COMPARAISON DE l'APPROCHE SECURITE MULTI-DOMAINE

David Mailland, Martial Schaff, Amélie Thionville, Julie Beugin

COMPARAISON DE L'APPROCHE SECURITE MULTI-DOMAINE

MULTI-DOMAIN COMPARISON OF SAFETY APPROACH

David MAILLAND
THALES ALENIA SPACE
26 avenue J.F. Champollion
31037 Toulouse Cedex 1 – France

Martial SCHAFF
THALES ALENIA SPACE
26 avenue J.F. Champollion
31037 Toulouse Cedex 1 – France

Amélie THIONVILLE
Valeo Electronics
14 avenue des Béguines - BP 68532
95892 Cergy Pontoise Cedex - France

Julie BEUGIN
IFSTTAR/Cosys/ESTAS
20 rue Elisée Reclus – BP 70317
59666 Villeneuve d'Ascq Cedex

Résumé

Cet article rappelle les fondements de la démarche démontrant la sécurité (origines, et motivation des critères) dans les différents domaines sélectionnés pour cette étude : Spatial, Aéronautique, Automobile, Ferroviaire.

A la fin de chaque partie, les auteurs ont proposé leurs conclusions pour de nouveaux domaines ou des missions multi-domaines, issues par exemple du numérique.

Summary

This article recalls the foundations of the approach demonstrating safety (origins and criteria) in the different domains selected for this study : Space, Aeronautics, Automobile, Rail.

At the end of each part, the authors proposed their conclusions for new domains or multi-domain missions, resulting for example from digital transformation.

Contexte

Les industriels sont à la recherche de solutions saisissant l'opportunité technologique de la révolution numérique. Pour cela ils inventent des solutions mettant en relation des domaines que tout séparait jusqu'à présent.

Dans le domaine spatial les ballons stratosphériques autonomes comme le projet Stratobus de Thales Alenia Space, à mi-chemin entre un drone et un satellite sont le moteur des réflexions actuelles. Concernant le domaine automobile, la voiture autonome, véritable disruption du numérique et qui doit être conçue pour garantir la sécurité de ses occupants et des autres usagers de la route est perçue comme la solution d'avenir. Les avions de transport civil sont également de plus en plus connectés, ce qui améliore la sécurité ainsi que le confort des passagers mais fait apparaître de nouveaux risques, tels que ceux liés à la cybersécurité par exemple. L'apport des technologies innovantes pour le développement du train autonome est également un enjeu dans le domaine ferroviaire, notamment dans le cadre du nouveau programme Tech4Rail de la SNCF. L'objectif est d'améliorer en toute sécurité la fluidité des circulations par l'automatisation de certaines fonctions du train jusqu'à implanter une intelligence à bord capable de prendre des décisions sans intervention humaine.

Afin d'anticiper cette transformation et dans le but de se positionner durablement en tant que leader de ces nouveaux marchés il est essentiel pour ces industriels de proposer avec leur produit de nouvelles approches de sécurité.

Enfin, il arrive régulièrement que deux domaines s'hybrident, et des difficultés ne manquent pas d'apparaître au niveau des interfaces. C'est par exemple le cas dans le cadre de l'utilisation des systèmes satellitaires pour le domaine ferroviaire, en particulier EGNOS[1] qui répond à des standards spécifiques. Une tendance forte du marché est en effet d'évoluer vers des systèmes de systèmes critiques.

Des initiatives similaires ont déjà vu le jour comme par exemple le projet OPENCOSS (Open Platform for EvolutioNary Certification Of Safety-critical Systems) financé par la Commision Européenne dont l'objectif était d'essayer de standardiser l'approche de sécurité pour certains domaines (avionique, ferroviaire et automobile). Le projet DREAMS (Distributed REal-time Architecture for Mixed Criticality Systems) également pour but de développer une architecture et des outils multi-domaines pour des réseaux de systèmes complexes. Ou encore, le projet européen USE-IT (users, safety, security and energy in transport infrastructure) a pour but d'identifier des axes de recherche communs à plusieurs modes de transport, en particulier en ce qui concerne leurs infrastructures.

Afin de dégager des pistes pour une démarche sécurité multi-domaine, une équipe a été constituée faisant intervenir un expert pour chacun des domaines suivants : Spatial (dans un contexte sécurité, par exemple avec l'utilisation des systèmes satellitaires pour la navigation), Aéronautique, Automobile et Ferroviaire.

Ces domaines ont été choisis pour plusieurs raisons :

- Après plusieurs décennies de stabilité, ces domaines liés au transport, s'apprêtent à subir de profondes mutations du fait de l'apparition du numérique. Preuve en est le thème de la conférence TRA2018 (Transport Arena Research) : « a digital era for transport ».
- Ils présentent tous des problématiques de sécurité des biens et des personnes.

Chaque expert a documenté la méthodologie sécurité pour son domaine en précisant :

- Quelles sont les objectifs quantitatifs de haut niveau.
- Comment est établie la classification des risques.
- Quelles sont les exigences qualitatives.
- Comment sont pris en compte les aspects développement logiciel.
- Comment sont traités les aspects certification

Pour pouvoir comparer les différentes approches, les origines historiques de chacune des exigences, ainsi que leurs limites ont été indiquées. Enfin un travail de réflexion a été mené entre les experts de chaque domaine pour tirer des conclusions sur la comparaison effectuée (facteurs communs et éléments différenciateurs) en vue de l'application à de nouveaux types de mission.

