Méthodologies de sûreté de fonctionnement pour les applications automobiles

Alessandra Nardi, Directrice Software Engineering Group, Solutions Automobiles, Cadence
Antonino Armato, Ingénieur principal Produits, Solutions Automobiles, Cadence

La voiture autonome est aujourd'hui un sujet récurrent dans les médias. Ce nouveau marché constitue un élément moteur extraordinaire pour l'évolution des développements de System-On-Chip (SoC) pour les applications automobiles. Les systèmes avancés d'assistance à la conduite (ADAS), précurseurs des véhicules autonomes, ont conduit à l'augmentation exponentielle du nombre de circuits électroniques dans les véhicules, mais aussi de leur complexité. Ces applications sont basées sur le traitement d'un volume très important de données qui nécessite le support de nœuds technologiques avancés de façon à répondre aux exigences de performances et de consommation. En conséquence, l'industrie automobile doit également faire face à un défi encore plus important en termes de fiabilité avec l'utilisation de technologies de pointe.

La sécurité devient une exigence fondamentale des systèmes automobiles pour garantir un niveau de risque tolérable. Deux normes de sécurité s'appliquent aujourd'hui : IEC 61508 (IEC), qui couvre le marché de l'électronique général, et l'ISO 26262 (ISO), spécifiquement dédiée à l'automobile.

Les constructeurs et équipementiers automobiles se conforment depuis longtemps à ces exigences. Toutefois, compte tenu de la complexité croissante, tous les participants de la chaîne logistique sont désormais sollicités pour apporter leur concours et permettre la mise en œuvre de normes couvrant la sûreté de fonctionnement et les divers aspects liés à la fiabilité. Ces métriques deviennent donc partie intégrante du flot de conception des semiconducteurs.

Les bases de la sûreté de fonctionnement

Définition

Selon les termes de la norme ISO 26262, la sûreté de fonctionnement est définie comme « l'absence de risques déraisonnables susceptibles d'être engendrés par le dysfonctionnement de systèmes électriques/électroniques. »

Cette définition peut être représentée sous la forme d'une chaîne d'implications (Fig. 1).



Fig. 1 : Chaîne d'implications selon la norme ISO 26262

Classification des défaillances et métriques des défaillances aléatoires sur matériels

La norme ISO 26262 classe en deux catégories les dysfonctionnements des composants électriques / électroniques :

- **Défaillances systématiques** : induites de manière déterministe pendant le développement, la fabrication ou la maintenance (problèmes de process).
- **Défaillances aléatoires** : apparaissent pendant la durée de vie d'un matériel, sont produites par des défauts aléatoires inhérents au process ou aux conditions d'utilisation, et peuvent aussi être classées en défaillances permanentes et transitoires.

Les défaillances aléatoires sont prises en compte pendant la phase de conception et de vérification des éléments matériels/logiciels, en intégrant des mécanismes de sûreté ayant pour vocation de s'assurer que l'architecture est en mesure de détecter des erreurs ou de contrôler des défaillances avec l'objectif de maintenir ou de parvenir à un état de sécurité adéquat.

L'efficacité d'un mécanisme de sécurité est mesurée par trois métriques permettant de détecter le taux de défaillances aléatoires (FIT) et de déterminer la probabilité globale du risque :

- **Métriques des points de panne uniques** : reflètent la robustesse d'un composant/fonction par rapport à un évènement ponctuel, soit par conception ou par respect des procédures de sécurité.
- **Métriques des défaillances potentielles** : reflètent la robustesse d'un composant/fonction, soit par conception, couverture de la défaillance via les procédures de sécurité, ou via l'identification par le conducteur de l'existence d'une défaillance, avant qu'un objectif de sécurité ne soit enfreint.
- **Métriques probabilistes pour les défaillances matérielles** : fournissent les raisons expliquant que les risques résiduels découlant de la violation d'un objectif de sûreté, en raison de défaillances matériel aléatoires, demeurent suffisamment faibles (Chang).

De manière intuitive, le point de panne unique peut conduire directement à la violation d'un objectif de sûreté, alors que la défaillance potentielle est un événement non détecté qui laisse la voie libre à une autre défaillance qui peut quant à elle engendrer une situation dangereuse.

Ces trois métriques consistent essentiellement à mesurer la sûreté de fonctionnement des composants matériels. Dans le reste de cet article nous mettons surtout l'accent sur la façon de les analyser et d'assurer une valeur cible.

