Influence des fautes transitoires et des performances temps réel sur la sûreté des systèmes X-by-Wire

Cédric Wilwert

Département de formation doctorale en informatique

Institut National
Polytechnique de Lorraine

École doctorale IAEM Lorraine

Influence des fautes transitoires et des performances temps réel sur la sûreté des systèmes X-by-Wire

THÈSE

présentée et soutenue publiquement le 24 Mars 2005

pour l'obtention du

Doctorat de l'Institut National Polytechnique de Lorraine

(spécialité informatique)

par

Cédric Wilwert

Composition du jury

Président :	M. Yvon Trinquet
Rapporteurs :	M. Jean Arlat
	M. José Alberto G. Fonseca
Examinateurs :	Mme Marie-Claude Portmann
	Mme Françoise Simonot-Lion
	M. YeQiong Song
Invité :	M. Jean-Louis Dufour

Laboratoire Lorrain de Recherche en Informatique et ses Applications — UMR 7503

Mis en page avec la classe thloria.

Remerciements

Je remercie tout d'abord Françoise Simonot-Lion, qui a encadré ces travaux avec enthousiasme et bienveillance, et qui a, de part sa rigueur et son expérience, largement contribué à leur aboutissement. Je remercie aussi particulièrement YeQiong Song, qui a su cadrer et aiguiller efficacement les recherches menées au cours de ces trois années. Sans eux, ces travaux ne seraient pas ce qu'ils sont et mon avenir ne serait pas ce qu'il est.

Je remercie Yvon Trinquet d'avoir accepté de présider mon Jury, et Jean Arlat et José Alberto G. Fonseca de m'avoir fait l'honneur d'être rapporteurs de ces travaux de thèse. Je remercie aussi Marie-Claude Portmann d'avoir accepté d'être examinatrice de ces travaux.

Je remercie Jean-Louis Dufour (mon nouveau mentor en sûreté de fonctionnement) d'avoir encouragé ces travaux et participé au jury de thèse. Je remercie tout particulièrement Anne Charlois, qui a accepté d'encadrer cette thèse avec un point de vue d'industriel particulièrement avisé et formateur. Je remercie aussi Pierre Bouilleux pour m'avoir fait confiance, et m'avoir engagé dans son service, et Alain Gilberg pour avoir initié ces travaux.

Je tiens aussi à exprimer mes sincères remerciements à Nicolas Navet pour la qualité technique de ses conseils et pour la qualité humaine de nos échanges. De même, je remercie François Simonot pour sa très sympathique participation aux travaux et Olivier Zendra pour avoir accepté de m'aider à la mise en page du manuscrit.

Mes remerciements vont aussi à Eric Rondeau, Thierry Divoux et Fabien Michaut, qui m'ont donné la fibre de la recherche et m'ont encouragé à me lancer dans ces travaux de thèse.

Bien sûr, je remercie aussi toute l'équipe TRIO, et notamment Mohamed pour sa générosité et la richesse de nos entretiens, Ricardo, Mathieu, Xavier et Raul pour leur sympathie, Giancarlo pour sa persévérance, Orazzio et Gerardo pour le soleil, Manu pour son engagement, Michel, Philippe, Jian, Jean-Pierre, Josette, Laurence, Fabrice, Ning, Li Ping... et tous les autres.

Enfin, merci à tous les branks, et merci à mademoiselle, aussi douée en réconfort qu'en compilation LaTeX.

Table des matières

Introduction

Depuis quelques dizaines d'années, une part importante des systèmes mécaniques d'une automobile ont été assistés ou remplacés par des systèmes électroniques. Le remplacement intégral des organes de freinage et de direction par des systèmes "tout-électrique/électronique/informatique" - les systèmes X-by-Wire - pose cependant des problèmes nouveaux. Outre les questions liées au coût, à la standardisation (voir paragraphe 1.6.2), à la disponibilité de la technologie et à l'alimentation, ce sont les problèmes relatifs à la sûreté de fonctionnement qui sont de réelles sources d'interrogation pour les constructeurs d'automobiles, mais aussi - et surtout - pour les consommateurs (voir paragraphe 1.5). En effet, ces systèmes sont dépourvus des redondances mécaniques qui permettent d'assurer la maîtrise du véhicule en cas de dysfonctionnement des composants électroniques ou logiciels.

En parallèle, le monde de l'aéronautique a déjà opté depuis plusieurs années pour l'introduction des systèmes by-wire - les systèmes Fly-by-Wire - pour des fonctions tout aussi critiques que le sont la direction et le freinage pour le monde de l'automobile, et la sûreté de fonctionnement de leur flotte n'en a pas pour autant été entâchée. Cependant, les contraintes de place, de coût, de maintenance et de formation de utilisateurs ne sont pas comparables.

Les systèmes X-by-Wire étant à l'étude depuis la fin des années 90, la majeure partie des problèmes énoncés précédemment sont aujourd'hui résolus, ou partiellement résolus :