Objectifs quantitatifs

Les exigences quantitatives des **avions de transport** (plus de 5670kg) sont décrites dans l'AC 25.1309, document

[1] EGNOS (European Geostationary Navigation Overlay Service) est un SBAS (Satellite-Based Augmentation Systems) composé de satellites géostationnaires et de stations au sol prévus pour améliorer les performances des systèmes de navigation et de géolocalisation par satellites, tels le GPS ou Galileo. Pour cela, les satellites d'EGNOS diffusent des données de correction d'erreurs et d'alerte en cas de perte d'intégrité des signaux de navigation, aux utilisateurs munis d'un récepteur adapté.

expliquant quels sont les moyens acceptables de satisfaire à la réglementation sur la navigabilité. La CS 25.1309 reste générale en indiquant que « les équipements doivent être conçus pour fonctionner correctement dans toutes les conditions prévisibles ».

L'AC 25.1309 associe les conséquences d'une panne classée suivant une échelle de gravité des conséquences d'une défaillance, à une probabilité d'occurrence.

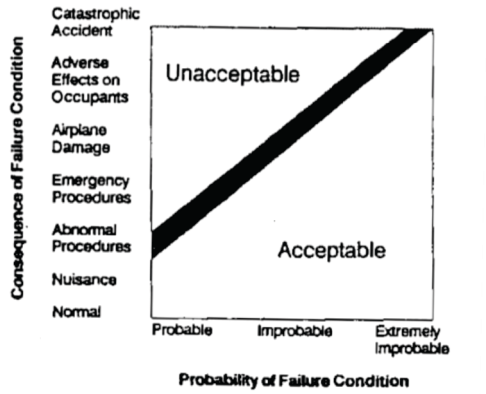

Figure 1. Quantification des risques dans le domaine aéronautique.

Les objectifs probabilistes sont précisés dans le même document.

(3) Extremely Improbable failure conditions are those having a probability on the order of 1 X 10^{-9} or less.

Figure 2. Exemple d'objectifs probabilistes dans le domaine aéronautique.

L'AMJ 25.1309, document décrivant de quelle manière il est possible de démontrer la conformité aux documents mentionnés précédemment revient sur ces probabilités et en donne l'origine, précisant qu'historiquement les premières analyses étaient purement qualitatives (pas de panne simple) et que les analyses quantitatives ont été introduites par la suite pour prendre en compte les pannes multiples.

Ces objectifs sont issus des données historiques. Un accident d'avion « grave » (qu'il faut comprendre comme « catastrophique ») a lieu tous les millions d'heures et environ 10% de ces accidents peut être imputé à des pannes. L'AMJ indique qu'il semble donc « raisonnable » d'allouer à tous les futurs avions une probabilité d'accident « grave » due à une panne inférieure à 10^{-7} par heure de vol. Faisant l'hypothèse que les analystes identifieront pour chaque avion de transport une centaine de « Failure conditions » « Catastrophiques », chacune d'entre elles se voit attribuer une probabilité de risque acceptable de 10^{-9} par heure de vol.

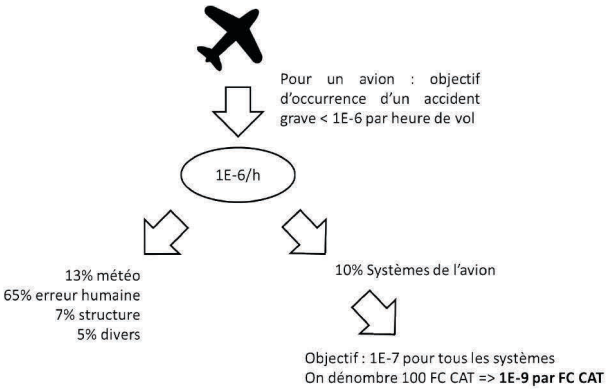

Figure 3. Origine de l'allocation des objectifs associés aux « failure conditions » dans le domaine aéronautique.

Dans le domaine **ferroviaire**, les objectifs quantitatifs, en particulier les objectifs de sécurité, dépendent du niveau selon lequel le système ferroviaire est considéré : au niveau de l'ensemble du réseau ferré avec l'ensemble des trains qui y circulent, au niveau d'un train, au niveau d'un sous-système du train ou d'un composant.

Des objectifs de sécurité communs (OSC ou CST – Common Safety Target) sont décrits dans les décisions européennes (ex. décision 2012/226/UE). Il concernent le système ferroviaire vu à son plus haut niveau.

Les RAC-TS (Risk Acceptation Criteria-Technical System) sont des critères d'acceptation des risques définis pour les systèmes techniques (hors procédures, méthodes organisationnelles, etc.). Les valeurs utilisées actuellement (10^{-9} ou 10^{-7} défaillance par heure d'exploitation pour, respectivement, des conséquences catastrophiques ou critiques) sont définies dans le règlement (UE) 2015/1136. Ces critères sont à utiliser uniquement lorsqu'il n'est pas possible de s'appuyer sur un système de référence duquel on peut tirer les exigences cibles (application du principe GAME très présent dans le domaine ferroviaire : Globalement au Moins Équivalent).

Les THR (Tolerable Hazard Rate) sont des objectifs de sécurité qui se présentent sous la forme de taux maximal d'occurrence acceptable pour des situations dangereuses. Un THR peut également être alloué aux fonctions de sécurité du système technique dès lors que leur défaillance est susceptible de mener à une situation dangereuse (Ouedraogo et al. 2018). La norme EN 50129 définit un tableau de correspondance THR/SIL pour relier le SIL (Safety Integrity Level – Niveau d'Intégrité de la Sécurité) des fonctions liées à la sécurité à ce taux. Ce tableau (cf. Annexe A.5.2, Tableau A.1) est tel que :

THR [h-1]	SIL
10-9≤THR＜10-8	4
10-8≤THR＜10-7	3
10-7≤THR＜10-6	2
10-6≤THR＜10-5	1

Table 1. Niveau d'Intégrité de la Sécurité dans le domaine ferroviaire.