Niveaux d'intégrité de sûreté automobile (ASIL)

Prenons comme exemple la défaillance d'une fonction définie au niveau du véhicule (par ex. un système ABS). S'ensuit une analyse des risques et des dangers afin de déterminer le risque de blessures pour les passagers et de dommages pour le véhicule. Cette analyse est basée sur l'exposition, la criticité et la contrôlabilité du danger et du risque qui en résultent, et permet de déterminer le niveau d'intégrité de sûreté automobile (ASIL), à savoir, le niveau de réduction des risques nécessaire pour parvenir à un seuil tolérable. La Fig. 2 montre un exemple de détermination ASIL. ASIL A est le niveau le moins contraignant en termes de réduction des risques ; le niveau ASIL D est le plus contraignant.

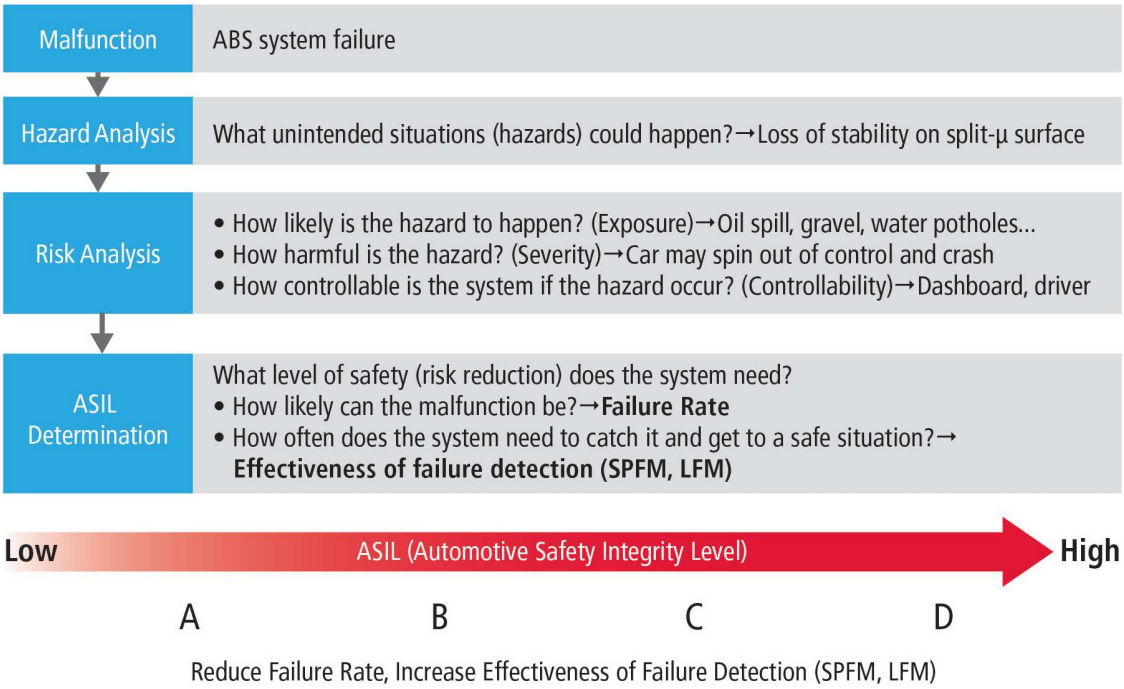


Fig. 2 : Exemple de détermination du niveau d'intégrité ASIL, avec dysfonctionnement d'un système ABS, basée sur l'analyse des dangers et des risques au niveau de la phase conceptuelle.