- la standardisation : comme détaillé au paragraphe 1.6.2, certaines normes disponibles aujourd'hui semblent être adaptées à la conception de systèmes X-by-Wire, de plus, il s'agit d'un des objectifs avérés de certains consortiums comme le FlexRay Consortium [1] ou Autosar [2].
- la disponibilité de la technologie : la présentation par des grandes sociétés (constructeurs et équipementiers) de prototypes roulants (voir [46] et [47]), indique que les équipementiers sont aujourd'hui en mesure de concevoir et fournir ce type de systèmes,
- l'alimentation : le problème de l'alimentation est crucial. Si l'implantation de systèmes type Brake-by-Wire ou Steer-by-Wire sur des véhicules de petite taille (segment A) est possible avec un batterie 14 Volts, ce n'est pas le cas pour les véhicules des segments B et C. Or, comme la majorité des systèmes innovants, les premiers Steer-by-Wire (système de direction by-wire sans redondance mécanique) et le Brake-by-Wire (système de freinage by-wire sans redondance mécanique) de série seront destinés aux véhicules les plus onéreux, soit aux véhicules du segment C. C'est pourquoi la mise en série de ces systèmes est directement tributaire de la maturité de la technlogie 42 Volts. Cependant, le virage vers les véhicules tout électrique semble se rapprocher à grands pas, et si le 42V pouvait être une étape vers une technologie telle que la pile à combustible, cette étape pourrait aussi être trop onéreuse par rapport à sa durée de vie. Il a ainsi été clairement exprimé au SAE (Society of Automotive Engineers) [101], en 2003, que cette technologie ne serait pas mature avant 2010 et que son avenir était incertain. Cette annonce a considérablement estompé l'engoue-

[1] http ://www.flexray-group.com
[2] http ://www.autosar.org

ment pour l'implantation à court terme des systèmes Steer-by-Wire et Brake-by-Wire [7]. Cependant, très récemment, Kelm [61] a insisté à la conférence Convergence sur le fait que cet argument était plus économique que technique, et que le pessimisme actuel était au moins aussi exagéré que l'emphase généralisée des constructeurs au début des années 2000.

– le coût : comme expliqué précédemment, les premiers systèmes Steer-by-Wire et le Brake-by-Wire de série seront destinés aux véhicules haut de gamme. En effet, le besoin en sûreté de fonctionnement imposera certainement des redondances diversifiées - physiques et logicielles - particulièrement onéreuses. Cependant, dans l'éventualité d'un accueil positif du public, une production en masse de ces systèmes en diminuerait considérablement le coût.

Ainsi, si l'on fait abstraction des problèmes énoncés précédemment, il est possible de résumer le problème de l'introduction des systèmes X-by-Wire dans des véhicules commercialisés en série par la question suivante : comment concevoir des systèmes Brake-by-Wire et Steer-by-Wire au moins aussi fiables que les systèmes de freinage et de direction embarqués aujourd'hui, sans augmenter le coût de la fonction[3] ?

La criticité des fonctions visées et l'architecture même d'un véhicule automobile font des systèmes X-by-Wire des systèmes distribués temps réel, la communication entre les différents sites étant organisée sur un réseau qui se doit de respecter les contraintes temps réel imposées par la fonction. Ces caractéristiques rendent les systèmes X-by-Wire particulièrement complexes. C'est pourquoi l'étude de la sûreté de fonctionnement de ces derniers requiert un champ de compétences qui va de l'automatique à l'informatique, en passant par l'ingénierie des réseaux, la mécanique et naturellement l'ingenierie de la sûreté de fonctionnement. Or, que ce soit au sein des services des constructeurs d'automobiles ou dans les laboratoires de recherche, il est relativement rare de trouver un pôle de compétences capable de traiter l'ensemble des problèmes propres aux compétences citées. Cependant, le monde de la recherche montre aujourd'hui un réel engouement pour ces problèmes qualifiés de "multidisciplinaires". Les travaux réalisés dernièrement LAAS de Toulouse, au Royal Institute of Technology de Stockholm ou encore au LORIA de Nancy en sont les meilleurs exemples. C'est donc tout naturellement que la société PSA Peugeot Citroën a décidé de se tourner vers la recherche universitaire pour obtenir des éléments de réponses sur la problématique de l'étude de la sûreté de fonctionnement des systèmes X-by-Wire.

1 La sûreté de fonctionnement des systèmes X-by-Wire : périmètre des travaux

Dans le contexte de l'évaluation de la sûreté de fonctionnement des systèmes X-by-Wire, nous avons décidé de focaliser nos travaux sur la prévision quantitative de fautes. En effet, la seule préconisation quantitative avancée aujourd'hui est une exigence exprimée en terme de probabilité d'occurrence de défaillances catastrophiques par heure de fonctionnement - nous appelerons cette grandeur *sûreté* dans la suite du document -. Comme précisé précédemment, la sûreté de fonctionnement sera dans un avenir proche soumise à une réglementation. Pour l'instant, malgré quelques recommandations issues de projets d'étude (Brite Euram 111, Palbus) (voir paragraphe 1.6.1), seules des préconisations internes aux entreprises sont ciblées. Nous nous attacherons dans ce document à vérifier que la sûreté d'un système donné est garantie si la probabilité d'occurrence de défaillances critiques au niveau véhicule est inférieure à 5.10^{-10} ; 5.10^{-10} est la quantification avancée, mais ramenée à l'heure de fonctionnement,

[3] Exemples de *fonctions* dans notre contexte : braquage des roues selon une requête conducteur, fourniture d'effort au volant cohérent avec l'environnement véhicule, freinage réparti cohérent avec l'effort pédale, ...

dans les conclusions du projet Brite Euram 111.

Les techniques de prévision de fautes axées sur l'étude de l'architecture matérielle et les fautes permanentes dues au vieillissement des composants sont aujourd'hui parfaitement maîtrisées et appliquées chez tous les constructeurs d'automobiles (voir chapitre 2). En outre, les systèmes X-by-Wire sont des systèmes temps réel stricts, avec des contraintes sur les temps de réponse de bout-en-bout de l'ordre de quelques dizaines de millisecondes. Ces systèmes étant particulièrement sensibles aux perturbations, et notamment aux perturbations d'ordre électromagnétique, chaque faute transitoire peut devenir la cause d'une défaillance catastrophique. Or, si l'on considère que l'erreur causée par une faute transitoire se caractérise par la perte d'un ou plusieurs échantillons consécutifs du même signal, il est indispensable de connaître les performances temps réel du système pour analyser son comportement entre la transmission du dernière échantillon valide et l'occurrence de l'erreur, ou entre la fin de l'occurrence de l'erreur et la transmission du prochain échantillon valide (d'où le besoin "multidisciplinaire" énoncé au paragraphe précédent).