Certains objectifs sont plus spécifiquement définis dans les règles nationales ou dans les règles européennes (ex. la STI-CCS –règlement (EU) 2016/919– stipule que « pour le danger "dépassement des limites de vitesse et/ou de distance conseillées à l'ERTMS/ETCS[2]", le taux admissible est de 10^{-9}/h pour les défaillances aléatoires pour l'ERTMS/ETCS bord et pour l'ERTMS/ETCS sol ».

Dans le domaine **spatial** appliqué à la navigation aéronautique, les exigences proviennent de l'Annexe 10 de l'ICAO SARPS : Les statistiques historiques sur les aéronefs ont conduit à un taux d'accidents mortels de l'ordre de 1e-6 / heure de vol. La plupart des accidents ont été causés par des erreurs humaines ou météorologiques et 10% par les sous-systèmes de l'avion.

Sur ces considérations, 1e-7 / h ont été alloués aux systèmes de l'avion et une allocation a ensuite été répartie entre les phases de la mission, par ex. une probabilité de 1e-8 est calculée par approche ou 5e-8 / h en phase de croisière.

Pour le SBAS EGNOS, l'allocation de ce chiffre se fait par l'intermédiaire d'un arbre de défaillance dédié (la spécification est relâchée car le SBAS n'est pas un système de niveau « catastrophique » mais seulement « dangereux » (critique)) pour finalement attribuer un risque d'intégrité d'approche au SBAS. système. Ce niveau de sécurité cible de 1e-7 / h est également conforme à l'objectif quantitatif ARP4754 pour les événements dangereux.

[2] ERTMS (European Railway Trafic Management System) correspond à un standard européen qui vise à faciliter le passage des trains aux frontières et à renforcer l'efficacité et la sécurité de leur circulation. ERTMS utilise le sous-système de contrôle-commande et de signalisation ETCS (European Train Control System).

Les objectifs quantitatifs pour le programme EGNOS, vis à vis de chacun des événements redoutés suivants sont finalement les suivants :

- integrity risk <2e-7/approach (with Time To Alert of 6s)
- integrity risk<1e-7/h (with Time To Alert of 10s)
- continuity risk<8e-5/approach
- continuity risk<1e-5/h

Pour le domaine spatial appliqué à la localisation ferroviaire, les exigences de l'ICAO en termes de disponibilité, de continuité, de précision et d'intégrité de la localisation, n'ont pas de correspondance directe avec les critères de performances utilisés dans le domaine ferroviaire (Marais et al. 2017). Ces derniers sont en lien avec les performances FDMS (cf. norme EN 50126).

Dans le secteur **automobile**, la définition des évènements redoutés est issue d'une analyse des dangers et d'une évaluation des risques (Hazard analysis and Risk Assessment selon l'ISO2626-3 :2011). Le point de vue est limité à un seul véhicule, et non une flotte d'automobiles. Ce point a été très discuté lors de la définition des niveaux de sécurité automobile car le fait d'avoir un défaut sur un calculateur entraînant le rappel d'un million de véhicules n'a pas le même impact que l'accident de 5 personnes.

Cette analyse systématique des dangers permet d'identifier les objectifs de sécurité (Safety Goal) pour une fonction véhicule donnée et le niveau d'intégrité de la sécurité associé (ASIL, Automotive Safety Integrity Level).

Ce niveau d'intégrité est déterminé à partir de trois facteurs :

- La sévérité,
- L'exposition au risque,
- La contrôlabilité

La sévérité est évaluée sur 4 niveaux : S0 : pas de blessures à S3 : blessures fatales. Pour caractériser ces niveaux, la norme s'appuie sur les études réalisées par l'Association for the Advancement of Automotive Medicine (AAAM).

L'exposition au risque est évaluée sur 5 niveaux E0 : Peu probable à E4 : Forte probabilité. La caractérisation de cette probabilité s'appuie soit sur un pourcentage du temps par rapport au temps opérationnel soit sur la fréquence de la situation.

Le dernier facteur, la contrôlabilité, correspond à la capacité du conducteur à compenser/rattraper le défaut. A titre d'exemple il est beaucoup plus facile de gérer une augmentation du volume sonore de l'autoradio, par rapport à une perte de la direction du véhicule.

Le niveau d'intégrité de la sécurité est déterminé selon le tableau suivant :

Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Table 2. Niveau de sévérité dans le domaine automobile.

Bien que ces critères s'appuient sur des définitions précises, l'évaluation laisse une part de subjectivité dans la définition du niveau de l'intégrité des objectifs de sécurité.

La norme SAE J2980 donne des orientations et des exemples sur la conduite de l'analyse des dangers en précisant les situations de vie à étudier.

Les objectifs quantitatifs, en particulier les objectifs de sécurité, dépendent de l'ASIL. Deux métriques fonction de l'ASIL sont proposées dans l'iSO26262-5 :

- L'évaluation du PMHF (Probabilistic Metric for random Hardware Failures)

ASIL	Random hardware failure target values
D	$<10^{-8}$ h^{-1}
C	$<10^{-7}$ h^{-1}
B	$<10^{-7}$ h^{-1}
NOTE The quantitative target values described in this table can be tailored as specified in 4.1 to fit specific uses of the item (e.g. if the item is able to violate the safety goal for durations longer than the typical use of a passenger car).	

Table 3. Objectifs quantitatifs dans le domaine automobile (première métrique).

- L'évaluation de chaque cause pouvant entraîner la violation des objectifs de sécurité en considérant à la fois l'occurrence du défaut et l'efficacité du mécanisme de sécurité

ASIL of the safety goal	Diagnostic coverage with respect to residual faults			
	≥99,9 %	≥99 %	≥90 %	<90 %
D	Failure rate class 4	Failure rate class 3	Failure rate class 2	Failure rate class 1 + dedicated measures[a]
C	Failure rate class 5	Failure rate class 4	Failure rate class 3	Failure rate class 2 + dedicated measures[a]
B	Failure rate class 5	Failure rate class 4	Failure rate class 3	Failure rate class 2
[a] The note in requirement 9.4.2.4 gives examples of dedicated measures.				

