STRUCTURATION DE MODÈLES SDF DE CONCEPTION SYSTÈMES EN NIVEAUX D'ABSTRACTION

SYSTEM DEPENDABILITY-SAFETY MODELING IN ABSTRACTION LEVELS

E. Arbaretier, Z. Brik,
APSYS
22, quai Gallieni
92150 Suresnes
emmanuel.arbaretier@apsys.eads.net

V. Brindejonc B. Desmarquest et B. Robert
PSA Peugeot Citroën
Rte de Gizy
78943 Vélizy-Villacoublay Cedex
vincent.brindejonc@mpsa.com

Résumé

La complexité des systèmes ne cessant d'augmenter, les études de sûreté de fonctionnement (SdF) deviennent de plus en plus conséquentes et délicates à réaliser dans un de temps imparti qui reste inchangé.
La méthode proposée permet de gérer la complexité des études système à travers une structuration en couches d'abstractions. Inscrite dans une démarche de conception sûre, cette méthode offre la possibilité de vérification, de mise à jour, d'automatisation facilitée, et la possibilité de couplage avec la conception.

Summary

The increasing complexity of systems, leads to Safety and dependability studies more significant and difficult to be conducted in development time.
The method proposed allows managing the complexity of system dependability-safety studies through an organization in abstraction layers. Integrated in safe design process, this method allows model checking, updating and automation of coupling with design tools.

Introduction

Dans de nombreuses branches de l'industrie, la complexité des objets techniques développés ne cesse de s'accroître sous la pression des attentes client vis-à-vis du produit, mais également des possibilités techniques offertes par les avancées technologiques, en particulier mécatroniques et informatiques. Dans l'industrie automobile, cette complexité se traduit souvent par un partage important de nombreuses ressources (capteurs, calculateurs, actionneurs, réseaux multiplexés, etc.) qui se voient ainsi attribuer des responsabilités dans plusieurs fonctions.

Cette complexité oppose par elle-même de nombreux défis à la Sûreté de Fonctionnement (SdF) d'autant plus que les durées de développement sont de plus en plus réduites. Ces défis peuvent être classés en trois familles.

a) La capture des données de conception utilisables par la SdF : la représentation des systèmes entre concepteur de système et analyste SdF ne coïncident pas nécessairement.

b) L'analyse SdF en elle-même. En effet, une architecture et un fonctionnement complexes conduisent généralement à un grand nombre de modes de défaillances et à des liens causaux non triviaux. La structuration du modèle est donc cruciale et doit permettre de prendre en compte différents niveaux :

- Applicatif, exprimant ce que le concepteur attend du système qu'il développe,
- Logique, traduisant la manière d'atteindre ces buts,
- Physique, projetant cette manière sur des ressources physiques.

c) Le rebouclage de la SdF sur la conception à travers la mise en place de mécanismes de sécurisation, la génération d'exigences sur les modes de défaillances, l'émission d'exigences de contraintes sur des choix de conception, la traçabilité de ces exigences et la vérification de leur prise en compte correcte jusqu'au test.

La solution présentée permet d'apporter une réponse aux défis précités par un couplage entre l'outil de conception choisi par les métiers électroniques de PSA (Chaîne Outillée Continue) et une utilisation originale de l'outil SdF SIMFIA suivant des principes inspirés de l'Ingénierie Système Relativisée (ISR) [1] . Le couplage avec les outils de conception se fait au juste nécessaire en particulier en récupérant automatiquement dans l'outil SdF des éléments d'architectures. Cette récupération et les échanges entre conception et SdF ont été configurés dans les outils en construisant des scénarios d'utilisation métiers. Pour ne pas proposer de conception organique nous avons choisi de retenir comme niveau atomique les organes et les flux logiques entre ces organes. Cette approche permet également de bien séparer les sécurisations qui sont de responsabilité de l'architecte de celle qui sont de responsabilité du concepteur organique. Des éléments doivent être ajoutés au travers de l'environnement qui dans le modèle SdF permet de modéliser, outre l'environnement physique, la diversité, les aspects inter-systèmes et les événements redoutés.

Dans la suite du document, nous montrerons comment SIMFIA a été couplé avec les outils de conception et rappellerons les concepts de modélisation SIMFIA mis en jeux à ce stade, avant de décrire les modèles en niveaux d'abstraction et le format des exigences de sécurité au travers d'exemples métiers.

Couplage avec la conception

En 2007, en prévision de la publication de la Norme ISO 26262 [4][4], PSA a entamé une réflexion sur ce que nous avons appelé le processus de conception sûre. L'objectif a été de faire un état des lieux des pratiques et des outils en usage dans les différents métiers de conception et de définir les améliorations à apporter au regard de ce nouveau cadre, notamment en matière d'outil support. L'outil de conception en cours de développement était une Chaîne Outillée de Conception (COC), qui permet de réaliser les Schémas Opérationnels (SO) décrivant l'architecture fonctionnelle et l'allocation des fonctions élémentaires aux organes[1]. Dans un contexte d'intensification du développement de cette chaîne outillée, il a été décidé d'y accoster un outil SdF. Cet accostage avait pour but de réaliser les études de sûreté de fonctionnement sur la base des SO déjà définis et récupérés de manière à garantir l'adéquation entre les structures respectives du modèle fonctionnel et du modèle dysfonctionnel. Ce logiciel devait pouvoir évoluer pour intégrer les exigences définies par la Norme ISO 26262.

Ces orientations générales ont entraîné un processus de réflexion sur la manière d'appréhender nos activités de maîtrise de la sécurité, et plus particulièrement sur trois axes : l'articulation avec la conception, la modélisation dysfonctionnelle et le retour vers la conception.

1 L'articulation avec la conception

Il s'agit tout d'abord de capturer les données de conception utilisables par la SdF. Ces éléments sont souvent issus d'une analyse de type analyse fonctionnelle dont l'interprétation est souvent ambiguë pour la SdF. Lorsque les ressources sont au centre de l'analyse (type Analyse Fonctionnelle de type AFNOR 50501), un seul niveau d'abstraction est pris en compte à chaque échelle de description du système. Deux niveaux d'abstraction inconciliables sont souvent alors en conflits: celui du concepteur centré sur les flux de besoins et celui du fiabiliste centré sur les flux physiques. Lorsque les fonctions sont au centre de l'analyse (type Structured Analysis: SADT, SART), les ressources n'apparaissent qu'après coup, en tant que collection de fonctions embarquées, et la présence de flux internes aux ressources est quasi impossible à éviter.