Nous proposons dans ce document un résultat d'ordre méthodologique dont l'objectif principal est d'*évaluer quantitativement l'influence des fautes transitoires et des performance temps réel sur la sûreté des systèmes X-by-Wire*.

Pour ceci, nous avons introduit un attribut de la sûreté que nous avons désigné sous le terme de *Fiabilité Comportementale* et qui est définie comme l'*aptitude du système à assurer un service en prenant en compte la dynamique de l'application embarquée (performances temporelles, tolérances aux défaillances)*. Nous avons également associé à cet attribut des *métriques* permettant de l'évaluer.

2 Approche méthodologique proposée dans la thèse

Il est important de noter qu'une de nos hypothèses de départ est que l'architecture fonctionnelle et logicielle est validée à priori : nous faisons l'hypothèse que l'influence des fautes transitoires liées à des défauts de conception (fautes intermittentes) est négligeable par rapport à celle des fautes transitoires liées à l'environnement.

Avant d'étudier le comportement d'un système aussi réactif qu'un système X-by-Wire soumis à des perturbations, il est indispensable de maîtriser son comportement en mode nominal (non-perturbé). Nous proposons donc en premier lieu une méthode d'analyse d'une architecture opérationnelle prenant en compte la distribution de l'architecture logicielle, les performances du matériel, et les politiques d'accès aux ressources en mode nominal (sans perturbation). Dans un deuxième temps, nous introduisons une méthode de prévision quantitative de fautes en mode perturbé, dont l'objectif est de mesurer l'influence des fautes transitoires liées à l'environnement et des performances temps réel du système sur la sûreté (probabilité d'occurrence de défaillances). Chacune de ces évaluations, mode nominal et mode perturbé, repose sur des mesures de l'influence d'une architecture du système et de l'environnement de celui-ci sur des critères de qualité mesurés au niveau du véhicule et définis par l'industriel partenaire de cette thèse. Enfin, pour des raisons contextuelles propres aux séjours effectués au sein de la société PSA Peugeot Citroën, nos travaux ont été appliqués sur les systèmes de direction Steer-by-Wire, mais les méthodes d'évaluation proposées sont génériques.

Les apports de cette thèse sont d'ordre méthodologique :

– la première contribution concerne le mode nominal. A l'aide d'un modèle Matlab-Simulink du système et de son environnement véhicule (voir Annexe A), nous observons l'influence du retard, dit "pur", dû aux performances de l'architecture informatique support et aux politiques d'accès aux ressources, en particulier aux protocoles de communication (intervalle de temps entre la production d'un échantillon de la consigne

conducteur et la consommation de cet échantillon, supposé non altéré, par les lois de commande au niveau des actionneurs) sur les critères de qualité cités ci-dessus. Comme il n'est pas possible d'exhiber une forme analytique exprimant les critères en fonction de ce délai, le "pire retard pur tolérable" tel que les critères sont acceptables est obtenu par simulations successives. Nous étudions alors analytiquement l'architecture opérationnelle du système pour évaluer quel est le retard calculé dans le pire cas.

– la deuxième contribution porte sur l'évaluation du système en mode perturbé. Dans ce cas, grâce au même modèle Matlab-Simulink auquel un générateur d'erreurs a été ajouté, nous observons l'influence de plusieurs erreurs consécutives, correspondant à la perte d'un nombre paramétrable d'échantillons du même signal, sur les critères de qualités cités précédemment. Nous obtenons alors l'intervalle maximal tolérable entre l'arrivée de deux instances valides du même signal, les instances intermédiaires étant perdues en raison de perturbations. L'exigence de sûreté est vérifiée à partir d'un modèle d'erreur (probabilité d'occurrence des perturbations, de leurs durées et des erreurs associées), construit à partir de statistiques réelles sur l'environnement électromagnétique du réseau routier français, sur lequel nous projetons l'intervalle de temps, évoqué ci-dessus, mesuré sous Matlab/Simulink. Nous obtenons alors des mesures pour évaluer la *Fiabilité Comportementale*.

3 Plan du document

Le document se décompose en trois parties. La première est consacrée au contexte universitaire et industriel de nos travaux (chapitre 1), et à l'état de l'art relatif aux différentes méthodes disponibles pour la prévision de fautes (chapitre 2), ainsi que les contributions de la thèse. La deuxième partie décrit l'ensemble des méthodes proposées dans ce document. Plus précisément, le chapitre 3 est consacré aux critères de qualité de service des systèmes de direction chez PSA Peugeot Citroën, le chapitre 4 à l'analyse du système en mode nominal et le chapitre 5 à l'analyse du système en mode perturbé. Dans la troisième partie, au chapitre 6, les méthodes d'évaluation proposées sont appliquées à une étude de cas, à savoir une architecture opérationnelle Steer-by-Wire réaliste dont le protocole de communication est de type TDMA (Time Division Multiple Access), et qui peut être soumise à des perturbations d'ordre électromagnétique telles que rencontrées dans des trajets de référence d'un véhicule. La technique fournissant des résultats quantitatifs, plusieurs études de sensibilité sont réalisées, comme, par exemple, l'influence de la durée du cycle de communication sur un protocole de communication de type TDMA (Time Division Multiple Access), l'influence de la diversification dans la redondance des sous-systèmes, ou l'influence de mécanismes de détection d'erreurs proposés par les protocoles de communication TTP/C et FlexRay. La cohérence des résultats obtenus dans cette étude de cas et le souci de réalisme qui accompagne chacune des quantifications et des hypothèses démontrent l'intérêt de la méthodologie proposée dans l'optique d'une commercialisation en série de véhicules équipés de systèmes X-by-Wire.