Cycle de la sûreté de fonctionnement et phases de développement

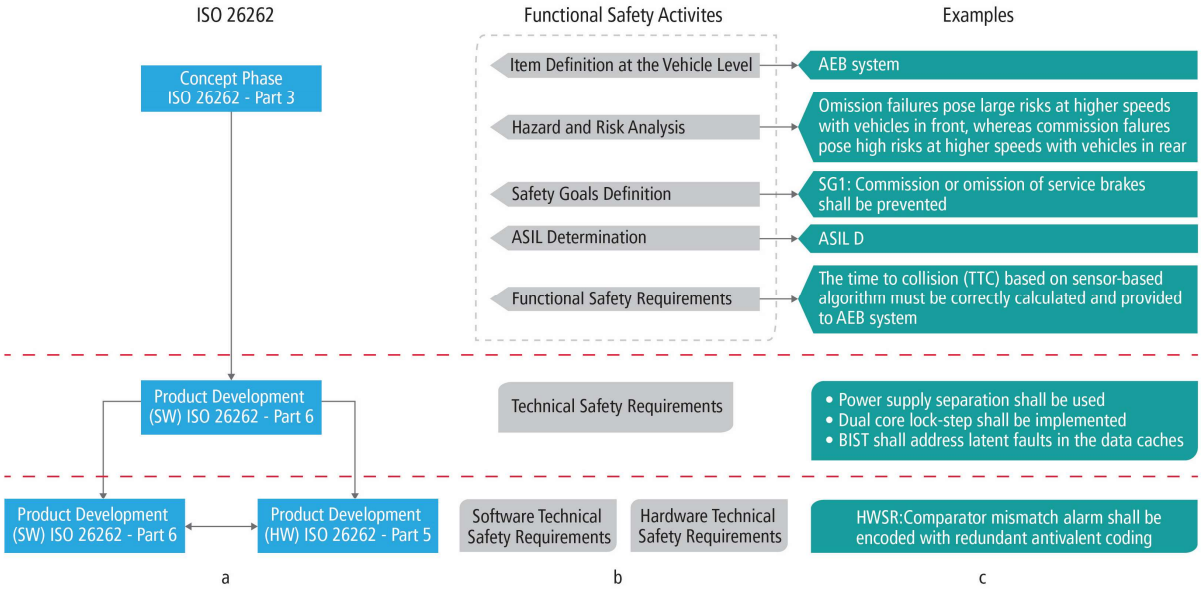


Fig. 3 : Processus de développement de la sûreté de fonctionnement, exigences associées et exemples

Toutes les phases du cycle de sûreté de fonctionnement sont définies et documentées par la norme ISO 26262. La Fig. 3a illustre les différentes phases de conception et de développement. Les Fig. 3b et 3c rapportent les activités de sûreté de fonctionnement correspondantes, avec des exemples. Les objectifs de sûreté commencent au niveau du véhicule et sont cartographiés et définis pendant la chaîne de développement, jusqu'à ce que les métriques de défaillance matérielle soient définies et affectées aux différents sous-systèmes matériels.

Analyse de la sûreté de fonctionnement

L'analyse de la sûreté de fonctionnement est utilisée pour évaluer le niveau de sûreté atteint par le produit. Elle comporte des évaluations quantitatives, comme l'analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC), une analyse temporelle, et des évaluations qualitatives, comme l'analyse de défaillance dépendante.

AMDEC

L'AMDEC est une approche structurée permettant de définir les modes et les taux de défaillance, ainsi que les capacités diagnostiques d'un composant matériel.

Basée sur la fonctionnalité des composants, la hiérarchie AMDEC est structurée en parties/sous-parties des modes de défaillance (ISO 26262). Pour chaque mode défini affectant les objectifs de sûreté, les données de base requises incluent :

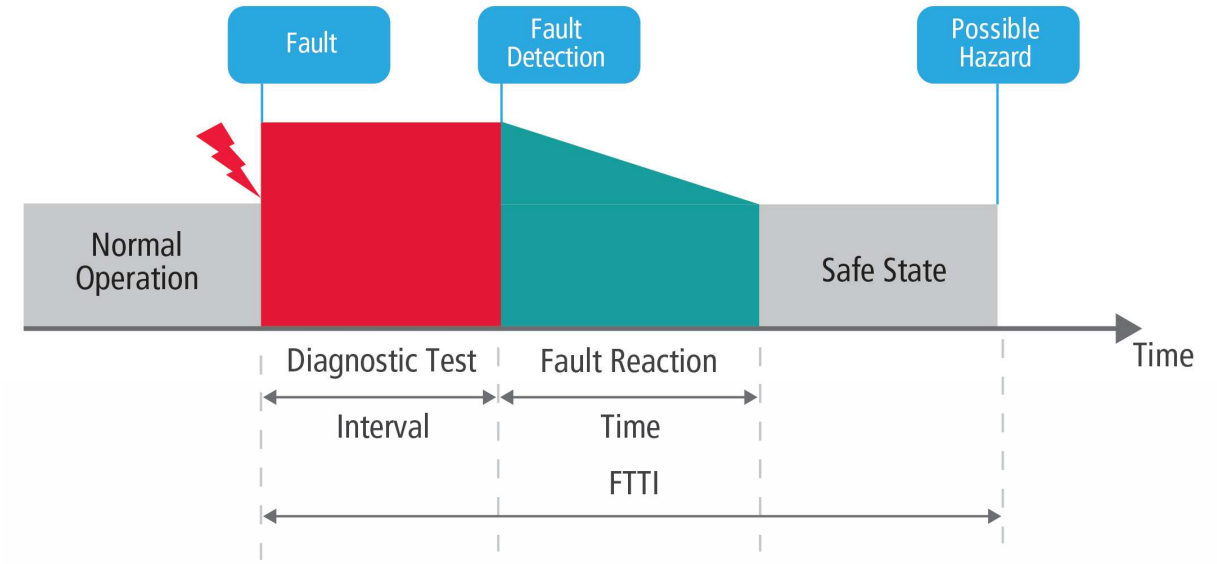
- **Taux de défaillance :** taux auquel le composant considéré subit des pannes. C'est donc sa fiabilité. Ce taux est exprimé en taux de défaillances aléatoires (FIT), qui est le nombre de défaillances attendu par milliard d'heures de fonctionnement.
- **Mécanisme de sûreté et couverture diagnostique :** présence d'un mécanisme de sûreté et son efficacité dans la détection des défaillances.