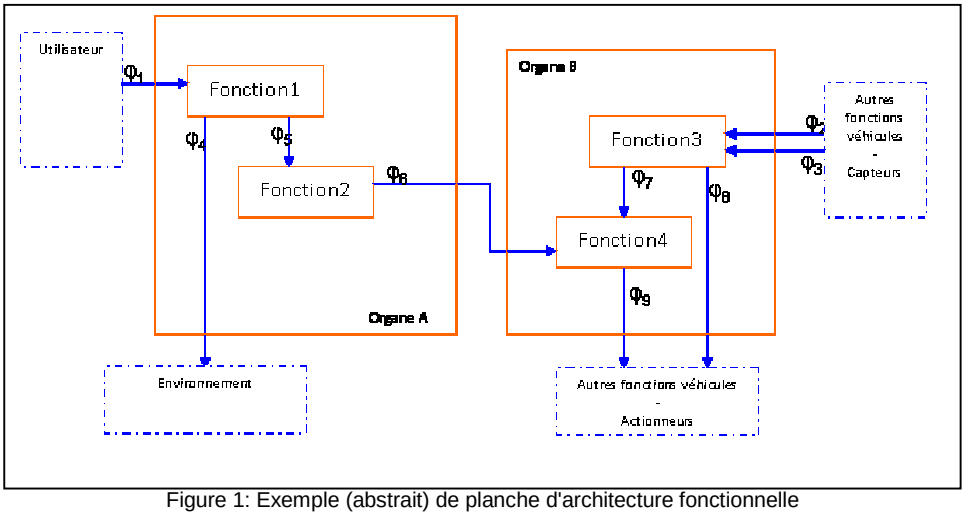

Figure 1: Exemple (abstrait) de planche d'architecture fonctionnelle

Sur la planche exemple proposé Figure 1~~Figure 1~~, l'analyste SdF doit faire abstraction des fonctions élémentaires (Fonction1, etc.) représentées par des rectangles en trait plein et doit prendre en compte les fonctions élémentaires en interface représentées par les rectangles en pointillé. La récupération d'un nombre suffisant d'objet dans la COC est nécessaire pour assurer la cohérence du modèle SdF. Il est néanmoins impératif de définir correctement l'angle de vue des éléments de conception qui seront étudiés, de manière à ne récupérer que les informations pertinentes pour les analyses de SdF, et de ne pas alourdir le modèle avec des informations ou objets inutiles.

En terme de volumétrie d'étude, le service SdF fournit des études pour plusieurs dizaines de dossier de conception dont plus de la moitié est mise à jour avec un rythme trimestriel. Ces dossiers comportent plusieurs planches d'architecture, selon la complexité de la fonction automobile spécifiée et les variantes techniques (boîte de vitesse manuelle ou automatique ; véhicule à moteur thermique, hybride, électrique ; etc.). Ces considérations nécessitent de définir des règles de modélisation qui soient simples, permettent à quiconque de vérifier aisément un modèle réalisé par une autre personne, ou de reprendre, dans le cadre d'un lissage de charge, un modèle déjà créé.

2 La modélisation dysfonctionnelle

L'analyse SdF représente elle-même un défi majeur. En effet, une architecture et un fonctionnement complexes conduisent généralement à un grand nombre de modes de défaillances et à des liens causaux non triviaux. La structuration du modèle est donc cruciale et doit permettre de prendre en compte différents niveaux traduisant différents points de vue complémentaires:

- Applicatif, exprimant ce que le concepteur attend du système qu'il développe,
- Logique traduisant la manière d'atteindre ces buts,
- Physiques projetant ces modalités sur des ressources physiques.

Considérant que les modèles dysfonctionnels statiques sont fondés sur la construction de polynômes logiques, décrivant les relations de dépendances entre les entrées et les sorties des constituants, trois approches sont envisageables pour prendre en compte la complexité liée aux organes. La première se fonde sur le caractère « boîte noire » des organes constituants élémentaires du point de vue de la conception. Cette approche, qui construit un polynôme unique par organe, conduit à des polynômes très complexes difficiles à lire, à communiquer et à maintenir. Une approche radicalement différente est celle de la

[1] Ces éléments sont ensuite utilisés pour simuler le fonctionnement de l'architecture ainsi définie.

décomposition fonctionnelle pratiquée au niveau conception. Cette approche décompose les fonctionnalités de l'organe en sous-fonctions. Elle ne respecte pas le caractère boîte noire des organes et présuppose une structuration interne. D'un point de vue pratique, l'expérience montre que cette approche conduit à multiplier les blocs internes à l'organe sans limiter les liens entre ces blocs et sans pour autant simplifier les polynômes de chacun de ces blocs. D'un point de vue conceptuel, la prescription de choix techniques internes aux organes - hors du périmètre de responsabilité et de compétence du métier prescripteur - conduit à une sur-spécification non maîtrisée car non-fondée sur les caractéristiques techniques de l'organe.

Nous ne saurons assez souligner ici la nécessité de mener une réflexion sur la manière de modéliser les systèmes. L'important n'est pas de déterminer quel est le meilleur outil, mais de savoir ce qui doit être manipulé, comment le récupérer, comment l'ordonnancer pour pouvoir exploiter et réutiliser les modèles, comment prendre en compte les variantes d'architecture, etc. La réalisation de maquettage à partir de l'atelier SIMFIA, version commercialisée au moment de la rédaction de notre cahier des charge, nous a permis de nous orienter vers une troisième approche, inspirée de l'Ingénierie Système Relativisée (ISR) [1]. Cette approche structure l'organe en vues partielles suivant quatre niveaux (ou couches) d'abstraction, similaires quel que soit l'organe :

- La couche physique qui gère l'interface de l'organe avec le monde extérieure,
- La couche de mise en forme qui permet de prendre en compte les contraintes de synchronisation en particulier pour les trames multiplexées,
- La couche de protocole qui permet de prendre en compte les mécanismes sécurisations : redondances spatiales, temporelles et surveillances,
- La couche applicative qui transforme les entrées en sorties.

Ce travail préalable nous a permis de faire mûrir l'expression de besoin initiale et de commencer à spécifier le nouveau processus d'analyse qui sera bientôt déployé. Nous reviendrons un peu plus loin sur les niveaux d'abstraction, au travers de son implémentation dans SIMFIA.