Partie 1

Chapitre 1

Contexte

A l'heure actuelle, les acteurs du secteur automobile ne sont soumis à aucune réglementation nationale ou internationale pour la justification de la sûreté de fonctionnement des architectures électroniques / informatiques embarquées dans leur véhicule. La plupart du temps, ce sont les constructeurs qui émettent leurs propres exigences, puis les imposent à leurs fournisseurs. Il est par conséquent indispensable pour eux de disposer de méthodes pour la vérification du respect de ces exigences. Le chapitre 2 "état de l'art" du présent document est consacré à la présentation de ces méthodes et de leurs limites. Notons qu'en l'absence de réglementation, les contraintes principales se posent en termes de coût et de taille des architectures. Néanmoins, un faible niveau de fiabilité ou de disponibilité peut rapidement devenir un critère discriminant pour la marque et un faible niveau de sécurité-inocuité augmente la probabilité de défaillances catastrophiques. C'est pourquoi les exigences fixées par les constructeurs atteignent généralement des niveaux élevés. Ces exigences sont fonction des niveaux de gravité des défaillances probables identifées. Par ailleurs, le retour expérience est le meilleur atout de l'ingénieur en sûreté de fonctionnement. Il lui permet notamment de vérifier que les exigences de sûreté de fonctionnement sont bien tenues et lui permet de disposer de statistiques pour l'évaluation des taux de défaillances des composants. Le cas des systèmes qui ne disposent d'aucun retour d'expérience - et c'est le cas des systèmes X-by-Wire (section 1.1) - pose par conséquent des problèmes complexes pour la quantification des exigences et la vérification du respect de ces dernières, que ce soit en mode nominal (non perturbé) (section 1.2) ou en mode perturbé (section 1.3). L'expérience acquise ces dernières années avec l'implantation des systèmes électroniques dans les véhicules de type automobile permet, au moins, de maîtriser correctement les entraves à la sûreté de fonctionnement de ces systèmes (section 1.4), même si le risque perçu peut être différent de celui perçu pour des systèmes plus "classiques" (section 1.5). Plusieurs études et autres projets ont déjà proposé certaines exigences à respecter pour l'implantation en série des systèmes de freinage et de direction sans redondance mécanique et la construction d'architectures opérationnelles X-by-Wire (section 1.6). Après avoir exposé ces caractéristiques propres au contexte dans lequel nos travaux ont été réalisés, nous présenterons alors le périmètre des travaux présentés, et plus particulièrement les exigences sur lesquelles nous avons décidé d'axer nos réflexions (section 1.7).

1.1 Systèmes X-by-Wire

1.1.1 Pourquoi les systèmes X-by-Wire ?

Le tendance qui voit les systèmes mécaniques et hydrauliques embarqués remplacés par des systèmes électroniques n'est pas nouvelle, et, malgré certaines réticences de la part des consommateurs [14], celle-ci ne semble pas prête de s'estomper. Les raisons de cette évolution sont à la fois technologiques et économiques. En effet, les composants électroniques disponibles aujourd'hui, du moins ceux ciblant les systèmes embarqués dans les transports, sont de plus en plus fiables et de moins en moins chers. De plus, l'introduction de l'électronique offre des possibilités de prestations qu'aucun système mécanique et/ou hydraulique serait capable de fournir (par exemple, la direction assistée ou la répartition électronique de freinage).

Le terme "X-by-Wire" est utilisé pour décrire les systèmes destinés à remplacer intégralement les systèmes mécaniques / hydrauliques. Si ces technologies sont particulièrement discutées depuis quelques années [52, 70], les concepteurs de systèmes électroniques embarqués n'en sont pourtant pas à leur coup d'essai. En effet, historiquement, la première fonction X-by-Wire critique fut le "Throttle-by-Wire" (accélérateur électronique), implanté dans la série Chevrolet Corvette en 1980 pour remplacer le câble d'accélérateur. Cette fonction est aujourd'hui disponible sur une grande majorité des véhicules. La fonction "Shift-by-Wire" ou "Gear-by-Wire" (automatisation du passage de vitesse) est aussi disponible sur des véhicules tels que les BMW séries 5 et 7. Par ailleurs, beaucoup des systèmes mécaniques / hydrauliques embarqués sont aujourd'hui assistés par la technologie électronique. C'est le cas des systèmes de freinages électroniques / hydrauliques, des suspensions semi-actives comme l' "Adaptative Damfpung System" de Mercedes, l' "Electronic Camshaft" du BMW Valvetronic, ou encore de la boîte de vitesse robotisée proposée aujourd'hui par une majorité de constructeurs.

Cependant, le remplacement des systèmes de direction et de freinage mécaniques / hydrauliques par des technologies intégralement électroniques n'a aujourd'hui été adopté par aucun constructeur. Si la faisabilité technologique de ce type de systèmes n'est plus à prouver [33], l'un des obstacles principaux à la mise en série de ces systèmes est de démontrer que toutes les exigences de sécurité sont respectées. En outre, ces systèmes étant aujourd'hui encore relativement onéreux, le client doit percevoir une différence de prestation notable pour accepter un prix plus élevé.

Notons de plus que l'implantation de systèmes type "Brake-by-Wire" ou "Steer-by-Wire" sur des véhicules de petite taille (segment A) est possible avec un batterie 14 Volts, ce n'est pas le cas pour les véhicules des segments B et C. Or, comme la majorité des systèmes innovants, les premiers "Steer-by-Wire" et le "Brake-by-Wire" de série seront destinés aux véhicules les plus onéreux, soit aux véhicules du segment C. C'est pourquoi la mise en série de ces systèmes est directement tributaire de la maturité de la technlogie 42 Volts.

