2006

Sur les rôles respectifs de l'homme et du matériel dans la sécurité d'un système de transport

par Robert GABILLARD

Professeur à l'Université
des Sciences et Techniques de Lille

et Michel FICHEUR

Ingénieur des Ponts et Chaussées
Directeur du Service Métro à l'Établissement Public
d'Aménagement de la Ville Nouvelle de Lille-Est

A l'occasion de la réalisation du métro de Lille, à partir du système VAL à conduite entièrement automatique, d'importantes études de sécurité sont menées par MATRA, ensemblier de la réalisation, avec le concours du maître d'ouvrage, le Service Métro de l'EPALE, et de l'équipe du Professeur Gabillard de l'Université des Sciences et Techniques de Lille. L'ensemble de ces études est suivi pour le Ministère des Transports par l'Institut de Recherche des Transports.

Le choix d'une conduite entièrement automatique pour le métro de Lille nous a amenés à reposer, avec une acuité particulière, le problème de la sécurité d'un transport terrestre et le fonctionnement de de celui-ci en mode dégradé.

A cette occasion, le débat a très vite porté sur les points fondamentaux de la sécurité intrinsèque, de la sécurité probabiliste, de la meilleure façon de rapprocher l'une et l'autre. Nous estimons que ces problèmes ont un caractère de généralité très grand qui dépasse le cas du métro de Lille et se posent pour tous les systèmes importants, réalisant des tâches logiques enchaînées.

C'est la raison pour laquelle, avec le Professeur Gabillard, nous avons pensé qu'il pouvait être intéressant de faire connaître l'état actuel de nos réflexions en ce domaine et la démarche que nous avons suivie.

1. INTRODUCTION

Dans le domaine des transports urbains, les réseaux de métros confient depuis longtemps à un seul agent la conduite de rames transportant plus de mille voyageurs.

Pour un observateur extérieur, il semble que la responsabilité de la sécurité d'un si grand nombre d'êtres humains repose sur un seul d'entr'eux.

Il n'entre pas dans nos intentions de vouloir retirer la moindre parcelle de mérite aux conducteurs des engins de transports, qu'ils soient placés aux commandes d'une rame de métro, d'une motrice de train à grande vitesse ou à celles d'un avion gros porteur.

Mais il est nécessaire de faire le point et de constater que le « pilote » est loin d'être seul à assurer la sécurité du système de transport.

Beaucoup d'autres hommes que le public ne voit jamais y participent, ce sont les contrôleurs des divers dispatchings et centres de commandes centralisés, les aiguilleurs des nœuds ferroviaires ou des aiguillages immatériels des voies aériennes, et tous les opérateurs qui, aux divers points vitaux de l'infrastructure du système, veillent sur sa sécurité.

Mais combien de voyageurs sont conscients de cette multitude d'autres hommes qui, au même titre que les premiers, veillent sur leur vie et sur leurs biens alors même qu'ils ne sont pas présents à l'instant considéré ? Nous voulons parler des ingénieurs et des techniciens qui, au cours de l'histoire des transports, ont peu à peu, conçu, puis amené dans son état de perfectionnement actuel le matériel de sécurité sans l'aide duquel, les « conducteurs » des engins, les agents de surveillance au sol ne parviendraient plus de nos jours à accomplir leur mission.

L'objet de cet article est de traiter de la frontière subtile qui sépare, en ce qui concerne la sécurité, les domaines d'action de deux catégories d'hommes : ceux qui font fonctionner à chaque heure de chaque journée les systèmes de transports et ceux qui, ayant conçu et réalisé le matériel de sécurité, ont, en quelque sorte, réussi à y transférer le meilleur de leur intelligence et de leur savoir faire.

Notre ambition est de persuader le lecteur que cette seconde catégorie d'hommes, lorsqu'elle prétend prendre place dans la loge de conduite d'un métro automatique, par l'intermédiaire du matériel qu'elle conçoit et des liaisons avec un poste central et y remplacer ainsi l'unique agent humain qui y subsiste encore, n'est pas déraisonnable.

2. LA SÉCURITÉ FIABILISTE PAR « REDONDANCE » DES TRANSPORTS AÉRIENS

2.1. Niveau de sécurité conventionnelle.

Pour certains modes de transport, dont le meilleur exemple est l'avion, le seul moyen d'obtenir la sécurité est de s'assurer que tous les organes vitaux de l'aéronef continueront à assurer leur fonction jusqu'à la prochaine escale.

C'est ainsi que les moteurs, les servo commandes des gouvernes, les générateurs d'énergie électrique et de pression de fluide, les dispositifs de radiocommunication et de navigation, etc... doivent continuer à fonctionner pendant un temps qui doit au moins atteindre plusieurs heures.

Le seul moyen connu d'obtenir à peu près sûrement ce résultat consiste à disposer à bord de l'appareil deux, trois ou quatre exemplaires de chacun de ces organes essentiels ; c'est la « redondance ».

Mais il est nécessaire de ne pas surcharger inutilement l'appareil et il s'est développé une discipline à la fois physique et mathématique appelée « Calcul de fiabilité » qui permet de calculer la probabilité pour qu'un organe mécanique, pneumatique, électrique et surtout électronique continue à fonctionner un temps déterminé après le décollage. Moyennant certains raffinements mathématiques, il est alors possible de calculer la probabilité d'apparition de « scénarios » complexes qui restent les seules possibilités d'accidents ; par exemple, pour un bimoteur, la probabilité pour que l'un des moteurs étant en panne un temps t après le décollage, le second moteur tombe à son tour en panne pendant le temps $(T - t)$ qui reste avant d'atteindre le plus proche aéroport.

A force d'accumuler de l'expérience et des résultats d'essais les spécialistes de la sécurité aérienne en sont arrivés à établir une correspondance entre les valeurs numériques P des probabilités ainsi calculées et le risque de voir les scénarios redoutés se produire effectivement. C'est ainsi que si, par exemple :

$P > 10^{-5}$, le scénario est « probable »,
$10^{-5} > P > 10^{-9}$, le scénario est « improbable »,
$P < 10^{-9}$, le scénario est « hautement improbable ».

On peut ainsi espérer équilibrer le compromis entre la simplicité souhaitable de l'appareillage et la nécessité des redondances pour que les scénarios résiduels d'accidents possibles, soient si hautement improbables, que *pratiquement* ils ne se produisent jamais.

Mais il faut bien se rendre compte :

— que le barème utilisé et la décision corrélative de ne pas se prémunir contre les évènements hautement improbables correspond en fait à un niveau de « *sécurité conventionnelle* » *admis par l'ensemble du public*, qui considère que les voyages en avion ne sont pas dangereux ; ce niveau de sécurité finit, avec le temps, par coïncider avec celui résultant de l'arbitrage des pouvoirs publics, qui intègre nécessairement les données provenant de l'expérience des exploitants, les études théoriques des spécialistes, et les réactions de l'opinion publique ;

— qu'il ne faut pas minimiser le rôle de l'homme qui demeure essentiel pour faire avorter les scénarios d'accidents.