3 Le retour vers la conception

Un troisième défi réside dans l'action de la SdF sur la conception par la mise en place de mécanismes de sécurisation, la génération d'exigences sur les modes de défaillance, l'émission d'exigences de contraintes sur des choix de conception, la traçabilité de ces exigences et la vérification de leur prise en compte correcte jusqu'au test. Ce rebouclage permet aux différents acteurs de la conception d'optimiser la solution technique choisie. Dans le cadre de SIMFIA elle se fonde sur une synthèse ALTARICA du modèle de conception et sur une comparaison de la structure du modèle ALTARICA obtenu avec celle issue du modèle SdF. Ainsi les évolutions structurelles apportées par les métiers de conception et SdF peuvent être tracées et prise en compte dans des processus parallèles qui finissent par converger vers une représentation unifiée.

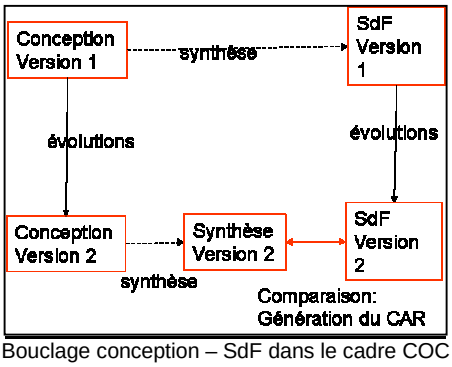

Figure 2: Bouclage conception – SdF dans le cadre COC - SIMFIA

Import des données saisies dans la COC

Le langage ALTARICA a été choisi comme format d'échange entre SIMFIA et la COC :

- Il est très approprié pour la description d'un grand nombre de systèmes,
- C'est un langage hiérarchique, où presque toutes les constructions syntaxiques ont une représentation graphique analogue,
- Il généralise les formalismes de description les plus utilisés tels que les réseaux de Pétri ou les diagrammes blocs.

Description du processus d'Import, de Modification puis de Stockage dans la COC

Le processus d'import peut se mettre en œuvre sous les modalités suivantes:

- Consolidation des éléments d'architecture saisis dans la COC sous forme de SO (Schéma Opérationnel) afin de constituer le fichier ALTARICA de la "Synthèse Initiale". Ce fichier prend en compte la structuration de chaque organe en différentes couches abstraites (couche physique, couche de mise en forme, couche de protocole et couche applicative),
- Invocation de SIMFIA à partir de la COC pour charger le modèle correspondant à la synthèse initiale,
- Enrichissement du modèle et ce en renseignant les relations logiques entre les flux entrées et sorties de chaque bloc élémentaire,
- Prise en compte des différentes situations de vie applicables ainsi que de la diversité (options et variantes),
- Génération de la resynthèse qui est constituée du fichier "Altarica" contenant le modèle et d'un fichier XML contenant les données utilisateur attachées aux objets ainsi que les coordonnées graphiques de chaque élément,
- Comparaison du modèle SIMFIA avec la synthèse initiale et génération du CAR (Change Analysis Report),
- Stockage de la resynthèse et du CAR dans la COC,

- Invocation de SIMFIA à partir de la COC pour charger la resynthèse,
- Modification du modèle puis stockage dans la COC.

Concepts de modélisation SIMFIA mis en jeux

1 Positionnement de l'Atelier SIMFIA

L'atelier SIMFIA s'est imposé naturellement dans cette démarche d'intégration de la connaissance de conception des systèmes ainsi que des points de vue associés de Sûreté de Fonctionnement.

Quelques atouts de SIMFIA se sont en effet présentés de la manière suivante:

- L'utilisation du langage ALTARICA a facilité l'interfaçage avec les outils de conception de PSA (Chaîne Outillée de Conception : COC) et la récupération automatique des modèles fonctionnels (Briques et flux) saisis dans la COC.
- La modularité du logiciel SIMFIA a permis de faire évoluer l'outil afin de répondre aux contraintes imposées par la norme ISO 26262 et de s'adapter aux besoins des analystes SDF PSA.

La prise en compte des situations de vie et de la diversité dans SIMFIA s'est également présentée comme un atout substantiel pour son intégration dans le cadre de l'Ingénierie Système. En effet, dans SIMFIA, le paramétrage des situations de vie et de la diversité est effectué lors de la création et de l'édition des phases de mission. Chaque phase de mission correspond à une configuration qui est combinaison d'une ou plusieurs situations de vie ainsi que des options et variantes applicables.

- Situation de vie : pour chaque situation de vie, une entrée extérieure sera crée et sera reliée au bloc environnement. Elle aura comme type la liste des valeurs prises par la situation de vie (exemple : situation manœuvre avec comme états "En manœuvre" et "Hors manœuvre").
- Variante : pour chaque variante, une entrée extérieure sera créée et sera reliée au bloc environnement. Elle aura comme type la liste de valeurs correspondantes (exemple : Boîte de vitesse avec comme états "automatique", "manuelle pilotée" et "manuelle").
- Option : pour chaque option, une entrée extérieure sera créée et sera reliée au bloc environnement. Elle aura comme type la liste de valeurs correspondantes (exemple : Autoradio avec comme états "Avec autoradio" et "Sans autoradio").

Ces entrées extérieures conditionneront les polynômes logiques définis afin de filtrer les éléments non présents dans une configuration donnée et d'inhiber les ER non applicables à la phase de mission. L'état initial de chacune d'entre elles sera défini pour chaque phase de mission.
Cependant, le positionnement de SIMFIA a clairement concerné l'aide à la conception au titre de la Sûreté de Fonctionnement, et en particulier au titre de la Sécurité des systèmes dans le cadre de la norme ISO 26262, comme développé ci-après.
Des modifications ont été apportées à SIMFIA pour produire une étude à un niveau organique en boîte noire, en utilisant la structuration en couche de ces organes. Ces évolutions ont permis aussi la génération automatique de tableaux AMDEC compatibles avec la norme ISO 26262, ainsi que d'arbres de défaillance permettant un calcul des probabilités. La gestion des mécanismes de sécurité mis en évidence par l'application de la norme a également été possible grâce à des évolutions de l'atelier SIMFIA.

2 Contrôle de la sémantique sous SIMFIA: documentation des objets et structuration des points de vue

La lisibilité des modèles dans l'Atelier SIMFIA est importante pour être en mesure par la suite d'interpréter les résultats des évaluations ou analyses effectuées au titre de la norme 26262; c'est pourquoi les données suivantes ont été spécifiées et associées aux différents objets constituant les modèles.