1.1.2 "Steer-by-Wire" et "Brake-by-Wire"

La notion de système "X-by-Wire" est aujourd'hui essentiellement utilisée pour décrire les systèmes "Steer-by-Wire" et "Brake-by-Wire", systèmes non disponibles à l'heure actuelle sur des véhicules de série (voir paragraphe précédent). Nous consacrons nos travaux, et en particulier cette section, à l'étude de ces derniers.

1.1.2.1 'Steer-by-Wire"

Le premier avantage d'un système "Steer-by-Wire" est la suppression de la colonne de direction. Du point de vue de la sécurité du conducteur, cette alternative permet une diminution considérable des risques en cas de choc, l'entrée de la colonne de direction à l'intérieur de l'habitacle étant souvent synonyme de graves blessures pour le conducteur. De plus, la disparition de cet organe particulièrement lourd et encombrant entraîne une réduction de

la consommation de carburant de 6% [70], ce qui représenterait un progrès non négligeable du point de vue de la protection de l'environnement.

En terme de prestation, la nouveauté majeure qu'offre le "Steer-by-Wire" est la démultiplication variable. Cette fonction permet d'adapter le ratio de braquage entre le volant et les roues en fonction de la situation de vie du véhicule. Par exemple, dans des situations telles que le parking ou la conduite en ville (vitesse véhicule faible), le ratio pourra être augmenté pour réduire la rotation et l'effort nécessaire au volant. Cette fonction est déjà présente sur les BMW série 5 équipées de direction dite "active".

1.1.2.2 "Brake-by-Wire"

L'implantation d'un système "Brake-by-Wire" avec un micro-contrôleur et un actionneur sur chaque roue permet de réduire la distance d'arrêt et d'adapter la pression de la force de freinage au conducteur, ce qui augmente considérablement la qualité du freinage. Comme pour les systèmes "Steer-by-Wire", la suppression du liquide de freinage réduira le poids du véhicule et donc sa consommation, mais c'est aussi le problème du recyclage de ces fluides particulièrement polluants qui sera définitivement réglé.

Un dérivé des systèmes "Brake-by-Wire", l'EHB (Electro Hydraulic Braking), est aujourd'hui produit en série. La différence majeure entre un EHB et un système de freinage classique est l'indépendance de la pression hydraulique sur chaque roue. Cependant, contrairement à un système "Brake-by-Wire" intégralement électrique, le circuit hydraulique classique est toujours présent. Le premier EHB de série a été implanté sur la Mercedes Roadster SL en 2001. Aujourd'hui, Toyota propose un "Regenerative EHB" sur sa Prius, qui utilise l'énergie dissipée lors de la décélération pour recharger la batterie.

1.2 Mode nominal : le respect des contraintes temps réel

Si l'essentiel de nos travaux porte sur la prévision de fautes en mode perturbé, la validation d'une architecture "X-by-Wire" passe aussi par sa validation en mode nominal. Or les systèmes "X-by-Wire" sont des systèmes à contraintes temps réel strictes, c'est à dire que le délai entre la consommation d'une donnée et sa production est borné, et qu'un dépassement de la borne maximale est susceptible d'entraîner une défaillance catastrophique - évènement redouté de gravité maximale (voir paragraphe 1.3.2) -. Ainsi, si un système n'est pas validé a priori du point de vue de ses contraintes temps réel, l'occurrence d'une défaillance catastrophique est probable sans que la moindre faute (voir paragraphe 1.3.1 pour la définition du terme faute) affecte le système.

1.3 Mode perturbé : généralités sur la sûreté de fonctionnement et application au domaine de l'automobile

Selon Laprie ([71] et [9]), les différents moyens pour mettre en oeuvre une politique de sûreté de fonctionnement sont la *prévention des fautes*, *la tolérance aux fautes*, *l'élimination des fautes* et *la prévision des fautes*. Les définitions des ces derniers termes sont les suivantes :

- *prévention de fautes* : comment empêcher l'occurrence ou l'introduction de fautes,
- *tolérance aux fautes* : comment fournir un service à même de remplir la fonction du système en dépit des fautes,
- *élimination de fautes* : comment réduire la présence (nombre, sévérité) des fautes,
- *prévision des fautes* : comment estimer la présence, la création et les conséquences des fautes.

L'objectif de nos travaux est d'évaluer la probabilité d'occurrences de défaillance, ils relèvent donc de la prévision des fautes : on quantifie la présence, la création et les conséquences des fautes. Laprie parle dans ce cas d'évaluation probabiliste ou d'évaluation quantitative ([71] et [9]).

1.3.1 Chaîne faute-erreur-défaillance

Pour comprendre la notion de fautes utilisée au paragraphe précédent, mais aussi celles d'erreurs et de défaillances, Laprie a donné les définitions suivantes ([71], mises à jour dans [9]) :

Défaillance :

- évènement survenant lorsque le service délivré dévie de l'accomplissement de la fonction du système.
- transition de service correct vers service incorrect.

Erreur :

- partie ou état du système qui est susceptible d'entraîner une défaillance.
- manifestation d'une faute dans un système.

Faute :

- cause adjugée ou supposée d'une erreur.
- cause d'erreur évitée ou tolérée.
- conséquence de la défaillance d'un composant pour le système qui le contient ou pour le, ou les composants, qui interagissent avec lui.

Cette terminologie peut être parfois difficile à manipuler pour des systèmes complexes embarqués dans des environnements hétérogènes. De plus, la chaîne faute-erreur-défaillance étant recursive, une défaillance d'un sous-système peut être la cause d'une erreur pour le système. Il existe cependant plusieurs techniques pour qualifier chacune des composantes en phase de conception :

- on arrête la recursivité aux fautes que l'on désire tolérer,
- une erreur ne peut pas être dormante, elle doit être détectable par le système,
- le service cité dans la définition de la défaillance doit correspondre au service tel que perçu par le conducteur.

