du type :

- Pas d'action,
- A surveiller,
- Re-conception nécessaire, sous telle durée,
- Interdiction d'exploitation tant que le système n'a pas été reconçu,
- …

Ici aussi, l'intérêt essentiel de la matrice est d'offrir une vision globale en plaçant les uns par rapport aux autres les risques gérés par l'exploitant afin d'éclairer les décisions à prendre : fixer des priorités, déterminer la nature des actions à consentir (prévention, protection…).

3.1.4. Si donc cette matrice n'est pas indispensable, par quoi la remplace-t-on ?

La noblesse du métier ferroviaire consiste à faire cohabiter harmonieusement des équipements de génération et de techniques différentes. Le problème qui se pose habituellement est de modifier un système préexistant, par exemple en y intégrant un nouveau type d'équipement (ex : nouveau type de matériel roulant, de poste d'aiguillage, de procédure, de processus…). **Dans ce cadre, il est clair que la matrice n'est d'aucun secours pour conduire les études relatives à la sécurité.** Il n'est en effet jamais vraiment possible de ré-identifier ni de réévaluer tous les risques potentiels,

car il faudrait alors rétro-concevoir l'ensemble du système. **Il y a heureusement d'autres façons de faire qui sont très convaincantes et généralement reconnues** y compris par les autorités de tutelle : en effet, le niveau de sécurité du système ferroviaire existant étant considéré comme satisfaisant, des **référentiels reconnus** (normes, règles de l'art, exigences techniques légales…) sont réputés clore les risques classiques. Dans cette logique, l'APR doit se concentrer sur l'identification des risques qui seraient nouveaux ou accrus en raison d'innovations, qu'elles soient fonctionnelles, technologiques, ou dans le domaine et l'environnement d'exploitation. Lorsqu'il n'y a pas de référentiel adapté, on peut comparer les risques identifiés à ceux d'un **système** dit « **de référence** » reconnu comme acceptable, et faire une étude des conséquences des écarts entre le système étudié et le système de référence susdit.

Reste alors ce qui, dans des nouveaux systèmes « clef en main » ne peut être traité ainsi que les aspects, finalement assez rares sur les réseaux existants, où l'on ne disposerait ni de référentiel ni de système de référence ; on doit alors prouver que les risques sont « négligeables ». Oui, mais « négligeables » par rapport à quoi ? C'est ici qu'un tableau qui met en face de chaque classe de gravité une fréquence maximale acceptable ou un objectif de sécurité est indispensable. **Ce qui est important dans ces quelques cas ce n'est donc pas la matrice, mais juste d'associer à chaque classe de gravité un objectif de sécurité adéquat**, donc permettant de conclure que le risque est « acceptable ».

Conclusion

On voit donc que ce qui semblait acquis et de pratique courante a masqué un travail de réflexion de fond sur le QQOQCP :

- Q (quoi) : qu'est-ce que la matrice ? (« fréquence », « gravité », « croisement des deux »)
- Q (quand) : quand dois-je l'utiliser ?
- O (où) : à quel niveau du système puis-je l'utiliser ?
- Q (qui) : qui définit la matrice, qui l'utilise et qui définit les actions à mettre en œuvre découlant de l'utilisation de la matrice ?
- C (comment) : comment la matrice est-elle définie et comment s'utilise-t-elle ? (en particulier, doit-on systématiquement réduire la criticité à une multiplication ?)
- P (pourquoi) : enfin, pourquoi avons-nous besoin d'une matrice ? la matrice est-elle un outil pertinent ?

Notre conclusion est donc qu'il convient de remettre en cause l'usage même de la matrice, sachant que les utilisateurs ont trop souvent concentré leur attention (et les efforts qui vont avec) sur l'outil lui-même plutôt que sur le but à atteindre.

Tout bien considéré, la matrice est surtout intéressante pour sa valeur pédagogique : elle permet d'expliquer les concepts essentiels de la maîtrise des risques en les mettant « spatialement » en scène. Elle est aussi intéressante lorsqu'il s'agit d'illustrer une situation globale (quels sont les grands enjeux, où en suis-je dans le traitement des risques présentés par le système en conception, où dois-je faire porter les efforts sur un système en exploitation étant donné le retour d'expérience disponible…), mais elle n'est pas très utile pour prendre des décisions précises (j'accepte ou non de prendre tel risque particulier). De fait, le secteur ferroviaire utilise les démarches d'acceptation du risque issues de son expérience et de sa spécificité évoquées au § 3.1.4, qui ne nécessitent pas cet outil.

Nous conclurons par cette question au lecteur : « les ambigüités vécues, les questions posées par les auteurs et leur façon de les résoudre sont-elles pertinentes dans des domaines autres que le ferroviaire… ? »

Références

Normes US de la série de MIL-STD.

EN 50126 : Applications ferroviaires – Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenablité et de la sécurité (FDMS)

EN 50128 : Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Logiciels pour systèmes de commande et de protection ferroviaire

EN 50129 : Applications ferroviaires – Systèmes de signalisation, de télécommunications et de traitement – Systèmes électroniques de sécurité pour la signalisation

De façon générale, tous les cours de SdF qui présentent la matrice des risques.

Mots clés

Matrice, sécurité, disponibilité, fiabilité, décision, GAME, ALARP