Création de données utilisateurs spécifiques aux modèles PSA

Données associées au flux logiques :

- Objet Physique : C'est l'objet porteur de l'information du flux logique et des caractéristiques techniques (exemples : pour un flux logique électrique: signal électrique, pour un flux MUX : nom de la trame, pour un flux d'éclairage: faisceau lumineux…),
- Vue physique: Caractéristique vérifiable sur l'objet physique (exemples : pour un signal électrique : U, I, etc., pour un flux MUX : signal dans la trame, pour un flux lumineux: intensité, directionnalité, ouverture, etc.),
- Type de liaison: Type liaisons normalisées dans le guide AMDEC (exemples : Fil : TOR+, MUX : CAN I/S, Mécanique, EM : Optique, Interne: DDIV etc.),

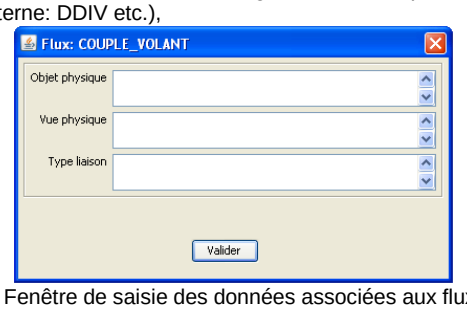

Figure 3 : Fenêtre de saisie des données associées aux flux logiques

Données associées aux modes de défaillance logiques

- Modes de Défaillance (MdD) physiques : Mode de défaillance des objets physiques sur leur vue physique,
- Causes FCC: Causes faisceaux connectiques normalisées en fonction du type de support. Ces causes permettent d'allouer des exigences de SdF au FCC (exemples : CO, CCM, CC+12V, CC+5V, CC+200V, CEM, Variation d'impédance…),
- Autres causes: causes organiques ou agression pouvant générer le mode de défaillance. Elles permettent d'orienter des tests par injection de faute,
- Type de défaillance: Typage des défaillances pour le calcul des métriques de l'ISO 26262 – 5 [4][4]. Les types sont "SPF, MPF-DP, MPF-L et SF",
- Exigence qualitative: Niveau ASIL hérité de l'ASIL natif ou décomposé à partir du niveau ASIL en se fondant sur les mécanismes de sécurité,

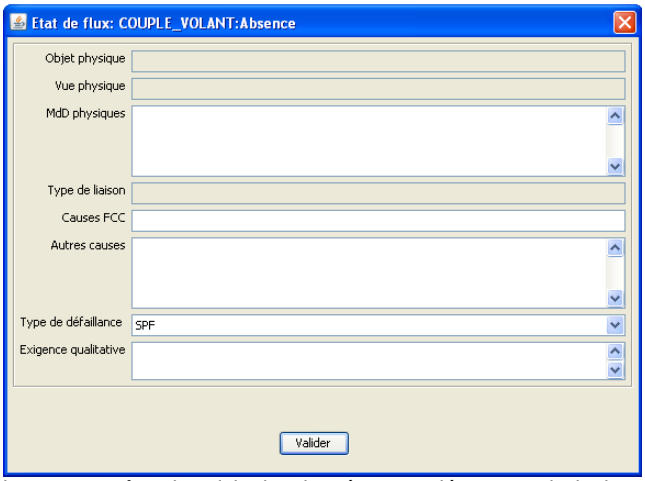

Figure 4 : Fenêtre de saisie des données associées aux MdD logiques

Remarques : Les données saisies sur les flux logiques sont rappelées dans cette fenêtre à titre informatif afin de faciliter la saisie des données sur les modes de défaillance logiques.

3 Génération automatique des tableaux AMDEC sous SIMFIA, dans le cadre de la norme 26262

L'AMDEC est un support essentiel à la mise en oeuvre de la norme 26262; sa génération automatique est assurée par l'atelier SIMFIA et a été customisée pour pouvoir répondre au plus près de ses exigences

Génération automatique de l'AMDEC

Le Format AMDEC utilisé par les analystes SDF chez PSA [3] est un format non standard créé pour répondre au mieux aux attendus de l'ISO 26262. Par conséquent une AMDEC spécifique a été programmée dans SIMFIA pour répondre à leur besoin :

- Récupération des données utilisateur : Une colonne AMDEC a été associée à chaque donnée utilisateur décrite ci-dessus.
- Modification de la propagation : L'AMDEC classique existante ne propageait que les pannes simples. La mise en place des mécanismes de sécurité était traduite dans SIMFIA par une porte "et" entre le mode de défaillance logique concerné et la défaillance du mécanisme de sécurité en place. Par conséquent dans la ligne AMDEC concernant ce mode de défaillance logique, la colonne ER était vide. Afin de se rapprocher de l'AMDEC pratiquée chez PSA, les modifications suivantes ont été apportées :
  - Lors de la pré-propagation, marquer toutes les portes "et" associées aux situations de vie ou à la diversité
  - Lors de la propagation de chaque mode de défaillance logique, les portes "et" non marquées ont été assimilées à des portes "ou". Ce qui permet d'associer à chaque mode de défaillance l'ER qu'il aurait entraîné en l'absence ou défaillance du mécanisme de sécurité
  - Lors de la propagation, SIMFIA récupérera pour chaque mode de défaillance logique les mécanismes de sécurité associés. Ces mécanismes ont été saisis sous forme de champs utilisateur associés aux états de flux de sortie de la couche protocole (condition : l'état de flux de sortie sur lequel le mécanisme est saisi doit appartenir au moins à l'un des chemins de propagation du mode de défaillance logique)
  - La saisie des données utilisateur "Type de défaillance" et "Exigence qualitative" nécessitent d'avoir une vue globale des ER entraînés par le mode de défaillance concerné ainsi que des mécanismes de sécurité qui lui sont associés. Une option a été rajoutée pour paramétrer l'ordre d'affichage des colonnes de l'AMDEC et autoriser la saisie interactive des données "Type de défaillance" et "Exigence qualitative" dans le tableau AMDEC puis de les réinjecter dans le modèle
  - Possibilité de générer une AMDEC multi-phases
  - Possibilité de paramétrer la granularité des origines des propagations (AMDEC au niveau organe (BSI, HDC, …), AMDEC au niveau intermédiaire (couche physique, couche protocole, …) et AMDEC au niveau élémentaire (Alim-Masse, Filaire, …)

Génération automatique des arbres de défaillance sous SIMFIA, dans le cadre de la norme 26262

Cette génération des arbres de défaillance se fait à partir des événements redoutés associés aux effets finaux des dernières colonnes de l'AMDEC; c'est pourquoi il est nécessaire de gérer ces événements redoutés de manière nette et précise.