2.2. Rupture des scénarios d'accidents.

La responsabilité primordiale du pilote est de se rendre compte à temps des premiers symptômes de l'apparition d'un scénario (qui peut seulement se manifester au début par un fonctionnement de certains organes légèrement en dehors de leurs régimes normaux) et de prendre les décisions aptes à empêcher ce scénario de se développer jusqu'à l'accident.

C'est le pilote qui doit commuter un équipement de secours à la place d'un organe défaillant et prendre, si nécessaire, la décision de dérouter son appareil vers un aéroport plus proche.

Mais encore faut-il que le pilote reste lui-même en état d'accomplir sa fonction. Malgré tous les contrôles médicaux, un homme peut avoir un malaise imprévu, ou même décéder subitement.

Pour garantir les passagers contre ce danger, c'est encore le principe de « redondance » que l'on utilise : l'équipage comprend toujours au moins deux hommes sachant chacun piloter.

On oppose souvent sécurité dite « fiabiliste » et sécurité dite « positive ». Notre ambition est de montrer qu'en fait elles ne s'opposent pas mais, au contraire, qu'on retrouve dans l'une et l'autre deux notions essentielles :

— celle de « niveau de sécurité conventionnelle »,

— celle de rupture, par l'intervention humaine, des scénarios pouvant conduire à un accident.

3. LA SÉCURITÉ « POSITIVE » DES TRANSPORTS FERROVIAIRES

Les véhicules des transports ferroviaires sont, par rapport aux aéronefs, dans une situation privilégiée. Ils possèdent en effet un « état de sécurité » qui est l'arrêt en un point quelconque de la voie, à condition que les dispositifs de signalisation au sol les protègent efficacement, dans cet état, d'une collision par les véhicules qui les suivent.

Contrairement aux avions qui ne tolèrent aucune panne les empêchant d'atteindre le prochain aéroport, les véhicules ferroviaires peuvent subir certaines défaillances de leurs organes (moteurs par exemple) les empêchant de poursuivre leur mission, mais qui sont sans conséquences graves, si elles conduisent à l'état de sécurité que nous venons de décrire.

Il en est de même des dispositifs de signalisation dont toute défaillance, n'ayant pour répercussion que d'arrêter le trafic, ne met pas en cause la sécurité des voyageurs.

Il s'est ainsi développée une doctrine appelée « Sécurité positive » ou « Sécurité intrinsèque » qui est à la base de la conception traditionnelle des systèmes de transports ferroviaires.

Selon cette doctrine on ne cherche pas à calculer la fiabilité des organes vitaux ni à faire en sorte qu'ils soient secourus par un organe de rechange en cas de défaillance (redondance), mais on s'intéresse essentiellement à la manière dont ils peuvent tomber en panne.

Il y a lieu de remarquer ici que les organes qui assurent la sécurité des transports ferroviaires sont pratiquement tous des organes à deux états stables : un signal est ouvert ou fermé, un frein d'urgence est serré ou desserré, une aiguille est en position droite ou déviée, etc... Généralement l'un de ces

deux états est « l'état de sécurité » : à savoir les positions fermées pour le signal ; serrées pour le frein ; droite pour l'aiguillage, etc...

Les ingénieurs qui conçoivent le système s'efforcent alors d'obtenir qu'il se positionne toujours dans son état de sécurité en cas de panne d'un organe quelconque. C'est ainsi que sur les anciens signaux formés d'un damier blanc et rouge pivotant autour d'un axe vertical, un contrepoids ramenait le signal en position fermée en cas de rupture d'une pièce de la tringlerie de commande.

Cet aspect binaire du fonctionnement des organes de sécurité s'est parfaitement adapté à l'évolution des technologies et en particulier à l'apparition des signaux électriques et plus récemment à celle des circuits électroniques.

4. LES MÉTHODES D'ÉTUDE DES DISPOSITIFS DE SÉCURITÉ CONÇUS EN SÉCURITÉ « POSITIVE »

On peut en ce monde se fier à peu de choses mais, tout de même, il existe plusieurs principes physiques qui ne seront probablement jamais violés. C'est ainsi qu'on peut croire que le sens de la gravitation terrestre ne va pas brusquement s'inverser et qu'un objet pesant ne va pas subitement s'envoler vers le ciel, on peut aussi croire que jamais on ne retirera d'un circuit électrique plus d'énergie que l'on n'y en a mis, ou que l'atmosphère terrestre ne vas pas brusquement devenir un gaz réducteur au sens chimique de ce mot, etc...

C'est sur ce genre de certitudes primaires que l'on se base pour réaliser des organes élémentaires en sécurité « positive ». C'est ainsi qu'un relais électromécanique de sécurité possèdera une masselotte dont le poids ouvrira les contacts si le courant vient à être coupé dans la bobine, ou qu'un circuit électronique élaborera sa tension de sortie à partir d'un oscillateur qui ne pourra pas osciller s'il n'est pas alimenté en énergie électrique ou encore qu'un seuil de tension dépendant de la valeur d'une résistance à film métallique ne pourra pas évoluer dans le mauvais sens, car cette résistance, au contact de l'oxygène de l'air, ne pourra qu'augmenter de valeur en s'oxydant, etc...

Ces certitudes secondaires sont déjà moins absolues que les certitudes primaires qu'elles mettent à profit.

Pour le relais, il faut être certain qu'on ne pourra jamais le monter à l'envers, que l'action du poids de sa masselotte ne sera jamais éliminé par un phénomène de grippage ou de rupture de pièce mécanique et que les contacts ne pourront jamais se coller.

Pour l'oscillateur, il faut être certain qu'un court-circuit intempestif avec un fil sous tension ne viendra pas le réalimenter, etc...

Ces évènements ne sont pas aussi « impossibles » que l'inversion du sens de la gravitation.

L'impossibilité de leur apparition va surtout dépendre de la qualité du travail des hommes chargés de faire fonctionner, et de maintenir en bon état le matériel de sécurité, fruit du travail des autres hommes qui l'ont conçu.

Or, nous allons maintenant montrer que le principe même de la sécurité « positive » rend difficile le travail des hommes qui conçoivent le matériel aussi bien que celui des hommes qui devront l'exploiter et que les intérêts de ces deux groupes d'hommes, qui devraient s'entr'aider pour obtenir la meilleure sécurité possible, sont en fait conflictuels.

Le fait que les circuits électroniques que l'on utilise de plus en plus dans la constitution des dispositifs de sécurité comportent de très nombreux composants n'est pas un obstacle pour le fiabiliste. En effet, le fiabiliste dispose de tables donnant les taux de défaillance horaire de chaque composant et de règles pour combiner ces taux de défaillances élémentaires suivant la manière dont les composants sont assemblés entr'eux.

Il peut ainsi obtenir la fiabilité du circuit global à l'aide d'un nombre d'opérations mathématiques qui n'est pas beaucoup plus élevée que le nombre des composants.

A l'issue de son calcul, le fiabiliste connaît la probabilité pour que le circuit tombe en panne un certain temps après sa mise en marche.