Il en résulte des métriques architecturales des matériels (métriques des points de panne uniques ; métriques des défaillances potentielles ; et métriques probabilistes pour défaillances matériel), qui indiquent la probabilité de défaillance du composant et le niveau de fiabilité du mécanisme de sûreté pour détecter l'incident et placer le système en situation de sécurité.

Le taux de défaillance des éléments matériels est estimé en fonction des données de fiabilité industrielles (par ex. IEC 61709, IEC TR 62380), dérivées des essais expérimentaux ou basées sur l'observation des incidents survenus sur le terrain, avec notamment l'analyse des matériaux qui sont retournés en raison de défaillances.

Analyse temporelle

L'évaluation complète des mécanismes de sûreté implique également les performances temporelles. De fait, le système doit pouvoir détecter les défaillances et assurer la transition vers un état de sécurité adéquat, dans l'intervalle de temps à tolérance de panne. Si tel n'est pas le cas, la défaillance peut se transformer en danger au niveau du système. La Fig. 4 illustre l'intervalle de test diagnostique, la partie de l'intervalle de temps à tolérance de panne allouée à la détection de l'événement (ISO 26262). A titre de référence, l'intervalle de test diagnostique dans un CPU peut être d'environ 10 ms, alors que 100 ms environ seront alloués à l'intervalle de temps à tolérance de panne pour l'ensemble du système.



Analyse de défaillance dépendante (DFA)

Un autre aspect à évaluer, notamment lorsque le système a des ressources partagées, est l'analyse de défaillance dépendante, autrement dit, l'analyse des causes communes possibles et des défaillances en cascade entre des éléments donnés. Elle permet d'identifier les causes uniques qui pourraient contourner l'indépendance requise, ou la non interférence entre des éléments donnés, et contrevenir à une exigence ou à un objectif de sûreté (ISO 26262).

L'ISO 26262 fournit une liste d'événements initiateurs de défaillances dépendantes à évaluer, et les contremesures types pour les éviter et en diminuer l'impact. On peut citer comme exemples d'initiateurs de défaillances dépendantes, avec les ressources partagées, les dysfonctionnements affectant les éléments d'horloge, les éléments d'alimentation électrique ou la logique commune de

réinitialisation ; alors que les initiateurs de défaillances dépendantes associés à des causes physiques aléatoires comprennent, par exemple, les court-circuits, le verrouillage et la diaphonie.

Exigences de la sûreté de fonctionnement et flot de conception

Cet article a essentiellement pour objectif d'expliquer comment la sûreté de fonctionnement est mise en œuvre dans le cadre du flux classique de conception/vérification RTL à GDS pour parvenir aux métriques de sûreté requises au niveau des matériels. L'AMDEC conduit l'exploration de la conception pour répondre aux objectifs de sûreté de fonctionnement, en vérifiant les mécanismes de sûreté et leurs métriques. Il pilote également les campagnes d'injection de défaillances permettant d'obtenir une évaluation plus précise de la couverture diagnostique des mécanismes de sûreté. Une analyse de défaillance dépendante est réalisée pour s'assurer de la viabilité des mesures prises pendant le flux RTL à GDS, afin de garantir l'indépendance et éviter les défaillances à cause commune.