Chaque modèle SIMFIA contient un bloc nommé "Environnement". Il permet de modéliser :

- L'environnement physique : milieux extérieurs,
- Les aspects inter-systèmes : autres systèmes véhicules,
- La diversité : variantes possibles du système,
- Les événements redoutés : combinaison d'un effet système avec une situation de vie.

L'événement redouté est représenté par une sortie du bloc environnement. Il est combinaison de l'effet système (entrée du bloc environnement), des différentes situations de vie et de la diversité. Des données utilisateur ont été associées à chaque ER :

- Réf ER : Référence de l'événement redouté,
- Réf ST : Référence de l'objectif de sécurité portant l'ER,
- Libellé ER : Description normalisée de l'événement redouté telle que reprise de la spécification,
- Gravité ER : Gravité associée à l'ER dans l'objectif de sécurité,
- Niveau ER : Contient à minima le niveau ASIL pour les ER fonctionnels de gravité 4,
- Objectif ER : Probabilité cumulée - $F(t_{ref})$ – telle que spécifiée dans l'objectif de sécurité,
- Durée de Référence : donnée de t_{ref}.

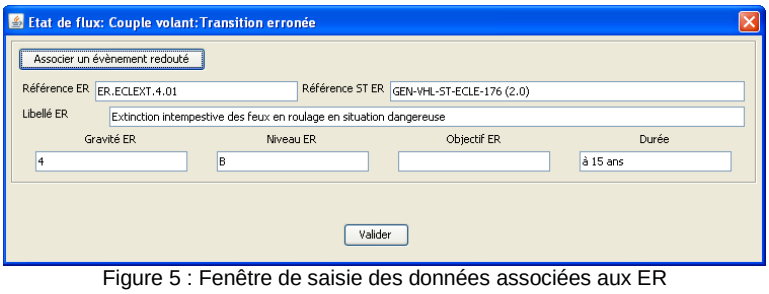

Figure 5 : Fenêtre de saisie des données associées aux ER

Aide à la détermination des mécanismes sous SIMFIA, dans le cadre de la norme 26262

Les mécanismes de sécurité sont un moyen essentiel d'améliorer le niveau de sécurité vérifié par un système, et la norme 26262 permet de structurer l'approche adoptée pour identifier le bien fondé de ces mécanismes et en justifier le financement et la mise en œuvre. Dans SIMFIA, ces sécurisations se voient associés deux vues :

- Ils sont modélisés dans la couche protocole (cf. le paragraphe correspondant).
- Des données utilisateurs ont été ajoutées à SIMFIA pour structurer leur spécification.

Modèles en niveaux d'abstraction

1 Présentation générale

Le cadre ISR de représentation en boîte noir s'exprime sous forme de niveaux d'abstraction articulés suivant le schéma suivant [2].

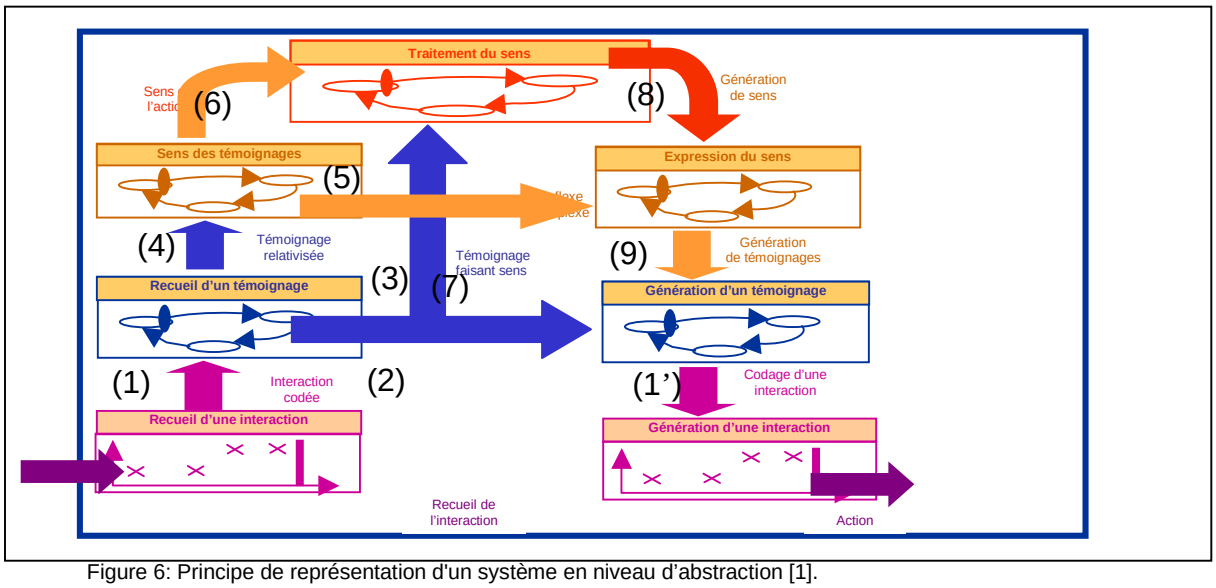

Figure 6: Principe de représentation d'un système en niveau d'abstraction [1].

Dans la Figure 6~~Figure 6~~ chaque information capturée (1) ou délivrée (1') par l'organe doit être transcrite en ou depuis un format compréhensible par l'organe (recueil d'une interaction) avant de pouvoir fournir un « témoignage » de l'interaction. Ce témoignage peut donner lieu par acte reflexe (2) à une nouvelle interaction en sortie de l'organe (exemple : passerelle trame) ou être traité par l'applicatif (3). Plusieurs témoignages de même nature (redondance temporelle) ou de nature différente (redondance spatiale) peuvent être croisés (4) dans un témoignage complexe qui à son tour peut être traité par l'applicatif (6) ou générer un témoignage (5) (exemple : passerelle sécurisée). Le niveau applicatif construit le sens et transforme l'information. Elle peut être traitée par un niveau de témoignage complexe (8) afin d'être sécurisée, par un niveau de témoignage simple (7).