Les fautes dont les occurrences peuvent provoquer des erreurs au sein des systèmes étudiés dans ce document seront énoncées au paragraphe 1.4. Nous préciserons dans cette même section le type de fautes sur lequel nous avons décidé de focaliser notre étude. Le chapitre 5 qualifiera clairement chacune des composantes de la chaîne faute-erreur-défaillance pour un système de type "Steer-by-Wire".

1.3.2 Niveaux de gravité des évènements redoutés dans le domaine de l'automobile

Certaines fautes peuvent éventuellement être tolérées. Dans le cas contraire, elles peuvent conduire à des défaillances qui, pour l'ingénieur en sûreté de fonctionnement, deviennent des évènements redoutés dont il faut prévoir les conséquences - et notamment leurs gravités - et la probabilité d'occurrence.

Toute évaluation quantitative de la Sûreté de Fonctionnement d'un système doit être précédée d'une Analyse Préliminaire des Risques (APR). L'APR permet de qualifier les événements redoutés (ER) en fonction des conséquences de leurs occurrences. On associe ainsi un niveau de gravité - ou niveau de criticité - à chaque ER. Dans le monde de l'automobile, 4 niveaux de gravité sont communément utilisés. Une gravité de niveau 4 est associée aux évènements relatifs à la sûreté (ex : défaillance définitive de l'ensemble du système de freinage en roulage) et

une gravité de niveau 3 est associée aux événements relatifs à la disponibilité du véhicule (ex : défaillance d'un ou plusieurs composants remontée au conducteur afin qu'il stoppe le véhicule dans les plus brefs délais). Les événements de gravités 1 et 2 sont relatifs à la fiabilité des composants [79]. On appelle ainsi *système critique* un système dont les défaillances sont susceptibles de mettre en danger les occupants du véhicule. Par exemple, les systèmes participant au confort des passagers ne sont pas des systèmes critiques.

1.3.3 Notion de sûreté

Les notions de risque et de confidentialité sont généralement associés à la notion de sécurité. Ce qui peut poser certains problème quand le thème est évoqué. La définition de la fiabilité est donnée quant à elle par la Commission Electronique Internationale (CEI) est la suivante : "aptitude d'un dispositif à accomplir une fonction requise, dans des conditions données, pendant une période donnée" [23]. Villemeur ajoute que, "au sens mathématique, la fiabilité est généralement caractérisée ou mesurée par la probabilité que l'entité accomplisse une ou plusieurs fonctions requises dans des conditions données pendant une durée donnée" [117]. Laprie [71], estime quant à lui que la fiabilité est la "mesure de la délivrance continue d'un service correct, ou, de façon équivalente, du temps jusqu'à défaillance", mais il insiste sur le fait que la "sécurité-inocuité" peut être assimilée à une mesure du temps jusqu'à défaillance catastrophique. La notion de sécurité étant fréquemment associée à celle de confidentialité, nous utiliserons le terme de "sûreté" pour qualifier la "sécurité-inocuité" - d'où le titre du document -. En conséquence, *l'objectif de nos travaux est de quantifier la sûreté d'un système X-by-Wire donné.*

1.4 Entraves à la sûreté de fonctionnement des systèmes X-by-Wire

Comme précisé précédemment, il est primordial de savoir quelles fautes le système doit tolérer. Sachant que nous focalisons notre étude sur les fautes accidentelles, le retour d'expérience chez PSA Peugeot Citroën et des documents tels que [121], [63] ou encore [122] nous ont permis de dresser une liste exhaustive des fautes susceptibles de provoquer des défaillances des sous-systèmes (et donc des erreurs pour le système X-by-Wire).

1.4.1 Classification des différentes classes de fautes selon leur cause

- *fautes de conception* : la complexité des méthodes de conception et la multiplication des composants logiciels peuvent générer une multitude de fautes de conception si aucune vérification rigoureuse n'est appliquée.
- *fautes de production* : elles sont essentiellement dues au processus de fabrication et à la qualité des matériaux employés.
- *fautes d'interaction* dues à l'homme : elles sont aujourd'hui extrêmement importantes. En effet, contrairement au monde de l'aéronautique, l'utilisateur du système n'est pas régulièrement formé pour l'appréhender, d'où un nombre considérable d'erreurs humaines. Ces fautes d'interactions peuvent aussi être causées par une mauvaise manipulation d'un réparateur.
- *fautes d'interaction* dues à l'environnement : cette classe représente la majeure partie des fautes transitoires (voir paragraphe suivant).

1.4.2 Classification des différentes classes de fautes selon leur durée

- *fautes permanentes* : ce sont les fautes dites "traditionnelles". Elles sont essentiellement anticpées par la connaissance de la durée de vie des composants. Les problèmes de température peuvent aussi entraîner des

fautes permanentes.

– *fautes intermittentes* : elles ont une durée limitée, et les causes peuvent être internes (ex : faute de conception) et indépendantes de l'environnement.
– *fautes transitoires* : elles ont une durée limitée, et leurs causes sont strictement dépendantes de l'environnement. Le meilleur exemple de faute transitoire est la perturbation électromagnétique (voir paragraphe 5.1.2).