Table 4. Objectifs quantitatifs dans le domaine automobile (seconde métrique).

Ces objectifs quantitatifs ne portent que sur les défaillances aléatoires du matériel.

Classification des risques

Dans le domaine **ferroviaire**, chaque pays de l'Union Européenne possède sa propre échelle de gravité pour les événements dangereux. Pour la France, l'EPSF (Établissement Public de Sécurité Ferroviaire) définit une échelle de gravité à six niveaux pour les événements qu'il recense:

- Événement « mineur » de sécurité
- Événement qui aurait pu avoir des conséquences sur les matériels, voire des blessés légers
- Événement qui aurait pu avoir des conséquences humaines individuelles (un ou deux blessés graves) ou une personne tuée
- Événement qui aurait pu avoir des conséquences humaines collectives (nombreux blessés graves et/ou plusieurs personnes tuées)
- Accident qui a eu des conséquences significatives
- Accident qui a eu des conséquences graves.

Les types d'événements dangereux dépendent du système considéré. Pour le système européen ERTMS, le principal événement dangereux pour le sous-système de contrôle commande ETCS est *exceedance of the safe speed or distance as advised to ETCS*.

Les principaux accidents ferroviaires dont un système ferroviaire doit se prémunir sont (cf. article 22 de l'arrêté du 19 mars 2012):

- les collisions (frontales, par rattrapage, à une intersection, à un passage à niveau, avec un obstacle sur la voie)
- les déraillements (en pleine voie, en courbes, à une intersection)
- divers (feux et explosions, chute de personne du train, accident de personne à quai)

En France, l'EPSF porte les règles nationales de sécurité ferroviaires et se réfère à des textes officiels, notamment à l'Arrêté du 19 mars 2012 fixant les objectifs, les méthodes, les indicateurs de sécurité et la réglementation technique de sécurité et d'interopérabilité nationale.

En Europe, l'EUAR (Agence Ferroviaire Européenne) porte les règles et exigences d'interopérabilité ferroviaire au niveau européen (notamment les STI : Spécifications Techniques d'Interopérabilité). Elle publie et met à jour les textes qui concernent le système interopérable ERTMS (European Railway Traffic Management System).

Dans le domaine **aéronautique**, les niveaux de criticité sont définis de la sorte :

Catastrophique :

- Dommages importants sur l'environnement

- Dommages et décès collatéraux
- Mort des occupants
- Perte de l'avion

Critique :

- Réduction importante des marges de sécurité et des capacités fonctionnelles.
- Charge de travail trop importante pour que l'équipage puisse exécuter ses tâches de manière précise et complète
- Blessures ne permettant pas à l'équipage d'assurer sa mission correctement
- Blessures sérieuses ou fatales sur une petite partie des occupants

Majeur :

- Réduction significative des marges de sécurité et des capacités fonctionnelles.
- Augmentation de la charge de travail de l'équipage et diminuant son efficacité.
- Inconfort pour les occupants de l'avion
- Blessures légères possibles.

Mineur :

- Faible réduction des marges de sécurité et des capacités fonctionnelles.
- Augmentation légère de la charge de travail.
- Modification possible du plan de vol.
- Génération d 'une gêne pour les occupants

Dans le domaine de la navigation par satellite, le client définit généralement les événements redoutés avec l'aide du fournisseur, dans un process itératif: « *Afin de mener à bien l'analyse de sécurité, le contractant devra analyser les événements redoutés suivants :*

- effet critique: perte de l'intégrité du signal (c.-à-d. génération d'informations erronées ou trompeuses pouvant avoir des répercussions graves au niveau de l'utilisateur en supposant que le récepteur de celui-ci fonctionne parfaitement)

- effet majeur: perte de continuité du service de navigation EGNOS niveau 2 ou niveau 3

- effet mineur: transmission de données d'interface ATC trompeuses ou erronées. »

Dans le secteur **automobile**, la définition des évènements redoutés est issue d'une analyse des dangers et d'une évaluation des risques (Hazard analysis and Risk Assessment selon l'ISO2626-3 :2011).

La sévérité est évaluée sur 4 niveaux :

- S0 : pas de blessures
- S1 : blessures modérées
- S2 : blessures graves, potentiellement mortelles, survie probable
- S3 : blessures mortelles ou incertaines

Le point de vue est limité à un seul véhicule, et non une flotte d'automobiles. Ce point a été très discuté lors de la définition des niveaux de sécurité automobile car le fait d'avoir un défaut sur un calculateur entraînant le rappel d'un million de véhicules n'a pas le même impact que l'accident de 5 personnes.

Objectifs qualitatifs

La réglementation **aéronautique** (AC 25.1309) requiert qu'aucune panne simple ne mène à des répercussions catastrophiques dans l'exigence suivante :

(1) In any system or subsystem, the failure of any single element, component, or connection during any one flight (brake release through ground deceleration to stop) should be assumed, regardless of its probability. Such single failures should not prevent continued safe flight and landing, or significantly reduce the capability of the airplane or the ability of the crew to cope with the resulting failure conditions.

Figure 3. Extrait de l'AC 25.1309 concernant les pannes simples.

Par ailleurs, la structure de l'avion est également concernée par l'absence de panne simple via les exigences de l'AC 25.571 : « *The damage tolerance evaluation of structure is intended to ensure that should serious fatigue, corrosion, or accidental damage occur within the design service goal of the airplane, the remaining structure can withstand reasonable loads without failure or excessive structural deformation until* the damage is detected. »

Dans le domaine **automobile**, la tolérance aux pannes s'appuie sur les métriques d'architectures, les critères ASIL :

	ASIL B	ASIL C	ASIL D
Single-point fault metric	≥90 %	≥97 %	≥99 %

Table 5. Critères ASIL pour les pannes simples.