Cette structuration en niveau d'abstraction ne constitue en rien une sous-structure à l'organe. En effet, c'est le même flux logique en entrée de l'organe qui est transmis jusqu'à la couche qui l'utilise soit pour générer un flux de sortie (couche

applicative), soit pour sécuriser un autre flux (couche de protocole). Les différentes couches ont pour certaines d'entre elles (couche physique et couche applicative) une sous-structure normalisée. Outre l'optimisation du traitement de la complexité entre polynômes et blocs, cette structure organique permet de standardiser tant la construction des modèles que leur lecture et leur exploitation. Des modifications ont été apportées à SIMFIA pour produire une étude à un niveau organique en se basant sur la décomposition en couche de ces derniers. De même les sécurisations autrefois décrites dans des colonnes de l'AMDEC sont à présent rattachées à la couche de protocole mais les champs liés (description, taux de couverture, exigences amont), sont rattachés sur le flux sécurisé dans la couche de protocole.

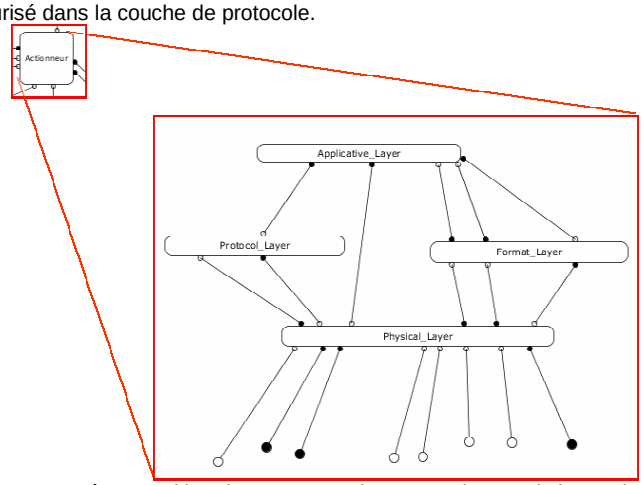

Figure 7: Décomposition d'un organe suivant ses niveaux d'abstractions.

La modélisation SIMFIA suivra ce principe afin de gérer la complexité et éviter de représenter sur un organe un grand nombre de polynômes logiques sans classification. Cette approche permet une grande homogénéité des différents aspects des modèles, des modèles entre eux et une lisibilité directe facilitant la portabilité et la maintenance.

2 Couche Physique

La Couche physique (Niveau codage dans [1], , [2] et sur la Figure 6~~Figure 6~~) permet de représenter l'encodage des interactions électriques, mécaniques, optiques. En particulier dans un contexte de SdF, la couche physique produit les défaillances faisant perdre toute capacité de l'organe de communiquer avec son environnement :

- Défaillances mécaniques,
- Défaillances des alimentations,
- Défaillances des entrées filaires,
- Perte des réseaux multiplexées,
- Endormissement intempestif des réseaux multiplexés.

Pour aider dans la modélisation, la couche physique est couramment décomposée en plusieurs briques élémentaires :

- Une couche physique mécanique,
- Une couche physique filaire,
- Une couche physique multiplexée,
- D'autres ci besoins : électromagnétique, chimique, …

Ces briques élémentaires permettent de classer les types de média des informations

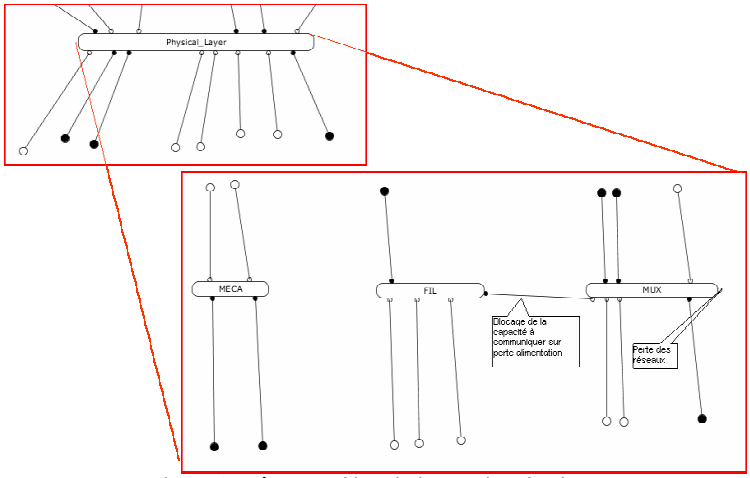

Figure 8: Décomposition de la couche physique

Dans le cas des informations multiplexées, la couche physique permet de prendre en compte l'influence de la perte ou de l'endormissement des réseaux sur la perte des flux associés. Pour ce faire un état réseau est ajouté à la couche physique (Figure 8~~Figure 8~~). Dans le même ordre d'idée, la couche physique filaire inclut, outre les entrées sorties de commandes, les alimentations et masses. La perte de ces entrées de puissance conduit à un blocage des capacités de communication de l'organe (Figure 8~~Figure 8~~).

3 Couche de mise en forme

La Couche de mise en forme (Niveau Témoignage dans [1], [2] et sur la Figure 6~~Figure 6~~) permet de rendre compte de l'arrivée simultanée de plusieurs interactions. Elle permet typiquement la représentation des trames MUX et permet ainsi de caractériser cette unité d'information et ses défaillances.

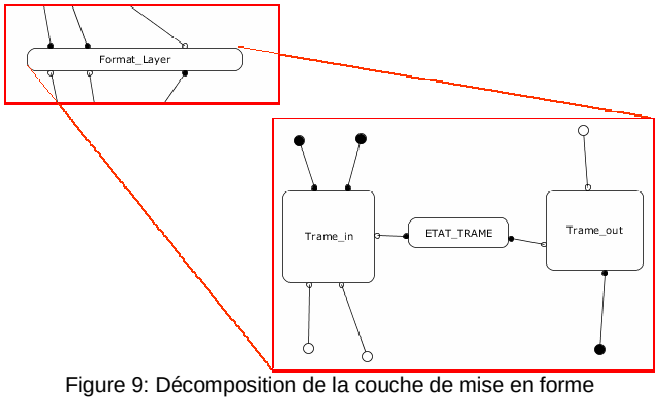

Figure 9: Décomposition de la couche de mise en forme

C'est en particulier dans cette couche que l'on trouvera les modes de défaillance de perte de trame sans perte réseau (ETAT_TRAME sur la Figure 9~~Figure 9~~). Si le nombre de trames acquise ou émise par l'organe la couche de mise en forme pourra inclure un bloc par trame et autant d'état de perte de trame.