Comme expliqué en introduction, nous faisons l'hypothèse dans cette étude que l'architecture fonctionnelle et logicielle est validée à priori, et qu'aucune faute de conception ni de production ne peut apparaître. *Nos travaux ciblent l'influence sur le système des fautes transitoires d'interactions dues à l'environnement.*

1.5 Quantification de la sûreté et risque perçu

La notion de risque est depuis quelques années au coeur des grands débats, qu'ils soient sociaux, politiques ou environnementaux [33]. Les campagnes récentes dans le domaine de la santé publique sont un excellent exemple pour illustrer l'évolution de l'intérêt croissant du domaine du risque (voir les campagnes anti-tabac et l'augmentation sans précédent de la prévention et de la répression en matière de sécurité routière). Cette focalisation grandissante peut avoir un impact non-négligeable sur les exigences en terme de sûreté de fonctionnement des systèmes à haut niveau de criticité embarqués dans l'automobile.

1.5.1 Gestion des risques

[117] nous donne la définition suivante du risque : "mesure d'un danger associant une mesure de l'occurrence et une mesure de ses effets ou conséquences". Cette vision très "objective" du risque ne correspond pas forcément au risque perçu par les individus. Si les objectifs de sûreté de fonctionnement doivent être tenus essentiellement pour des raisons d'assurance et de respect des normes, la perception par les clients et les médias de la fiabilité ou de la disponibilité du système peut être tout autre, et avoir un coût conséquent.

Les travaux de Starr [107] ont montré que l'acceptation du risque par la société et les individus est essentiellement influencée par le caractère volontaire ou involontaire du risque encouru. On parle d'un risque à caractère volontaire lorsque l'individu décide librement d'y être confronté (tabagisme, sports extrêmes, ...). On parle, par contre, d'un risque à caractère involontaire lorsque le choix et le contrôle de celui-ci semblent échapper à l'individu concerné.

1.5.2 Conduite de véhicule équipé de systèmes "X-by-Wire" : risque volontaire ou involontaire ?

[33] classe les risques d'accident automobile dans les risques volontaires. En effet, si l'individu est tout à fait conscient qu'en prenant son véhicule il court un risque, il sait aussi qu'il a une certaine emprise sur ce dernier. Starr indique que le public acceptera un risque avec une probabilité d'occurrence de l'événement redouté 1000 fois supérieure s'il est volontaire [107]. On peut donc se poser la question suivante : le risque - tel que perçu par un individu ou un groupe d'individus - associé à la conduite du véhicule équipé de systèmes "X-by-Wire" est-il volontaire ou involontaire ? Plusieurs paramètres tendent à prouver que ce risque sera perçu comme involontaire :

– dans le cas des systèmes de direction ou de freinage "by-wire", la moindre défaillance du système peut entraîner la perte de contrôle du véhicule.

– les véhicules équipés d'un grand nombre de systèmes électroniques sont aujourd'hui perçus comme moins fiables que leurs prédécesseurs plus "mécaniques" [116]. Certains médias [14] désignent directement le multiplexage comme principal responsable d'une éventuelle diminution de la fiabilité des véhicules. Plus récemment, la médiatisation du blocage d'un régulateur de vitesse à 190km/h (hypothèse soumise à vérification) a accentué et relancé le débat sur la fiabilité de ces systèmes [28].

S'il est conscient de ces 2 paramètres, l'individu aura le sentiment d'avoir beaucoup moins d'emprise sur le risque d'accident et le risque pourra effectivement être perçu comme involontaire.

1.5.3 Quantification du risque perçu

La probabilité de décès lors d'un trajet en véhicule à moteur est statistiquement estimé à $24/100000$ par an [33]. Par ailleurs, 3% des accidents d'automobiles sont causés par des défauts de conception [93]. Ainsi, le risque de décès causé par un défaut de conception est proche de $7,2 \times 10^{-6}$/an. Or, une étude de Otway et Erdmann sur le risque perçu lors de l'implantation d'une centrale nucléaire (risque involontaire) indique qu'à 10^{-6}/an, les risques n'inquiètent pas les individus, à 10^{-5}/an, le risque est identifié, et au dessus il n'est pas toléré [87]. Il y a par conséquent fort à parier que le public surestime encore le risque de mortalité lors d'un trajet en véhicule à moteur. Mais jusqu'à quand et jusqu'à quel seuil ? La frilosité du public envers les compagnies aériennes à bas coût après l'incident de Charm El-Cheikh montre qu'un seul événement peut décupler le risque perçu. Ainsi, pour minimiser l'impact d'un événement indésirable, il est indispensable de pouvoir prouver que le risque d'accident grave Rp provoqué par une mauvaise conception du système est au maximum de Rp = 10^{-6}/an.

Le taux de défaillance précéonisé pour l'aéronautique est de 10^{-9} par heure [118] [48] et peut varier entre 10^{-9} et 10^{-12} pour le ferroviaire [2] [1]. Si, par exemple, le taux de défaillance préconisé pour les véhicules λ est de 10^{-7} par heure, et si l'on considère que, sur une année, ce taux de défaillance est constant, pour 8760 heures dans une année, on peut donner la formule de fiabilité R(t) du système (voir paragraphe 2.1.3.1) :

$R(t) = e^{-\lambda \times t}$

Si l'on considère que $t = 1\ heure$:

R_{heure}= $e^{-\lambda \times 1}$

On considère qu'il y a 8760 heures dans une année, ainsi, on peut écrire :

R_{an}= $e^{-\lambda \times 8760}$

Ainsi, si l'on recherche le Mean Time To Failure $MTTF'$ du système et le taux de défaillance λ' du système par an, on peut écrire, toujours d'après le paragraphe 2.1.3.1 :

$R_{an} = e^{-\frac{1}{MTTF'}}$

et

$MTTF' = -\frac{1}{\lambda}\left[e^{-\lambda t}\right]_0^{8760}$

$MTTF' = -\frac{1}{\lambda}\left[e^{-\lambda.8760} - 1\right]$

or

$MTTF' = \frac{1}{\lambda'}$

Soit :

$\lambda' = -\frac{\lambda}{e^{-\lambda.8760}-1} = 9,99 \times 10^{-8}$

Le taux de défaillance par an des systèmes est donc de $9,99 \times 10^{-8}$.