C'est ce qu'il appelle le MTBF (*). Mais il ignore totalement de quelle manière la panne se présentera.

(*) *MTBF : « Mean Time Between failure » en français : temps moyen entre pannes.*

Le concepteur d'un circuit en sécurité positive, lui, se soucie beaucoup plus de ne pouvoir observer que le type de panne non dangereux (correspondant à l'état de sécurité), plutôt que du temps au bout duquel cette panne risque de se produire.

Il doit donc tenir compte non seulement du taux global mais aussi de tous les types de défaillances que chaque composant peut présenter. Ceci multiplie incroyablement le nombre de cas à envisager.

Pour fixer les idées considérons un dispositif formé de n composants pouvant présenter chacun p types de pannes. La formule suivante permet de calculer le nombre N de pannes différentes pouvant se produire.

$$N = \sum_{j=1}^{n} p^j \frac{n!}{j!\,(n-j)!} \qquad (1)$$

avec $n = 30$ (*) et $p = 2$ cette formule donne :

$$N = 2.10^{14}$$

Il est bien évident qu'il est impossible d'examiner tous les cas. Même en disposant d'un ordinateur capable d'analyser chaque cas de panne en une milliseconde, il faudrait 6.340 années !

Les spécialistes de la conception des dispositifs en sécurité intrinsèque sont donc bien obligés de limiter leur étude à l'essentiel.

Ils commencent par essayer de diminuer le nombre p de type de pannes de certains composants en prenant des précautions technologiques.

C'est ainsi qu'on peut considérer comme impossible :

– le court-circuit entre deux fils, isolés et suffisamment espacés tout au long de leurs trajets ;

– le fait que certains modèles de résistances puissent diminuer de valeur ;

– le fait qu'un condensateur, faisant partie d'un filtre puisse se débrancher.

Pour cela, on construit des condensateurs spéciaux possédant quatre fils de sortie. Ces fils servent ainsi non seulement à brancher le condensateur, mais aussi à relier une cellule du filtre à la suivante. Si l'un des fils se coupe, ce qui débranche le condensateur, le filtre se trouve aussi entièrement débranché et

(*) *30 est un ordre de grandeur raisonnable pour le nombre de composants d'un appareil électronique de complexité moyenne.*

cette panne n'est pas dangereuse car elle est aussitôt détectée, etc...

Ensuite, une première analyse consiste à étudier l'une après l'autre les conséquences des pannes possibles de chacun des n composants. Cela ne fait que $n.p.$ cas à analyser.

Il faut que chacune de ces pannes place la sortie du circuit dans son état de sécurité, qui est généralement l'absence de tension. Si l'une des pannes produit l'effet inverse, *il faut modifier le circuit* jusqu'à ce que sa conséquence devienne l'absence de tension.

Mais le cas le plus pernicieux se rencontre si l'une des pannes simples ainsi étudiée ne *produit aucun effet sur le fonctionnement du circuit.*

Une panne n'est pas dangereuse si son effet immédiat est de mettre un signal au « rouge permanent ». En effet, ce type de panne se signale d'elle-même au personnel d'exploitation et d'entretien qui pourra l'éliminer (nous verrons toutefois un peu plus loin qu'il faut nuancer cette affirmation).

Mais si une panne ne se manifeste par aucun effet immédiat, elle constitue une épée de Damoclès, car elle peut très bien être le premier acte d'un scénario dont le second acte sera l'apparition d'une autre panne dont le résultat combiné avec la première pourrait être la *« mise au vert » d'un signal qui devrait être rouge.*

C'est-à-dire ce que nous appellerons : *une panne sécurité.*

Quand une panne de composant non détectée est trouvée au cours de l'étude d'un circuit de sécurité, les spécialistes qui effectuent l'étude doivent tout recommencer !

Il leur faut, en présence de la panne non détectée, étudier à nouveau systématiquement les conséquences de chacun des ($n.p. - 1$) cas d'autres pannes simples pouvant se produire. Et au cours de cette étude, des cas de « pannes doubles sans effet immédiat » peuvent être découverts, ce qui nécessiterait d'étudier les pannes triples, et ainsi de suite...

Ce travail n'a pas de fin ou, plus exactement, il pourrait durer jusqu'à ce que les $N = 2.10^{14}$ cas de pannes multiples possibles aient été étudiés !

Mais il faut bien, après une certaine durée d'étude, livrer les dispositifs de sécurité au personnel d'exploitation. L'ingénieur responsable de ces études ne le fera que lorsqu'il aura atteint *l'intime conviction* que les seules causes d'insécurité qui subsistent sont des scénarios si tortueux et de probabilité si faible que, *pratiquement*, ils ne peuvent pas se produire.

Bien que cette conviction intime soit le résultat d'une investigation du système par des méthodes éprouvées, appliquées selon des règles de l'art qui donnent l'assurance que tout ce qui était *possible* de faire pour déceler les risques d'accidents a été fait, elle demeure cependant entachée d'une part d'incertitude, car la *démonstration rigoureuse de la sécurité* n'a pu être faite au sens mathématique du terme.

Le concepteur du système en est bien averti et il ne prend jamais pour une certitude sa conviction intime dont il sait qu'elle possède *une part non négligeable de subjectivité.* Mais, par ce moyen, il propose au public un niveau de *sécurité conventionnelle*, essentiellement subjectif lorsqu'il est appréhendé par le voyageur, mais *acceptable* par celui-ci pour le système de transport considéré.

Mais l'ingénieur, qui sait que son étude n'a pas pu être exhaustive, ignore en quoi consistent ces scénarios résiduels, et il ne connaît pas leur probabilité puisqu'il n'a pas pu les étudier. Il devrait donc être hanté par l'idée du scénario oublié à probabilité non négligeable que ni lui, ni aucun de ses collaborateurs, n'a réussi à imaginer et qui pourrait un jour créer un accident dont il serait tenu pour responsable, et cette crainte devrait l'inciter à continuellement douter de ses certitudes et à remettre constamment à l'étude les circuits qu'il a qualifiés de sûrs.

En d'autres termes, le groupe d'hommes qui conçoivent les dispositifs de sécurité suivant le principe de la sécurité « positive », qu'il se l'avoue ou non, a la crainte « d'être joué par le diable » et c'est probablement cette crainte salutaire qui est à l'origine de la sécurité extraordinairement élevée que connaissent actuellement les systèmes de transports ferroviaires.

Mais cette crainte salutaire peut aussi conduire à des efforts considérables pouvant n'être qu'insuffisamment justifiés par les risques encourus, au blocage de l'évolution de la technologie et à un renchérissement très important des coûts du matériel.

5. LE CONFLIT ENTRE LA SÉCURITÉ POSITIVE ET LA DISPONIBILITÉ

Entre les hommes qui conçoivent les dispositifs en sécurité positive et ceux qui sont chargés de les faire fonctionner, il existe une divergence fondamentale d'intérêt.