4 Couche de protocole

La Couche de protocole (Niveau Description dans [1], [2]) permet de rendre en compte des corrélations faites entre différentes interactions. Cette couche est fondamentale à l'étude SdF, elle contient en particulier les mécanismes de sécurisation. Les flux inter systèmes de sécurisation (flux logiques produits dans la vue courante par un autre système partageant une ressource commune avec la vue courante) sont pris en compte directement à ce niveau sans passer par les couches basses.

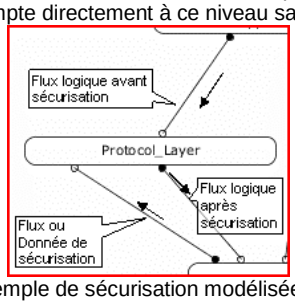

Figure 10 : Exemple de sécurisation modélisée dans SIMFIA

Les « Flux logique avant sécurisation » et « Flux logique après sécurisation» en entrée et en sortie de la couche de protocole sont identiques (par exemple un flux VERROUILLAGE constitué par la couche applicative sur la base des flux d'entrées). Par contre certains de ses modes de défaillances voient leur propagation endiguée par le mécanisme utilisant « Flux ou Donnée de Sécurisation » par exemple un flux INFO_SECU_FILAIRE. En effet, avant la mise en place du mécanisme de sécurité, le mode de défaillance entraînait l'effet système en panne simple. Après la sécurisation du flux VERROUILLAGE ce mode de défaillance n'entraîne l'effet système qu'en panne double, ce qui améliore la sécurisation du système.

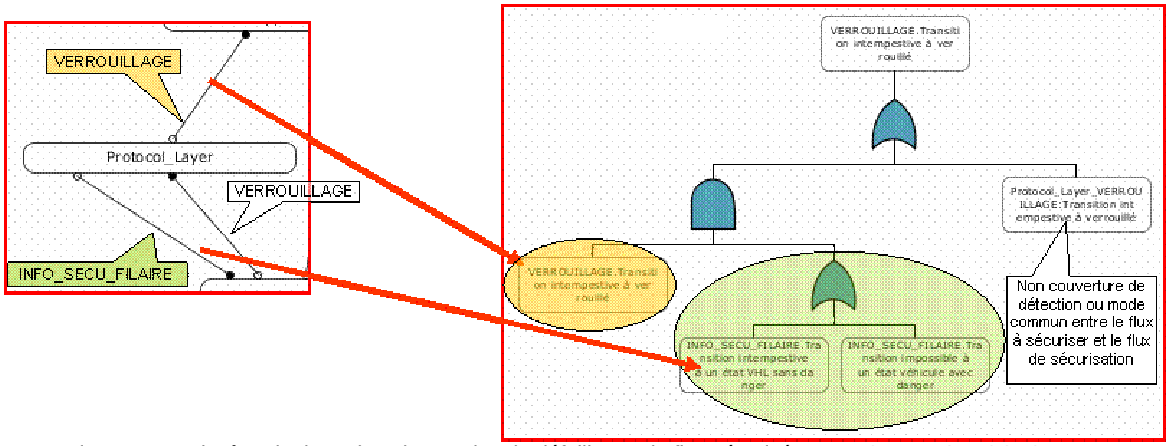

Figure 11 : Polynôme logique d'un des modes de défaillance du flux sécurisé "VERROUILLAGE_COLONNE".

5 Couche applicative

La couche applicative permet de représenter la construction des flux de sortie à partir des flux d'entrés. C'est la couche de construction de sens, qui reste donc la plus complexe du point de vue de ces polynômes logiques. Sa construction demande une analyse fine de la conception. À la différence des polynômes des autres couches qui ajoutent la contribution de certains modes de défaillances aux modes de défaillance d'un flux principal identique en entrée et en sortie de la couche, les polynômes de la couche applicative sont construits entre des modes de type différents en sorties et en entrée de la couche. Il est cependant important de noter que toute la complexité associée aux autres couches en a été extraite.
La plupart des flux inter-systèmes applicatifs peuvent être pris en compte par l'organe directement à ce niveau sans être prétraités par les couches plus basses. Les paramètres de diversité et les calibrations sont intégrés à cette couche.

Exigences de Sûreté de Fonctionnement

Trois types d'exigences de SdF sont utilisés au niveau conception :

- Des exigences fonctionnelles de sécurisations spécifiant le comportement du système en cas de défaillance,
- Des exigences de performances de SdF spécifiant les objectifs qualitatifs et quantitatifs à tenir par les modes de défaillance des organes,
- Des exigences de contraintes de conception spécifiant certains choix de conception contraints par la SdF tel que le choix d'un type d'interface filaire en fonction de l'impact des circuits ouverts ou court circuit à la masse.

Le modèle SIMFIA réalisé est configuré pour pouvoir générer les exigences de performances et les exigences de sécurisation. Il permet actuellement de prendre en compte les contraintes de conception.

1 Intégration des exigences de sécurisation

Les exigences de sécurisations sont intégrées dans des données utilisateurs attachées au mode de défaillance couvert par le mécanisme en sortie de la couche de prototocole. Les champs renseignés pour structurer cette exigence sont :

- Numéro de Sécurisation: C'est le repérage de la sécurisation "SECU_nom fonction_nom organe_numéro",
- Exigences DC : Liste des exigences de conception associées à la sécurisation. Ce champ permet d'assurer la traçabilité avec la conception comme demandée par l'ISO 26262 - 8[4][4],
- Organe : Acronyme de l'organe,
- Principe: description libre de la sécurisation,
- Pré-conditions : listes des conditions nécessaires et suffisantes au déclenchement de la sécurisation,
- Événement déclencheur : événement provoquant le déclenchement de la sécurisation. Il s'agit soit d'une défaillance, soit d'une erreur d'usage,
- État sûr (mode refuge) : valeur du flux de sortie forcé par la sécurisation,
- Postconditions : Conditions de sorties du mode refuge,
- Temps de mise en sécurité: temps de mise en place de la sécurisation,
- Couverture : pourcentage des défauts couverts par le mécanisme. Il s'agit de la couverture de test dans le cas d'une surveillance ou de la couverture des défauts par une redondance.