La sélection des meilleurs mécanismes de sécurité requiert un compromis judicieux entre couverture diagnostique et coût, en termes de consommation électrique, surface, métriques de sûreté et performance temporelle. Les mécanismes de sûreté peuvent être des tests logiciels mise en œuvre dans la pile logicielle, ou des tests matériels élaborés manuellement au niveau RTL, ou insérés automatiquement dans le flot de conception.

Conception et implémentation

L'auto-test intégré (BIST) en ligne est le mécanisme de sûreté le plus notable déjà automatisé dans le flot de conception. Cet auto-test est exécuté lorsque les circuits fonctionnels se trouvent en mode opérationnel normal (mode mission) : il contribue aux métriques des points de panne uniques et présente des exigences temporelles plus rigoureuses dans la mesure où il intervient dans le cadre de l'intervalle de tests diagnostiques. L'auto-test intégré hors ligne est exécuté lorsque les circuits fonctionnels ne se trouvent pas en mode opérationnel normal ; par ex. pendant une remise à zéro lors du démarrage du moteur : il contribue aux métriques de défaillances potentielles, et les exigences temporelles sont alors moins rigoureuses.

A titre d'exemples de mécanismes de sûreté basés sur la redondance, on peut citer une **triple redondance modulaire** et le **mode lockstep double cœur (DCLS)**. Lorsque l'architecture de sûreté est basée sur une redondance matérielle, l'analyse de défaillance dépendante est nécessaire pour adresser la défaillance à cause commune due à des ressources partagées (par ex. alimentation électrique, horloge, signal de reset) et à des causes physiques uniques : essentiellement, l'indépendance logique doit se traduire en indépendance physique. Des techniques de conception spéciales sont nécessaires pour maintenir un haut niveau de couverture diagnostique.

Vérification

Lorsqu'une analyse AMDEC initiale est mise en œuvre pour évaluer l'état de préparation à la sûreté d'un IP/SoC, la couverture diagnostique pour les mécanismes de sûreté peut être estimée sur la base des valeurs pouvant être atteintes (faible, moyenne, haute), telles que définies dans la norme ISO 26262.

La simulation par injection de défaillances est une technique qui peut être utilisée pour vérifier plus précisément la valeur de couverture diagnostique, évaluer l'intervalle de tests diagnostiques et le temps de réaction à la défaillance (cf. tableau 2) ou pour confirmer l'effet de cette dernière.

La vérification de la sûreté de fonctionnement est réalisée à partir de la vérification fonctionnelle standard définissant la charge de travail à exécuter, les points d'observation (les points où observer l'effet des défaillances) et les points de détection (les points où observer la réaction d'un mécanisme de sûreté.)

Les défaillances peuvent être classées en fonction des effets sur les points d'observation et de diagnostic :

- **Défaillance dangereuse détectée** : l'effet est constaté à la fois au niveau des points d'observation et de diagnostic. Ce qui signifie que le mécanisme de sécurité l'a correctement détecté.
- **Défaillance dangereuse non détectée** : l'effet est constaté au niveau des points d'observation, mais pas des points de détection. Autrement dit, le mécanisme de sûreté ne l'a pas détectée.
- **Défaillance sûre** : la défaillance n'affecte pas le point d'observation. Il est important de noter que la défaillance peut être classée comme « sûre » uniquement si la charge de travail offre une bonne couverture pour la vérification fonctionnelle.

Lorsqu'une campagne d'injection de défaillances est mise en œuvre, décider du point d'injection des pannes demeure un élément critique. En fait, le mécanisme de sûreté en cours d'évaluation est ciblé en fonction d'un mode de défaillance spécifique du circuit. Les défaillances doivent être injectées uniquement dans la logique appartenant au mode de défaillance associé.

Conclusion

Le développement des voitures autonomes, avec l'accroissement concomitant du contenu électronique et la complexification qui s'ensuit, se traduisent par la nécessité de partager la responsabilité de garantie de la sûreté de fonctionnement à tous les niveaux de la chaine logistique, en comblant l'écart entre, d'une part, les constructeurs automobiles/équipementiers et, d'autre part, les fabricants de semiconducteurs et les fournisseurs d'outillage. Nous souhaitions, avec le présent article, présenter les fondamentaux de la sûreté de fonctionnement et divers aspects relatifs à la façon dont les méthodologies de conception captent et prennent en compte les nouvelles métriques de sûreté via la conception / implémentation et la vérification. A n'en pas douter, les méthodologies de conception vont continuer à progresser, élargissant ainsi l'éventail des possibilités de support des exigences de sûreté.