Les concepteurs des dispositifs de sécurité souhaitent obtenir une absence quasi-totale d'accidents, et nous avons vu que pour y parvenir, ils s'efforcent d'obtenir que toute panne de leurs dispositifs ait pour effet d'arrêter les trains.

Les hommes chargés de l'exploitation souhaitent aussi n'avoir aucun accident, mais la mission dont ils sont chargés est de faire marcher les trains.

Il existe là une incompatibilité qui est susceptible d'être une source d'accidents.

En effet, lorsqu'un appareil de sécurité tombe en panne tout en remplissant son rôle, le trafic est interrompu. Mais l'appareil n'est pas toujours réparable immédiatement et il n'est pas raisonnable d'attendre qu'il soit réparé pour faire repartir le trafic, car il ne s'agit en fait que d'une fausse alarme.

Les hommes de l'exploitation sont ainsi parfois obligés de donner aux conducteurs l'ordre de franchir un signal en panne qui, si les hommes des dispositifs de sécurité ont bien fait leur travail, sera un signal au rouge.

Dans un tel cas, les conducteurs reçoivent un ordre écrit et leur attention est mise en alerte. Mais l'homme est un être incroyablement complexe, dont les réactions sont bien plus difficiles à prévoir que celles d'un automatisme.

L'homme possède surtout la propriété unique d'être intelligent. A cause de son intelligence, il peut interpréter des faits se produisant dans son environnement et réagir d'une manière personnelle à des événements imprévus.

Dans certains cas, cette réaction intelligente peut éviter un accident, mais dans d'autres cas, l'homme peut se laisser abuser par une apparence trompeuse et créer lui-même un accident qu'un automatisme, appliquant stupidement une consigne, n'aurait pas produit.

6. L'EFFET TANTOT NÉFASTE OU PARFOIS PRÉCIEUX DE L'INTELLIGENCE DE L'HOMME

Nous allons imaginer deux exemples montrant, l'un une action néfaste, l'autre une action bénéfique de l'intervention de l'homme :

– Sur une ligne de métro, un signal est en panne et les conducteurs reçoivent l'ordre de le dépasser en marche à vue. Malheureusement, ce signal est à l'entrée d'une courbe et la marche à vue nécessite un ralentissement considérable. L'un des conducteurs aperçoit dans une ligne droite les fanaux arrière de la rame qui le précède. Ce fait imprévu, qui lui permet d'apprécier la distance qui le sépare de cette rame, lance son cerveau dans un processus de réflexion intelligente dont le résultat est que, compte-tenu d'un surstationnement de 10 secondes qui se produit à la prochaine station, la rame aval doit avoir pris une telle avance que le franchissement du signal en panne peut sans danger se faire à vitesse normale. Le raisonnement était inattaquable, mais ce que n'imagine pas le conducteur est que, juste après la courbe, un voyageur de la rame aval, pour une raison quelconque, va tirer le signal d'alarme, et provoquer l'arrêt de la rame. La collision qui se produit est due au fait, qu'autorisé une première fois à transgresser une consigne (le franchissement du signal rouge en panne), le conducteur a cru pouvoir de sa propre autorité en transgresser une autre (le ralentissement) à la suite d'un raisonnement que son *intelligence* lui présentait comme irréprochable mais qui ne tenait pas compte d'un fait dont il n'avait pas connaissance.

Si ce conducteur *avait disposé de davantage de temps pour réfléchir*, peut-être aurait-il pensé à l'éventualité du signal d'alarme.

Notre second exemple met en scène un cas de « panne sécurité ». C'est-à-dire une possibilité d'accident non envisagée par les hommes ayant conçu le dispositif de sécurité.

– Par temps de gel sur une ligne aérienne, une rame de métro est obligée, à une station, de recourir au sablage pour pouvoir démarrer.

Des grains de sable s'incrustent dans les bandages à tel point que les roues d'un côté de la rame sont entourées d'un bandeau isolant et que leur contact électrique avec le rail n'est plus assuré. Ce phénomène avait été considéré comme impossible par les concepteurs de la signalisation, compte tenu du poids d'un wagon, et c'est la panne sécurité : les signaux restent au vert, ne protégeant plus la rame.

Toutefois, on est à l'heure de pointe, à intervalle très faible, et le conducteur de la rame suivante *a l'habitude* de découvrir les signaux au rouge et de ne les voir passer au vert que lorsqu'il s'en rapproche.

Le fait de voir constamment tous les signaux au vert déclenche chez le conducteur un processus de réflexion intelligente. Cette voie, systématiquement libre, ne lui paraît pas normale et sans s'expliquer l'origine de l'anomalie, il décide de freiner sa rame, alors que rien ne lui ordonne.

Sans la présence de l'homme, la collision était inévitable.

Ces deux exemples sont, bien sûr, inventés, mais certains exploitants leur trouveraient peut-être une ressemblance avec des événements leur étant réellement arrivés. Ils ont seulement pour objet de montrer :

– d'une part, que la présence de l'homme dans une cabine de conduite *n'augmente pas nécessairement la sécurité ;*

– d'autre part, *qu'un système automatique a quelquefois besoin de la réflexion intelligente d'un homme.*

7. LA REDONDANCE DE « DISPONIBILITÉ »

Le conflit que nous venons de montrer entre les hommes de l'exploitation et les concepteurs des dispositifs de sécurité, est propre au principe de la « sécurité positive ». Il ne se produit pas du tout dans le domaine des transports aériens ou l'objectif des constructeurs des appareils est identique à celui des exploitants : faire parvenir à tout prix le véhicule jusqu'à sa prochaine escale.

Nous avons vu au § 2 que la technique mise en œuvre dans ce cas était la redondance.

On est donc tenté, pour résoudre le conflit entre les impératifs de l'exploitation et ceux de la sécurité, d'installer en double exemplaire tous les dispositifs en sécurité intrinsèque des systèmes ferroviaires. Ceci pour permettre, par simple commutation d'un dispositif en veille à la place d'un dispositif en panne la reprise rapide du trafic arrêté par la fausse alarme consécutive à une panne.

Cette redondance de disponibilité est très certainement la solution qui doit permettre d'exploiter en sécurité des systèmes de transport du type métro sans personnel de conduite à bord des rames.

Mais nous allons montrer qu'elle ne doit pas être mise en œuvre sans précautions spéciales. Il importe en effet d'éviter plusieurs écueils qui sont :

1. L'abandon du concept de « sécurité positive » au profit d'une sécurité de type probabiliste, car alors on prive le transport terrestre de la supériorité décisive que l'existence de son « état de sécurité » lui confère par rapport au transport aérien (voir § 3).

2. La non mise à profit de la redondance de disponibilité pour tenter d'éliminer aussi le seul risque inhérent au principe de sécurité positive qui est la possibilité d'existence de scénarios non découverts de pannes sécurité.

L'existence de ces scénarios résultent comme nous l'avons montré au § 4 du fait que l'étude des circuits de base des dispositifs en sécurité intrinsèque ne peut que très rarement être exhaustive.