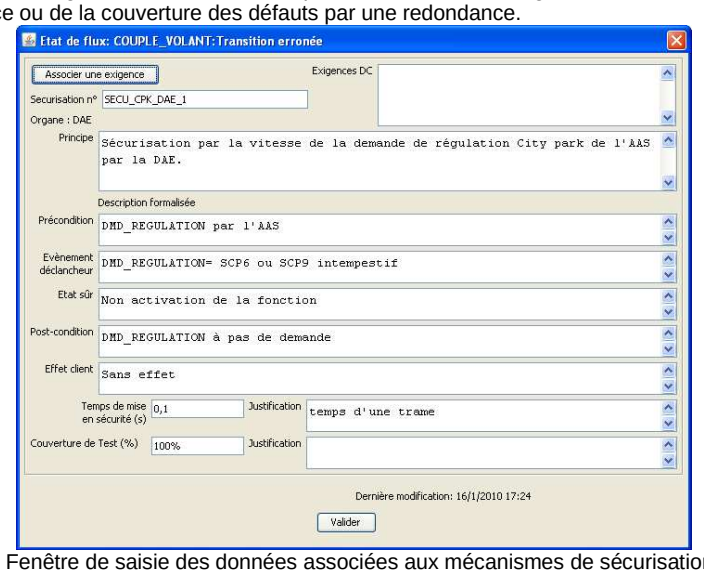

Figure 12 : Fenêtre de saisie des données associées aux mécanismes de sécurisation

2 Génération des exigences de performances

Les exigences de performances sont issues de l'étude SdF. Elles consistent à attribuer pour chaque mode de défaillance participant à des Événements Redoutés de sécurité ou de disponibilité

- des objectifs quantitatifs exprimés en probabilités et pour les événements sécuritaires en métrique,
- pour les événements sécuritaires, des exigences qualitatives sur le niveau ASIL hérité ou décomposé sur le mode.

Ces exigences sont gérées directement par le métier SdF et leur traçabilité avec les objectifs de sécurité amont est intégrée directement dans l'étude SdF. Afin de pouvoir gérer les évolutions des exigences (numéro d'exigence, version), l'AMDEC SIMFIA est exportée vers le format AMDEC PSA qui, outillé, permet de gérer les exigences.

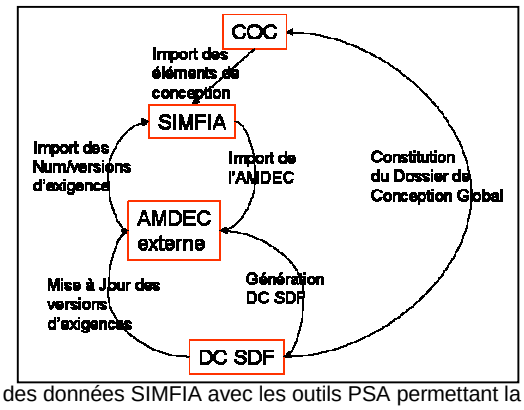

Figure 13 : Couplage des données SIMFIA avec les outils PSA permettant la gestion des exigences

Différences avec ISR, Retour d'expérience et perspectives

Comme précisé à plusieurs reprises l'approche développée ici emprunte plusieurs notions à ISR. Elle ne peut néanmoins pas en supporter tous les aspects et n'est pas directement raccordable à MCR (Méthode de Conceptualisation Relativisée – voir [1]).
Par exemple la logique de composition des briques dans SIMFIA (et dans ALTARICA) interdit de superposer des points de vues relatifs. L'approche proposée reste donc « mono point de vue ». L'environnement qui regroupe les milieux extérieurs physiques, les autres systèmes véhicules, les situations de vies (aspects temporels), ainsi que les ER, n'a pas la richesse du modèle de contexte ISR qui intègre entre autre les aspects sous-jacents situés hors du périmètre de conception.
Malgré les différences importantes avec ISR, l'approche proposée et en particulier la structuration des modèles, permet de gérer efficacement la complexité et d'y intégrer facilement les aspects dysfonctionnels. En effet, cette présentation de démarche d'automatisation partielle pour la génération de modèles dédiés à la Sûreté de Fonctionnement à partir d'un référentiel de conception, met une nouvelle fois en avant l'importance de la structuration des contenus à produire, ainsi que la maîtrise sémantique des objets les constituant.

Ce procédé permet aussi de pouvoir réaliser une étude au plus proche de la conception qui demeure fondée sur une approche fonctionnelle. Le couplage de SIMFIA avec les outils de conception offre la possibilité de faire évoluer l'étude de sûreté de fonctionnement en fonction de l'avancement de l'étude fonctionnelle. Pour cela, le premier niveau (décomposition en organe) fait apparaître tous les flux inter-organes et inter-systèmes. Le niveau deux (les différentes couches composant un organe) permet de faire apparaître tous les flux consommés et produits par un composant du système sans préjuger d'une solution technique. Le niveau trois (éléments de base de couche) permet de traduire la solution technique déterminée pour le système.
La répétition de modes de défaillance d'éléments (exemple : défaillance d'un connecteur) prouve qu'une automatisation de tâches peut être faite, ce qui allège fortement le travail à réaliser pour l'étude.
Appliquée à une centaine d'organes et à plusieurs dizaines de fonctions véhicules traitées par une dizaine d'analyste SdF, il est attendu que cette standardisation permette également une lisibilité et une portabilité accrues des modèles. D'autres critères qualité seront favorisés par ce processus d'ingénierie de modèles : évolutivité, « réutilisabilité », structuration, accessibilité du contenu, configurabilité, « calculabilité » (aptitude à être soumis à des traitements de différentes natures), plus grande facilité de caractérisation, de capitalisation et d'archivage…

1 Remerciements

Les auteurs tiennent à remercier les équipes SdF PSA qui s'investissent dans la démarche et la font progresser.

2 Références

[1] H. Boulouet, V. Brindejonc, M. Mugur-Schächter, Analyse de risques dans le cadre d'une Ingénierie Système Relativisée - Lambda Mu 16,
[2] V. Brindejonc, H. Boulouet, Une approche des signaux faibles- Lambda Mu 16,
[3] V. Brindejonc, G. Marcuccilli, S. Petit, Démarche AMDEC système dans le cadre de l'ISO 26262- Lambda Mu 17,*
[4] ISO DIS 26262 Road vehicles — Functional safety
Part 1: Vocabulary
Part 2: Management of functional safety
Part 3: Concept phase
Part 4: Product development: system level
Part 5: Product development: hardware level
Part 6: Product development: software level
Part 7: Production and operation
Part 8: Supporting processes
Part 9: ASIL-oriented and safety-oriented analyses
Part 10: Guideline on ISO 26262