	ASIL B	ASIL C	ASIL D
Latent-fault metric	≥60 %	≥80 %	≥90 %

Table 6. Critères ASIL pour les pannes latentes.

Ces exigences sont analysées de la sorte : dans 99% des cas, une panne de niveau ASIL D doit être détectée. Quant aux pannes latentes, elles ne sont tolérées que sur les mécanismes de détection (monitoring). On doit pouvoir les détecter au démarrage du véhicule, 1 fois par cycle de roulage, chaque cycle ayant une durée de 2h environ.
La tenue de ces métriques a un impact direct sur l'architecture. A titre d'exemple, pour assurer un taux de couverture de 99% sur la perte d'un signal, on pourra être amené à redonder le signal de manière réfléchie pour éviter les modes *communs*. Ces choix d'architecture sont décrits dans un concept de sécurité.

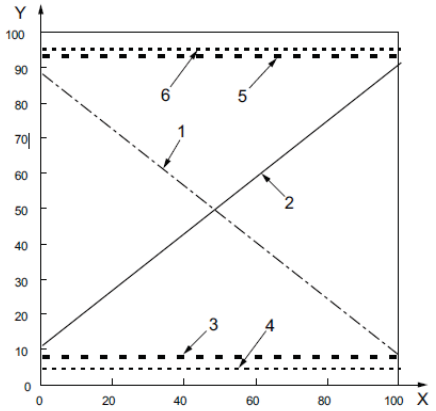

Figure 4. Exemple de redondance sur un signal dans le domaine automobile.

Dans le domaine **ferroviaire**, et d'après la norme EN50129, en cas de panne aléatoire simple, il est nécessaire de s'assurer que les systèmes relatifs à la sécurité (notamment de SIL 3 et SIL 4) restent dans un état de sécurité (fail-safe). Ce principe de sécurité intrinsèque peut être obtenu de différentes manières:

1) Sécurité composite

A l'aide de cette technique, chaque fonction relative à la sécurité est réalisée par au moins deux entités. Chacune de ces entités doit être indépendante de toutes les autres, pour éviter toute défaillance de mode commun. Des activités non restrictives ne sont autorisées que lorsque le nombre suffisant d'entités est d'accord. Une panne dangereuse dans une entité doit être détectée et passivée dans un délai suffisant pour éviter une panne similaire sur une seconde entité.

2) Sécurité réactive

Cette technique permet à une fonction relative à la sécurité d'être réalisée par une entité simple, à condition que son fonctionnement sûr soit assurée par une détection rapide et une passivation de toute panne dangereuse (par exemple, par cryptage, calcul multiple et comparaison, ou par test continu). Bien qu'une seule entité réalise la fonction effective relative à la sécurité, la fonction de contrôle/test/détection doit être

considérée comme une seconde entité, qui doit être indépendante pour éviter toute défaillance de mode commun.

3) Sécurité intrinsèque

Cette technique permet à une fonction relative à la sécurité d'être réalisée par une seule entité, à condition que tous les modes de défaillance vraisemblables de l'entité soient non dangereux. Le fait que tout mode de défaillance soit considéré comme invraisemblable (par exemple, grâce aux propriétés physiques intrinsèques) doit être justifié.

Pour contrer les pannes systématiques, outre les techniques de gestion de la qualité et de la sécurité qui sont utilisées pour minimiser la probabilité d'occurrence d'une erreur humaine (voir 5.2 et 5.3 de l'EN50129), des mesures techniques doivent être prises de sorte que la présence d'une panne systématique dangereuse n'engendre pas, autant que raisonnablement réalisable, de risque inacceptable.

Dans le domaine **spatial**, la conception du système EGNOS doit être telle qu'aucune défaillance unique ou erreur de l'opérateur ne puisse avoir des conséquences critiques.

Pour les défaillances multiples résultant d'un mode commun matériel ou logiciel, EGNOS ne doit pas entraîner de conséquences critiques.

Le système EGNOS et ses parties doivent être conçus de telle manière qu'une défaillance amène le système dans un état sûr (état qui n'entraîne pas de conséquences critiques ou catastrophiques).

Lorsque la sécurité de fonctionnement du système dépend de services externes (alimentation, par exemple), la conception du système doit être telle que des conséquences majeures, critiques ou catastrophiques ne soient pas induites (au moins pour un certain intervalle de temps défini pour chaque projet) après la perte ou le rétablissement soudain de ces services.

Considérant que la probabilité de défaillance de 1 unité (ou 1 algorithme ou 1 erreur opérateur) peut être supérieure à 1e-3 / h (ou 1e-3 ou 1e-3 / h), une défaillance unique ou une erreur opérateur avec conséquences critiques n'est pas acceptable.

Un mode commun peut être considéré comme un échec unique. Une conception sûre implique que le comportement du système est prédictible même en cas de défaillance.

Développement Logiciel

Dans le domaine **aéronautique**, un niveau d'assurance, le FDAL (Function Development Assurance Level), est alloué aux « failure conditions » identifiées dans la FHA (Functional Hazard Analysis) en se basant sur la sévérité associée à chacune et sans considération d'architecture.

Top-Level Failure Condition Severity Classification	Associated Top-Level FDAL Assignment
Catastrophic	A
Hazardous/Severe Major	B
Major	C
Minor	D
No Safety Effect	E

Table 7. Relation entre le niveau FDAL alloué et la sévérité de la fonction.