3. Le recours intempestif à l'initiative humaine qui est comme nous en avons donné un exemple au § 6, parfois aussi dommageable que de se priver de la réflexion intelligente de l'homme.

Nous allons développer successivement ces trois points au § 11.

8. LA MÉTHODE DES OBJECTIFS DE SÉCURITÉ

Cette méthode s'est développée principalement sous l'égide de la Direction des Transports Terrestres du Ministère des Transports (réf. propositions pour une nouvelle réglementation de systèmes de transport collectif terrestre de voyageurs – Conseil Supérieur des Transports – Mars 1976).

Son idée principale repose sur la constatation que, même sur des systèmes de transports bénéficiant d'une très

grande réputation de sécurité, comme par exemple le réseau ferré urbain de la RATP, il se produit quand même, bien que très rarement, certains accidents.

Il est donc plus réaliste d'abandonner l'exigence de sécurité absolue des anciennes législations et d'exiger en ce qui concerne un système de transport nouveau, qu'il soit « au moins aussi sûr » que le métro de Paris qui peut légitimement servir de « mode de référence », étant donné l'excellente image de marque qu'il a dans le public sur le plan de la sécurité (application du principe de sécurité conventionnelle).

Cette méthode possède l'énorme avantage d'introduire des données quantitatives là où auparavant régnait le qualitatif, pour ne pas dire le subjectif.

C'est ainsi que l'exploitation des statistiques d'accidents observés pendant 15 années consécutives sur le métro de Paris permet d'établir que le nombre de voyageurs victimes d'accidents sur ce réseau de transport ne dépasse pas 2.800 pour 10^9 personnes transportées (ce qui correspond à peu près à une année d'exploitation). Ce nombre comprend en fait toutes les déclarations d'accidents mais on ne relève (en excluant les suicides) que 24 blessés graves ou tués imputables au système de transport pour la même période.

Des raisonnements assez simples, mais trop long à reproduire ici permettent (réf. : Objectif de sécurité pour le métro de Lille – R. Gabillard – Novembre 1977) d'établir qu'un système de transport nouveau à capacités unitaire et totale plus faibles que le mode de référence, jouira du même degré de sécurité que le métro de Paris si on n'y relève pas plus de, par exemple, 300 *victimes d'accidents* dus à des défaillances techniques pour 10^9 voyageurs transportés.

Il reste à savoir comment utiliser ce chiffre. Il est bien évident qu'il serait tout à fait choquant et inadmissible de le considérer comme un « objectif à atteindre ». Aucun des auteurs qui ont publié sur ce sujet ne l'ont d'ailleurs envisagé de la sorte. Ils l'ont plutôt présenté comme une « tolérance à ne pas dépasser », ou mieux, et c'est notre cas, comme une référence pour le dimensionnement et la conception du système de transport.

Même présenté de cette manière, la méthode des objectifs de sécurité se heurte au principe de déontologie qui veut que chaque responsable de la conception et de l'exploitation d'un système de transport doit faire tout son possible pour éviter les accidents.

Ayant nous-mêmes participé à l'invention, puis au développement au cours de plusieurs commissions d'études, de la méthode des objectifs de sécurité, nous avons continué à réfléchir à son utilisation, et nous sommes parvenu à la conclusion qu'il *fallait la considérer comme un outil de calcul permettant de répartir d'une manière optimum les efforts à accomplir pour tenter d'éliminer le plus complètement possible les accidents.*

9. APPLICATION DE LA MÉTHODE DES OBJECTIFS DE SÉCURITÉ A UNE ÉVALUATION DE LA VRAISEMBLANCE DE L'« AFFIRMATION » DE SÉCURITÉ RÉSULTANT DE LA CONCEPTION EN SÉCURITÉ POSITIVE

La seule méthode d'étude de la sécurité applicable aux transports terrestres qui ait l'ambition d'éliminer le plus complètement possible les accidents est la conception en sécurité « positive ».

C'est donc cette méthode de conception, qui doit être exigée des constructeurs de modes de transports nouveaux.

Mais il y a lieu de signaler ici sa contradiction intrinsèque.

Un dispositif en sécurité positive n'est mis en service que si tous ceux qui ont participé à son étude sont convaincus qu'il ne subsiste plus aucune cause « connue » d'insécurité.

Ceci revient à affirmer que la probabilité horaire d'apparition λ de « pannes sécurité » est strictement nul.

$$\lambda = 0$$

Mais cette affirmation est contredite à chaque fois qu'il se produit, très rarement heureusement, un accident. Cet accident est dû à l'un des scénarios résiduels dont nous avons parlé au § 4. Il était impossible de calculer sa probabilité puisqu'il était inconnu. Mais, dès qu'un accident l'a mis en évidence il devient possible d'y remédier et le système devient effectivement plus sûr.

Les spécialistes qui ont conçu le système sont donc amenés à affirmer de plus en plus fort, après chaque accident, la sécurité du système.

C'est cette affirmation de sécurité, se traduisant par la valeur nulle de λ qui fait à la fois la force et la faiblesse de la méthode de conception en sécurité positive :

– *Sa force* car elle ne peut qu'augmenter de vraisemblance avec le temps.

– *Sa faiblesse* car la valeur nulle de λ peut laisser croire aux ingénieurs qui développent le système complet à partir de circuits élémentaires dont on croit qu'ils sont vraiment de sécurité intrinsèque qu'ils peuvent assembler ces blocs élémentaires « infaillibles » n'importe comment.

En effet, si λ_1 et λ_2 sont les probabilités horaires de pannes sécurité de 2 blocs élémentaires et si l'on affirme que $\lambda_1 = 0$ et $\lambda_2 = 0$

Alors :

$$\lambda_1 + \lambda_2 = \lambda_1 . \lambda_2 \qquad (2)$$

et une association en OU de ces deux blocs est tout aussi sûre que leur association en ET. Ce qui n'est pas vrai si λ_1 et λ_2 ont des valeurs très petites mais non nulles.

La méthode que nous préconisons d'employer consiste à admettre que tous les scénarios résiduels non encore découverts qui peuvent se manifester un jour par un accident (si invraisemblable que l'on pourra peut-être croire à une « intervention du Diable ») ont une probabilité horaire ε non nulle.

Bien entendu, il est impossible de calculer cet ε par les méthodes classiques, car il est la probabilité de phénomènes dont nous ignorons à la fois l'origine et la manière dont ils se développent.

Mais si nous attribuons la même valeur de ε à chacun des blocs élémentaires (ce qui revient à traiter le Diable au forfait), nous pourrons exprimer en fonction de cet ε la probabilité globale d'accident du système complet :

$$P = P(\varepsilon)$$

En utilisant alors les procédés de calcul mis au point par les inventeurs de la méthode des objectifs de sécurité (réf. Propositions pour une nouvelle règle-

mentation de système de transport collectif terrestre de voyageurs = Conseil Supérieur des Transports : mars 1976), on peut traduire cette probabilité P, en nombre de voyageurs blessés pour 10^9 voyageurs transportés : N = N (P) = N (ε).

Si nous prenons, par exemple, 300 pour objectif de sécurité l'égalité :

$$N(\varepsilon) = 300 \qquad (3)$$

fournira une valeur de ε qui sera la mesure de la part d'activité maximum que l'on peut tolérer au Diable si l'on ne veut pas dépasser l'objectif fixé qui revient, rappelons le « à ce que le mode de transport étudié soit au moins aussi sûr que le mode de référence choisi ».

10. UTILITÉ DE CETTE ANALYSE

Le but de notre analyse est de déterminer la valeur que devrait atteindre ε pour que l'objectif de sécurité soit juste respecté. Plus la valeur de ε déterminée par la relation (3) sera grande, plus il sera facile de respecter l'objectif de sécurité pris comme référence, comme niveau de sécurité conventionnelle admissible.

Cette affirmation peut sembler paradoxale mais elle ne fait que traduire la sensibilité du système complet à des défaillances imprévisibles de ses constituants élémentaires.

Plus il sera nécessaire que la probabilité horaire de « défaillances (*) imprévisibles » des circuits élémentaires soit élevée pour produire des accidents conduisant à un nombre de victimes donné et plus le système sera sûr.

L'objectif de sécurité peut alors cesser d'avoir la signification d'un nombre de victimes que l'on s'accorde, pour prendre celle d'une hypothèse de travail, que l'on peut choisir à volonté aussi petite que l'on veut, et qui permet de calculer dans le cadre de cette hypothèse les valeurs de ε correspondant à divers types d'architecture du système de sécurité complet.

On peut alors en choisissant celle des structures conçues à partir des mêmes éléments en sécurité positive, qui conduit à la valeur la plus élevée de ε, déterminer par cela même le dispositif de sécurité qui sera le moins sensible à une « panne sécurité » de ses circuits élémentaires.

11. EXEMPLE D'APPLICATION

Nous avons au § 7 envisagé la redondance comme un moyen possible d'accroître la sécurité du système tout en solutionnant l'antagonisme entre les impératifs de l'exploitation et de la sécurité. Mais nous avions signalé plusieurs précautions à prendre. Nous sommes maintenant en mesure de les expliciter.

1) *Ne pas abandonner le principe de « sécurité positive » au profit d'une sécurité de type probabiliste.*

Considérons un organe essentiel, électronique par exemple, qui ne peut pas tomber en panne sans créer un accident.

Nous désignerons par un Lambda majuscule la probabilité de défaillance horaire Λ de cet organe, afin de ne risquer aucune confusion avec le Lambda minuscule déjà utilisé pour représenter le taux horaire λ de « pannes sécurité » d'un appareil conçu en sécurité positive.

T étant la durée du vol, la probabilité P d'avoir un accident au cours du vol sera si on ne dispose que d'un seul appareil :

$$P = 1 - e^{-\Lambda T}$$

Si T = 10 heures et $\Lambda = 10^{-5}$/h on aura :

$$P \# 10^{-4}$$

Si on se réfère au tableau d'interprétation des probabilités, connées au § 2, l'accident sera « probable ».

Mais si on dispose de deux appareils la probabilité pour qu'ils tombent tous les deux en panne avant la fin du vol sera donnée par la formule :

$$P = (1 - e^{-\Lambda_1 T})(1 - e^{-\Lambda_2 T})$$

Λ_1 et Λ_2 étant respectivement les probabilités de défaillance horaire des deux appareils.

Si on a :

$$\Lambda_1 T \ll 1 \text{ et } \Lambda_2 T \ll 1$$

P devient :

$$P = \Lambda_1 \Lambda_2 T^2$$

Si $\Lambda_1 = \Lambda_2 = 10^{-5}$/h et T = 10 h, on aura maintenant :

$$P = 10^{-8}$$

Le tableau du § 2 qualifiera alors l'accident d'« improbable » (notion de sécurité conventionnelle).

Mais d'une part, l'accident ne peut pas être considéré comme « impossible » et d'autre part, on suppose que la fiabilité du pilote chargé de mettre en service l'équipement de rechange à la place de l'équipement en panne doit être absolue (principe de rupture du scénario d'accident).

Supposons maintenant qu'un équipement électronique de complexité similaire soit utilisé pour assurer, par exemple, la sécurité anticollision d'un transport ferroviaire. L'existence de l'état de sécurité de ce type de transport permet de concevoir l'équipement en sécurité intrinsèque. La conséquence en est que, tant qu'il ne se produira pas d'accident prouvant le contraire, tout le monde sera persuadé que la probabilité de panne sécurité de l'équipement est nulle.

$$\lambda = 0$$

Dans ce cas un seul appareil suffit à assurer une sécurité d'apparence absolue, bien que sa probabilité horaire de panne Λ demeure du même ordre de grandeur que celle de l'appareil mentionné précédemment, par exemple :

$$\Lambda = 10^{-5}/\text{h}.$$

Le MTBF, c'est-à-dire le temps au bout duquel il est presque certain que l'appareil tombera en panne en produisant une fausse alarme est l'inverse de Λ c'est-à-dire 10^5 heures.

Ceci peut sembler satisfaisant mais si l'appareil est, par exemple, un équipement de protection de canton, on peut en avoir une centaine répartie le long de la voie. C'est alors toutes les 1.000 heures seulement, c'est-à-dire environ tous les 40 jours que le trafic de la ligne sera bloqué par la panne de l'un des équipements pendant le temps nécessaire à sa réparation. Ce temps s'appelle le MTTR (*) et par définition la « Disponibilité » D du système de protection de

(*) *Rappelons qu'il s'agit ici de la probabilité ε des défaillances ayant échappées à l'étude.*

(*) *« Mean Time to Repair » en français « Temps moyen de la réparation ».*

cantons assurant l'anticollision est donnée par la formule :

$$D = \frac{MTBF}{MTBF + MTTR} \qquad (4)$$

La mise en « sécurité positive » d'un équipement par les précautions qu'elle exige de prendre et les complications des circuits que cela entraîne, s'accompagne assez souvent d'un mauvais MTBF. Mais la formule (4) montre que c'est sans importance si le MTTR est très court.

La redondance de disponibilité n'a pour objectif que d'augmenter la disponibilité en réduisant le MTTR et nullement d'augmenter la sécurité puisque celle-ci apparaît déjà comme parfaite avec un seul équipement.

Il serait ridicule de ne pas profiter à chaque fois que cela est possible (c'est-à-dire quand il existe un état de sécurité) de l'apparence de sécurité absolue que procure la conception en sécurité positive. Car, si rien ne permet d'affirmer que la sécurité soit vraiment absolue, il n'est pas exclu non plus que pour certains dispositifs étudiés depuis longtemps, cet idéal de sécurité totale ne soit pas pratiquement atteint.

2) La seconde recommandation que nous avions faite au § 7 était : « *La mise à profit de la redondance de disponibilité pour tenter d'éliminer les « pannes sécurité » non découvertes* » (principe de rupture des scénarios d'accident).