Dans un second temps, en prenant en compte l'architecture proposée par le biais de l'arbre de défaillance décrivant chaque « failure condition », un ITEM DAL est alloué à chaque entité suivant les règles décrites dans le document ARP4754 Rev.A. À la fin de ce processus, chaque logiciel se voit attribuer un ITEM DAL (SW DAL). C'est alors que la DO-178B s'applique. De manière équivalente l'ITEM DAL des composants physiques devient un HW DAL et la DO-254 s'applique. La norme DO-178B s'adresse au fournisseur du logiciel, celui-ci peut avoir recours à des règles de réduction suivant l'architecture de son logiciel :

- Architecture parallèle
- Architecture série
- Safety monitoring

Il est important de souligner que chaque document s'adresse à un niveau bien précis : système (ARP4754), logiciel (DO-178B) et hardware (DO-254).

Cette approche prenant en compte les fonctions est similaire à celle du domaine **ferroviaire** (SIL). Les SIL sont des niveaux discrets définis sur une échelle de 1 à 4 pour spécifier le niveau cible d'exigences en matière d'intégrité de sécurité de fonctions relatives à la sécurité. Une fonction peut être assurée par des équipements matériels et/ou logiciels.

La propriété d' « intégrité de sécurité » caractérise la manière dont sont contrôlées les défaillances aléatoires et les défaillances systématiques liées à un mode de défaillance dangereux d'une fonction relative à la sécurité.

La norme EN50128-version 2001 a introduit la notion de SSIL (Software SIL). Cette notion est amenée à disparaître comme un SIL concerne une fonction et non un équipement HW/SW.

Dans le domaine de l'**automobile**, les ASIL sont des niveaux discrets (A,B,C,D) définis pour spécifier le niveau cible d'exigences en matière d'intégrité de sécurité de fonctions du véhicule. Une fonction peut être assurée par un ou plusieurs composants matériels et/ou logiciels.

La propriété d' « intégrité de sécurité » caractérise la manière dont sont contrôlées les défaillances aléatoires et les défaillances systématiques liées à un mode de défaillance dangereux d'une fonction véhicule.

Dans le domaine **spatial**, les règles sont en apparence assez simple : les logiciels pour lesquels un comportement erroné peut entraîner :

- Un effet critique, se voit attribuer un niveau DAL B.
- Un effet majeur, se voit attribuer un niveau DAL C.
- Un effet mineur, se voit attribuer un niveau DAL D.

Dans le cas du développement d'une fonction critique (c'est-à-dire équivalente à un niveau de DAL B) basée sur l'utilisation d'un FPGA, des conditions particulières s'appliquent.

Certification / Autorisation de mise en service

Il n'y a pas de certification dans le domaine **Automobile**. En revanche, il existe des « mesures de confirmation » :

- Revue de confirmation
- Audit de sécurité
- Evaluation de sécurité

Les revues vérifient la conformité de livrable spécifique par rapport à des exigences de l'ISO26262, l'audit permet de s'assurer que le processus a été respecté. Enfin l'évaluation de sécurité permet de vérifier l'intégrité de la fonction véhicule.

Ces mesures de confirmation sont réalisées par des personnes dont le niveau d'indépendance est suffisant par rapport à l'ASIL, à titre d'exemple :

Confirmation measures	Degree of independency[3] applies to ASIL				Scope
	A	B	C	D	
Confirmation review of the hazard analysis and risk assessment of the item (see ISO 26262-3:2011, Clauses 5 and 7, and, if applicable, ISO 26262-8:2011, Clause 5) Independence with regard to the developers of the item, project management and the authors of the work product	I3	I3	I3	I3	The scope of this review shall include the correctness of the determined ASILs and quality management (QM) ratings of the identified hazardous events for the item, and a review of the safety goals
Confirmation review of the safety plan (see 6.5.1) Independence with regard to the developers of the item, project management and the authors of the work product	—	I1	I2	I3	Applies to the highest ASIL among the safety goals of the item

Avec I3 : personne indépendante du département responsable de la mise en production.

Table 8. Définition du niveau d'indépendance des intervenants dans le domaine automobile.

Dans le domaine **aéronautique**, avant de pouvoir être opéré chaque avion de transport doit obtenir une certification de type de la part des autorités de certifications, l'EASA (European Aviation Safety Agency) pour les constructeurs situés dans l'Union Européenne. Lorsqu'un modèle d'aéronef détient un certificat de type, chaque exemplaire de cet aéronef doit également détenir un certificat de navigabilité. La certification permet à l'avion d'évoluer dans l'espace aérien européen. Afin de pouvoir survoler d'autres zones, comme par exemple le

territoire américain, il est nécessaire de satisfaire les exigences de la FAA (Federal Aviation Administration), en application des traités d'accord bilatéraux signés entre les différents pays.

Le processus est le suivant : le projet (généralement un avion entier ou un moteur) est présenté aux autorités qui en déduisent les exigences à respecter pour obtenir la certification. Un Programme de Certification est ensuite établi entre les deux parties dans lequel chaque exigence doit être démontrée à une certaine date.

L'avionneur est ensuite chargé de démontrer que chaque partie de son produit est conforme aux exigences, celles-ci étant séparées en plusieurs parties : moteurs, structure, systèmes électriques, performances. La démonstration est faite par divers moyens : analyse, tests au sol, tests en vol et cette phase peut prendre du temps. Ainsi le programme A380 d'Airbus a été lancé le 19 Décembre 2000, le premier vol a eu lieu le 27 avril 2005 et la certification des A380-841/-842 a été obtenue le 12 décembre 2006.

Lorsque l'EASA estime que l'avion est conforme aux exigences elle met fin aux analyses et délivre le certificat pour l'espace aérien européen.