Pour vraiment profiter de la redondance de disponibilité, il ne faut perdre aucun instant pour commuter un équipement en veille à la place d'un équipement en panne. Or, on pourrait être tenté de réaliser automatiquement cette commutation en associant les sorties des 2 équipements par un simple circuit logique « OU ».

En effet, la sécurité « positive » impose que l'interdiction de pénétrer sur un canton (signal rouge) soit transmise aux rames par l'absence de tension (niveau logique zéro) à la sortie de l'appareil.

L'appareil est donc conçu pour que toute panne pouvant se produire ait pour conséquence l'absence de tension. Par suite, si un appareil est associé par un circuit « OU » avec un autre appareil qui n'est pas en panne, c'est la tension de sortie de ce second appareil, qui, en cas de fausse alarme du premier (c'est-à-dire s'il n'y a pas lieu d'interdire la pénétration du canton) autorisera la poursuite du trafic.

Il sera seulement nécessaire de signaler à un poste de contrôle centralisé, la fausse alarme du premier appareil à l'aide d'un détecteur de discordance des tensions logiques de sortie des deux appareils. Mais les hommes du service d'entretien disposeront pour effectuer la réparation de l'appareil en panne d'un temps de l'ordre de grandeur d'une fraction raisonnable du MTBF de l'appareil qui a pris la relève. Et il n'y a aucune interruption de trafic.

Malheureusement, si l'éventualité que nous avons envisagée au § 9 se produit, c'est-à-dire si, à l'insu de tout le monde, la probabilité horaire λ de panne sécurité des circuits n'est pas strictement nulle, l'association en « OU » peut faire le jeu du Diable.

Nous avons : $\lambda = \varepsilon$.

Mais ε n'est pas calculable à partir de ce que l'on sait sur les circuits eux-mêmes.

Pour calculer un ordre de grandeur de ε il faut se donner un objectif de sécurité qui peut très bien être parfaitement arbitraire.

Par exemple on désire que le nombre de victimes d'accidents collectifs imputables au système de transport ne dépasse pas 13 pour 10^9 voyageurs transportés.

En l'occurence cet objectif n'est pas totalement arbitraire, il correspond à la condition pour le système de transport considéré d'être aussi sûr que le métro de Paris.

Il est possible, à l'aide de calculs exposé (réf. : Objectifs de sécurité pour le métro de Lille – R. Gabillard – Novembre 1977), de transformer cet objectif en probabilité horaire Po de collision pour une rame.

On trouve :

$$Po = 1{,}6.10^{-8}$$

En estimant que chaque appareil de sécurité de canton met en œuvre 5 circuits élémentaires en sécurité positive susceptible d'avoir chacun une probabilité horaire ε de panne sécurité, nous voyons que l'association en « OU » de deux appareils de sécurité de canton conduit pour chaque canton à une probabilité horaire de panne sécurité :

$$P_c = 10\,\varepsilon$$

Si, il existe N cantons sur la ligne, le risque horaire global d'apparition d'une panne sécurité est :

$$NP_c = 10\,\varepsilon\,N$$

Et si il y a n rames en circulation sur la ligne nous aurons, en faisant l'approximation très grossière qu'elles se répartissent équitablement le risque, une probabilité horaire de collision par rame (due aux installations fixes de protection de canton) :

$$Po = 10\,\varepsilon\,\frac{N}{n}$$

En égalant cette valeur à l'objectif de sécurité $Po = 1{,}6.10^{-8}$ et avec $N = 100$ et $n = 40$ nous obtenons :

$$\varepsilon \# 6.10^{-10}/h$$

Remarque.

D'autres calculs basés sur d'autres hypothèses moins grossières conduisent à des valeurs de ε comprises entre $1{,}5.10^{-10}$ et $1{,}6.10^{-9}$

Pour croire que l'objectif de sécurité que nous nous sommes fixé ne sera pas manqué, il faut donc croire qu'il n'existe dans les circuits élémentaires en sécurité positive aucun scénario de défaillances multiples non découvert conduisant à une probabilité horaire de panne sécurité comprise entre 10^{-9} et 10^{-10}. Compte tenu de la petitesse de ces chiffres, il est très difficile d'avoir cette certitude et la conclusion est que l'association en « OU » de la redondance de disponibilité a de sérieuses chances d'être dangereuse.

Pour pouvoir profiter de la redondance de disponibilité pour résoudre à la fois le problème de la disponibilité et éliminer le risque que nous venons de révéler il faut utiliser une association en « ET » et faire en même temps appel à la réflexion intelligente d'un homme.

Ceci nous conduit à la nécessité d'éviter le troisième écueil que nous avions signalé au § 7 : « Le recours intempestif à l'initiative humaine ».

L'association en ET (au même titre que la commutation automatique par association en OU) implique que les deux équipements soient simultanément en marche et reçoivent les mêmes informations en provenance des capteurs disposés le long de la voie. Simplement, l'équipement en veille n'est pas connecté à la commande des « signaux ». Les appareils électroniques n'étant pas soumis au phénomène d'usure le MTBF de l'équipement de secours est à peu près le même qu'il soit arrêté ou en veille active comme nous l'envisageons.

L'association en « OU » a pour effet de faire automatiquement commander les « signaux » en cas de discordance des deux équipements par celui qui fournit l'indication la plus permissive. Tandis que l'association en « ET » obéit aux indications de l'équipement le moins permissif.

L'association en « ET » empêche ainsi une panne sécurité ayant pris naissance dans l'un des équipements, de parvenir jusqu'à la commande des signaux.

En fait, le scénario conduisant à l'accident est devenu beaucoup plus tortueux, et il devient *possible à un opérateur humain de le rompre.*

Au lieu qu'une collision puisse se produire à la suite d'une panne sécurité apparaissant à n'importe quel moment dans l'un quelconque des dix circuits élémentaires en sécurité intrinsèque qui composent l'appareil actif et l'appareil de secours, il est nécessaire que se produisent les événements suivants :

— apparition à un instant quelconque d'une panne sécurité dans l'un des cinq circuits élémentaires de l'équipement actif,

— apparition, avant qu'il se soit écoulé un temps supérieur à l'intervalle entre deux passages de rames, d'une autre panne sécurité dans les circuits de l'équipement en veille.

En effet, si l'équipement en veille est encore en bon état au premier passage de rame suivant la panne sécurité de l'équipement actif, celle-ci sera détectée par la discordance entre les deux équipements et l'opérateur humain pourra intervenir.

Un autre scénario possible est la mise hors service du détecteur de discordance ou du « ET » d'association suivi d'une panne sécurité dans l'un des équipements.

Le calcul détaillé est assez complexe mais son résultat est plutôt rassurant puisque la valeur de ε est augmentée d'un facteur 100.

En effet, si l'on se fixe le même objectif de sécurité que précédemment (13 victimes pour 10^9 voyageurs transportés) on trouve que pour dépasser cet objectif il faudrait que la probabilité horaire ε de panne sécurité des circuits en « sécurité positive » dépasse la valeur :

$$\varepsilon = 10^{-7}$$

Il devient alors possible de croire que l'étude des circuits en « sécurité positive » n'a pas laissé échapper une possibilité de panne sécurité de probabilité relativement aussi élevée.