Cinq entités sont impliquées lors de la démonstration et l'évaluation de sécurité d'un projet **ferroviaire**:

- l'entité émettrice du besoin,
- l'entité proposant le changement (ex. nouveau train, nouveau sous-système de contrôle-commande),
- un (ou plusieurs) organisme(s) indépendant(s) d'évaluation de sécurité (ISA – Independent Safety Assessor). L'ISA permet aux différents acteurs du projet de s'assurer que les processus, méthodes et outils mis en œuvre sont conformes aux normes ferroviaires et au règlement MSC (on parle aussi de AsBo – Assessment Body pour la conformité à la MSC). Pour cela différents audits sont effectués tout le long du projet pour analyser les preuves de sécurité apportées, ceci afin de vérifier que les techniques d'évaluations utilisées sont appropriées et que les preuves apportées sont suffisantes. Il(s) délivre(nt) un ou plusieurs documents d'évaluation appelés « rapports ISA ».
- un organisme notifié (NoBo – Notified Body). Un organisme est notifié par un état membre auprès de la Commission Européenne pour l'interopérabilité ferroviaire grande vitesse et conventionnelle (ex. Certifer). Il est également indépendant du projet qu'il évalue et effectue des évaluations de conformité en accord avec les textes Européens (en particulier, les STI – Spécifications Techniques d'Interopérabilité). Il fournit des certificats de conformité pour chaque constituant d'interopérabilité (i.e. un certificat par sous-système évalué, ex. pour le contrôle commande, l'infrastructure, la gestion d'énergie,…).
- l'autorité de sécurité nationale (NSA – National Safety Authority) telle l'EPSF. Elle donne l'autorisation finale permettant de mettre le produit en exploitation (APIS – Authorisation for Placing Into Service). Elle s'appuie sur les différents documents liés à la sécurité fournis par les acteurs du projet.

Une sixième entité intervient pour vérifier le respect des règles nationales. Il s'agit de l'OQA (Organisme Qualifié Agréé) appelé au niveau Européen : Organisme Désigné (DeBo – Designated Body).

A la fin d'un projet, on parle d'autorisation de mise en service commerciale (AMEC / APIS en anglais) d'un système plutôt que de certification. La certification concerne un constituant spécifique.

La notion de « certification » apparait dans le domaine de la **Navigation par Satellite** pour des systèmes SBAS tel qu'EGNOS, certifié pour l'aviation. Ce type de Systèmes, considérés comme des Systèmes Safety Of Life –SoL-, fournit des informations de sécurité à un utilisateur « avion » pour le guider lors des phases d'approche. Il est de niveau « Critique ».

En Europe, la réglementation encadrant le développement et l'exploitation de tels systèmes est la réglementation Single European Sky (SES) vis-à-vis des Systèmes ATM/ANS. Les différents acteurs qui interviennent dans ce processus de certification sont les suivants :

- L'autorité de certification est l'EASA qui certifie le fournisseur de services ATM/ANS en tant qu'organisation et autorise le fournisseur de service à opérer le Système SBAS qui aura été qualifié.
- La Commission Européenne (EC): L'EC supervise le programme EGNOS. L'EC est propriétaire du Système SBAS Européen et délègue à la GSA (Agence européenne du système global de navigation par satellite) le rôle de gérer l'exploitation du SBAS Européen.
- La GSA est le « Design Authority » du Système EGNOS. La GSA est responsable de l'établissement du « Safety Case Part A » qui rassemble les preuves de la conformité de la conception du Système EGNOS.
- European Space Agency (ESA): En tant qu'Architecte Système, l'Agence Spatiale Européenne a la responsabilité de contrôler le design et le développement d'EGNOS. Elle assure que le système est conforme aux exigences de mission et aux exigences techniques spécifiées.
- L'industrie (Thales Alenia Space) est responsable de la conception et de la qualification d'EGNOS. Elle collecte toutes les preuves démontrant la conformité du système aux exigences spécifiées.

En terme de processus, le Système EGNOS pourra être mis en service sous les conditions suivantes :

- Le fournisseur de service est certifié en tant qu'organisation ANSP (Air Navigation Services Provider)
- Les Safety Cases part A (Design) et part B (operation et organisation) sont acceptés par l'EASA
- Le système EGNOS est qualifié et accepté par l'ESA et la GSA. Cela veut dire que toutes les revues de conception et de qualification ont été acceptées avec succès par l'architecte ESA et le « design authority » (GSA).

Ces systèmes SBAS sont fortement basés sur des logiciels assurant donc des fonctions de sécurité. On parle également de « certification » de ces logiciels car ils suivent les règles de développement de la DO-178B ou DO-278A. Leur certification individuelle fait partie du processus de qualification du Système SBAS.

Conclusions

La rédaction de cet article a permis aux différents experts de prendre du recul par rapport à leur domaine respectif. Lors des réunions de concertations, les points suivants ont été régulièrement abordés :

- Il existe de profondes différences de vocabulaire entre les domaines qui ne facilitent pas toujours les échanges. Ainsi le niveau « Système » des domaines spatial et du ferroviaire n'est pas équivalent au niveau « Système » de l'aéronautique et de l'automobile. Les deux premiers domaines considèrent en effet que le Système est l'ensemble des Segments, tandis que pour les deux autres un système est en réalité un « sous-système ». Autre exemple sur lequel les auteurs se sont longuement entretenus : le terme « intégrité » n'a pas du tout le même sens dans le domaine spatial (précision de la « localisation ») alors que les domaines ferroviaire et automobile considèrent qu'il s'agit de la confiance que l'on a dans la réalisation d'une fonction de sécurité.
- Les activités Safety ne sont pas toujours harmonisées au sein d'un même domaine (le modèle le plus disparate semble être le domaine automobile pour lequel chaque constructeur a sa propre liste d'événements redoutés par exemple), mais des initiatives existent pour aller dans ce sens (harmonisation européenne en cours dans le domaine ferroviaire par exemple).
- On remarque une gradation, dans la « sévérité » des analyses. Les domaines les plus sévères étant sans doute l'Aéronautique et le Ferroviaire. Les risques dans ce domaine sont perçus de manière très négative, s'il est acceptable d'avoir un accident de voiture, il en va autrement d'un accident d'avion.

- Concernant le développement logiciel, les analyses peuvent sembler a priori similaire entre les domaines. En particulier, il n'y a pas de critère quantitatif utilisé pour définir le niveau « SIL » ou « DAL ». De même, il n'y a pas de quantification associée aux erreurs logicielles dans les arbres de défaillance. Néanmoins, de subtiles différences existent, ce qui ne les rend pas compatibles entre elles et très difficilement comparables. Dans les domaines ferroviaire et automobile on parle de « SIL » mais les analyses sont complètement différentes par rapport à l'aéronautique et au spatial..
- Les causes externes sont prises en compte dans le domaine aéronautique (Analyses de Risques Particuliers comme l'impact oiseau), tandis qu'elles sont considérées hors du contour des analyses de Sécurité et couverts par des marges de sécurité dans le domaine automobile , et qu'elles sont traitées via des scénarios dédiés dans le ferroviaire.
- La remarque précédente peut être étendue aux autres points développés dans cet article : règle de tolérance aux pannes, exigences quantitatives, exigences qualitatives.
- L'inhomogénéité des risques couverts est assez nette entre les domaines (sécurité passagers, public extérieur, destruction du matériel …).
- Prise en compte différente du pilote / de l'opérateur entre les domaines. L'impact de l'opérateur intervient par exemple dans la détermination du « SIL » dans l'automobile ou le ferroviaire, ce qui n'est pas le cas dans l'aéronautique et le spatial. Généralement la prise en compte est indirecte, par relâchement des exigences de sécurité. Les erreurs de l'opérateur ne sont pas quantifiées dans les analyses par arbres de défaillances.
- Enfin les limites de l'étude du « croisement » de plusieurs domaines ont été identifiées : il n'est pas toujours possible d'appliquer les principes de conception d'un domaine à un autre pour des raisons de coûts, de performance ou de volume disponible.

A la question : est-il possible d'envisager de réaliser des analyses de sécurité mêlant plusieurs domaines ou relatives à de nouveaux domaines ? Les auteurs sont unanimes, oui, et c'est certainement un des grands enjeux des dix prochaines années.

Remerciements

Les auteurs remercient M. Guy Gregoris de Thales Alenia Space pour sa contribution et son regard bienveillant sur cet article, ainsi que M. Jean-Pierre Ollivier-Henry de Thales Alenia Space également.

Références

AC 25.1309, 1988, System Design and Analysis, FAA (Federal Aviation Administration) Advisory Circular linked to part 25 of FAR (Federal Aviation Regulations).

AC 25.571, 2011, Damage Tolerance and Fatigue Evaluation of Structure.

ARP4754A, 2010, Guidelines for Development of Civil Aircraft and Systems, EUROCAE (European Organisation for Civil Aviation Equipment) and SAE (Society of Automotive Engineers) Aerospace Recommended Practices.

CS 25.1309, Equipment, Systems and Installations, Certification Specifications of FAR (Federal Aviation Regulations).

Décision 2012/226/UE, 2nde série d'objectifs de sécurité communs pour le système ferroviaire, Commission Européenne.

DO 178B/C, 2012, Software Considerations in Airborne Systems and Equipment Certification, EUROCAE and RTCA (Radio Technical Commission for Aeronautics).

DO 278A, 2011, Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems, RTCA (Radio Technical Commission for Aeronautics).

DO 254, 2000, Design Assurance Guidance for Airborne Electronic Hardware, RTCA (Radio Technical Commission for Aeronautics).

EN 50126, 2000, Applications ferroviaires: spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS), Comité Européen de Normalisation Électrotechnique.

EN 50128, 2011, Applications ferroviaires: logiciels pour systèmes de commande et de protection ferroviaire. Comité Européen de Normalisation Électrotechnique.

EN 50129, 2003, Applications ferroviaires: systèmes de signalisation, de télécommunications et de traitement: systèmes électroniques de sécurité pour la signalisation. Comité Européen de Normalisation Électrotechnique.

ICAO, 2006, "International Standards and Recommended Practices, Annex 10 - Aeronautical telecommunications, Volume1 (Radio Navigation Aids)", International Civil Aviation organization.

ISO 26262, 2011, Véhicules routiers – Sécurité fonctionnelle, ISO - Organisation internationale de normalisation.

Marais J., Beugin J., Berbineau M., 2017, A survey of GNSS-based Research and Developments for the European railway signalling, IEEE Transactions on Intelligent Transportation Systems, vol. 18 (10): pp 2602-2618.

Ouedraogo K.-A., Beugin J., El-Koursi E.-M., Clarhaut J., Renaux D., Lisiecki F. (2018). Toward an application guide for Safety Integrity Level allocation in railway systems. Risk Analysis journal, DOI:10.1111/risa.12972.

Règlement d'exécution (UE) 402/2013, Méthode de Sécurité Commune relative à l'évaluation et à l'appréciation des risques d'un système ferroviaire, Commission Européenne, modifications apportées dans le règlement d'exécution (UE) 2015/1136 au 13 juillet.

Règlement (UE) 2016/919, Spécification technique d'interopérabilité concernant les sous-systèmes « contrôle-commande et signalisation » du système ferroviaire dans l'Union européenne, Commission Européenne.

SAE J2980 2015, Considerations for ISO 26262 ASIL Hazard Classification, SAE (Society of Automotive Engineers).

Transport Research Arena (TRA) 2018 – European Conference in Vienna, April 16-19, https://www.traconference.eu

USE-IT project, *users, safety, security and energy in transport infrastructure*, Horizon 2020 European Program, http://www.useitandfoxprojects.eu