Mais l'association en « ET » nécessite l'intervention humaine. En effet, une fausse alarme dans l'un *ou* l'autre des deux équipements arrête tout le trafic. C'est le prix qu'il faut payer pour qu'une « panne sécurité » de l'un des deux équipements ait aussi le même effet.

Il est bien préférable que l'homme alerté par l'indication de discordance soit situé dans un poste de contrôle centralisé plutôt que dans la loge de conduite de l'une des rames.

En effet, il dispose dans ce poste centralisé de toutes les informations nécessaires pour élaborer son action. Et il dispose aussi de tout le temps nécessaire pour faire fonctionner son intelligence, puisque l'association en « ET » de la redondance de disponibilité a arrêté tout le trafic en attendant sa décision.

C'est donc en définitive l'homme qui va décider lui-même avec toutes les ressources de son cerveau et toutes les aides à la décision dont il dispose dans son poste de commandement centralisé, de l'opportunité de faire repartir le trafic en inhibant par télécommande l'association en « ET » et en mettant en service par le même procédé celui des deux équipements qui lui semble en bon état.

Par rapport à une commutation automatique en « OU », ou à une commutation manuelle non réfléchie et qui risque ainsi d'être intempestive, le recours à la réflexion de l'homme après arrêt automatique du trafic augmentera certainement le MTTR de quelques dizaines de secondes.

Mais il nous semble que ce n'est pas payer trop cher le gain de sécurité qu'apporte la *mise en série, à titre consultatif, de l'intelligence humaine, dans la boucle de réaction de l'automatisme électronique.*

12. EXTENSION POSSIBLE A D'AUTRES SYSTÈMES

Nous le disions en introduction, ces notions de sécurité dégagées à l'occasion de l'analyse d'un cas précis, ont, nous semble-t-il, une portée extrêmement générale et nous avons montré sur un exemple, l'application de ces principes.

La première notion que nous avons dégagée est celle de *niveau de sécurité conventionnelle admissible* qui définit les risques inhérents à une activité humaine que notre société accepte tacitement ou explicitement. Comment évolue ce niveau de sécurité conventionnelle ? En fonction de quels éléments d'appréciation ?

Sans vouloir apporter une réponse complète à ces interrogations, il nous semble que ce niveau admissible dépend essentiellement :

— de la structure mise en place pour organiser le service apporté à l'usager,

— des conséquences de l'accident élémentaire.

Nous reviendrons plus loin sur ces points, en donnant notamment des exemples où ce niveau de sécurité conventionnelle admissible n'est pas défini objectivement.

A contrario, c'est ce qui explique, à nos yeux, l'acceptation tacite par notre société du niveau de sécurité extrêmement bas dans la conduite des véhicules individuels : absence d'organisation du service, laissée à l'initiative de chacun ; faiblesse relative des conséquences d'accidents correspondant. (A part quelques accidents exemplaires et dramatiques, mais dont le caractère de fatalité ou d'enchaînement extraordinaire est souvent mis en valeur.)

Après avoir montré que l'on ne pouvait échapper à utiliser un niveau de sécurité conventionnelle, de manière objective ou subjective, dans une analyse de sécurité de quelque type que ce soit, nous avons ensuite explicité, lorsque cela est possible, l'intérêt d'une formalisation objective de ce niveau de sécurité qui doit conduire à une optimisation des études de sécurité et *de leurs résultats.*

Ensuite, nous avons montré l'intérêt de la deuxième notion relative à la *rupture des scénarios d'accident.* Qu'il s'agisse d'enchaînements de pannes extrêmement peu probables (scénarios attribués à la « fatalité », ou de scénarios plus probables parce que résultant de défauts systématiques, nous avons alors montré, sur des exemples, le rôle essentiel de l'opérateur humain.

La généralisation pour d'autres systèmes complexes de ces méthodes d'étude peut être faite, avec cependant des particularités, ou des difficultés sur lesquelles nous voudrions insister.

En général, on pourra trouver par référence à ce qui existe, un niveau de sécurité conventionnelle admis pour la catégorie de systèmes construits (pour ce qui concerne les transports en commun urbains en site propre : le métro de Paris). Cependant, cela ne sera pas toujours possible, notamment lorsque les conséquences d'un accident élémentaire paraissent sans commune mesure avec ce qui existe par ailleurs. Les risques encourus par la réalisation des supertankers peuvent être donnés comme premier exemple. Compte tenu des conséquences dramatiques du naufrage d'un pétrolier de 250 000 à 500 000 tonnes, ce risque n'a aucune commune mesure avec celui encouru par le naufrage d'un pétrolier de 10 000 tonnes. Il n'est pas envisageable de transposer avec un facteur linéaire le niveau de sécurité admissible de l'une à l'autre catégorie de bateau.

La réalisation des centrales nucléaires est un autre exemple. Il n'y a là non plus aucune référence avec ce qui existe, et le risque de *référence* n'est pas un risque *admissible*.

Dans l'un et l'autre cas, il ne sera pas possible de définir ce niveau de sécurité conventionnelle admissible d'une manière objective. Les concepteurs de ces systèmes devront alors être animés de cette « crainte salutaire » évoquée en fin de paragraphe 4 (puisque nous avons montré que le niveau de sécurité conventionnelle dépend, dans ce cas, d'une appréciation subjective des concepteurs du système) et continuer à imaginer les scénarios de panne de plus en plus complexes et à se prémunir contre celles-ci. Ils pourront bien sûr utiliser l'analyse présentée dans les chapitres 9, 10, 11, mais comme une *analyse architecturale* du système construit, indépendamment de toute référence à un objectif de sécurité.

Aussi, cette analyse devra-t-elle être complétée par une démarche permanente de sécurité. La centralisation obligatoire des informations, même relatives à des fonctionnements simplement défectueux sans que la sécurité ait été mise en cause, est un élément essentiel de cette démarche de mise en *sécurité progressive* et *d'exercice positif de cette « crainte salutaire »*.

Par ailleurs, la mise en place, dès la conception, de dispositifs permettant de rompre les scénarios d'accidents pouvant se produire, notamment par l'intervention de l'intelligence des opérateurs dans les boucles de réaction des automatismes, devrait également être un élément essentiel pour atteindre un niveau de sécurité acceptable dès la mise en service des installations.

Ce nécessaire suivi de la sécurité va cependant entraîner :

– des dépenses supplémentaires par rapport aux coûts initiaux, pour le suivi de la sécurité et le perfectionnement ; ces dépenses peuvent devenir considérables, tant pour les coûts directs qu'indirects, si elles obligent à reprendre d'une manière importante des dispositifs construits et en fonctionnement ;

– une diminution de la disponibilité du système, donc de sa rentabilité, au moins dans les premiers temps de fonctionnement.

Ce sont cependant les deux prix qu'il faut payer, en définitive, pour faire coexister *sécurité et innovation*.

Villeneuve d'Ascq, Février 1979. ■