La proportion des accidents mortels par rapport à l'ensemble des accidents corporels était de 6% en 2003 [104]. Si l'on fait l'hypothèse (pire cas) que chaque défaillance critique du système entraîne un accident corporel, le risque réel Rr de mortalité par an sera de :

$Rr = 9,99 \times 10^{-8} \times 6/100$

$Rr = 1,67 \times 10^{-10}$ par an.

On remarque que $Rr < 10^{-6}$ par an. Par conséquent, la quantification du taux de défaillance par heure définie pour le concorde, si elle est respectée, est suffisante pour ne pas inquiéter le public.

Si ce petit calcul permet d'avoir une idée de la quantification du risque perçu selon des statistiques récentes, certains chiffres ont déjà été avancé quant aux objectifs de sûreté que les systèmes X-by-Wire doivent atteindre.

1.6 Evaluation quantitative de la sûreté : contexte de réglementation

1.6.1 Préconisations

Les premières statistiques recensant le nombre des pannes ont vu le jour avec le développement du transport aérien. On se basait alors sur ces chiffres pour déterminer les améliorations possibles et les objectifs à se fixer. Pugsley fut le premier à quantifier des objectifs. En effet, dans ses rapports publiés en 1939 et 1940 par l'Aeronautical Research Council de Londres, il demanda que le taux d'accident d'un avion - en considérant toutes les causes de pannes susceptibles d'entraîner un accident - ne dépasse pas 10^{-5} par heure de fonctionnement, dont 10^{-7}/ heure pour les causes liées à la structure de l'avion [117]. En France, le projet Concorde, projet fondateur pour la formalisation des études de Sûreté de Fonctionnement des systèmes électroniques / informatiques, a vu naître une des premières préconisations quant à la probabilité d'apparition d'un événement redouté au niveau véhicule. Cette préconisation était que le taux d'accident d'un avion - en considérant toutes les causes de pannes susceptibles d'entraîner un accident - ne puisse dépasser 10^{-7}/ heure. C'est cette exigence qui est appliquée aux véhicules dans le monde de l'automobile.

Les ingénieurs de sûreté de fonctionnement qui analysent les systèmes embarqués dans l'automobile font l'hypothèse suivante : l'ensemble des systèmes peut être la source de 100 événements redoutés *indépendants* de gravité 4. En d'autres termes, il existe potentiellement 100 défaillances critiques différentes de systèmes embarqués qui peuvent être la cause de l'occurrence d'un événement redouté de gravité 4 au niveau véhicule (voir figure 1.1).

En utilisant l'hypothèse d'indépendance des événements redoutés de gravité 4 au niveau système, on peut donc dire que la probabilité P d'occurrence d'un événement redouté de gravité 4 au niveau véhicule est la somme des probabilités P_i d'occurrences d'événements redoutés Er_i de gravité 4 au niveau des systèmes ($P = \sum_i P_i$). Ainsi, si la probabilité d'occurrence d'un événement redouté de gravité 4 visée au niveau d'un système est de 10^{-9} alors la probabilité d'occurrence d'un événement redouté de gravité 4 au niveau véhicule visée sera de 100×10^{-9}, soit 10^{-7}. Notons que l'usage dans le domaine automobile considère que une exigence de 10^{-9}par heure au niveau des systèmes assurera une exigence de 10^{-7} par heure au niveau du véhicule. Cette exigence sur les systèmes est encore aujourd'hui celle préconisée dans l'avionique, et c'est aussi celle communément utilisée dans le cadre de la sûreté des systèmes "X-by-Wire" [79, 45].

1.6.1.1 Conclusions du projet Brite Euram 111

L'objectif principal du projet "X-by-Wire, Safety Related Fault Tolerant Systems in Vehicle" [15], terminé en novembre 1998, était de définir un cadre de travail pour les futurs concepteurs de systèmes "X-by-Wire" :

- spécification et conception d'une architecture de référence,
- construction d'un démonstrateur,
- analyse de la sûreté de fonctionnement de l'architecture,

– recommandations pour le processus de conception et règles à respecter pour la certification.

Si chacun de ces points a été étudié en détail, les recommandations qui en découlent souffrent cependant d'un manque de clarté. En effet, certains termes comme "faute" ou "critique" sont avancés sans aucune précision, et les recommandations peuvent alors être interprétées de diverses manières. Nous les citerons tout de même, en essayant de coller au mieux au texte initial (voir rapport final du projet [15]). Ces recommandations de sûreté de fonctionnement peuvent être séparées en 3 parties : les recommandations qualitatives, les recommandations quantitatives et les recommandations de fond données aux ingénieurs. Elles sont indissociables l'une de l'autre mais ne concernent pas forcément les mêmes phases de la conception.

1. Recommandations de fond :
   – utiliser les meilleures pratiques possibles pour la conception des systèmes critiques,
   – prendre toutes les précautions raisonnables,
   – utiliser tout ce qui est raisonnablement faisable pour assurer la sûreté du système.
2. Recommandations qualitatives :
   – les technologies utilisées pour les capteurs et les actionneurs redondés doivent être différentes,
   – une défaillance du système ne doit pas conduire à un état dans lequel les vies humaines, l'économie ou l'environnement sont en danger,
   – en cas de faute critique, le système doit avertir le conducteur,
   – une seule défaillance d'un sous-système ne doit pas entraîner une défaillance du système complet,
   – chaque sous-système doit être lui-même tolérant aux fautes,
   – le système doit être tolérant à toutes les défaillances apparaîssant dans les hypothèses de fautes,
   – le conducteur doit être averti en cas de faute critique,
   – les fautes intermittentes doivent être mémorisées.
3. Recommandations quantitatives :

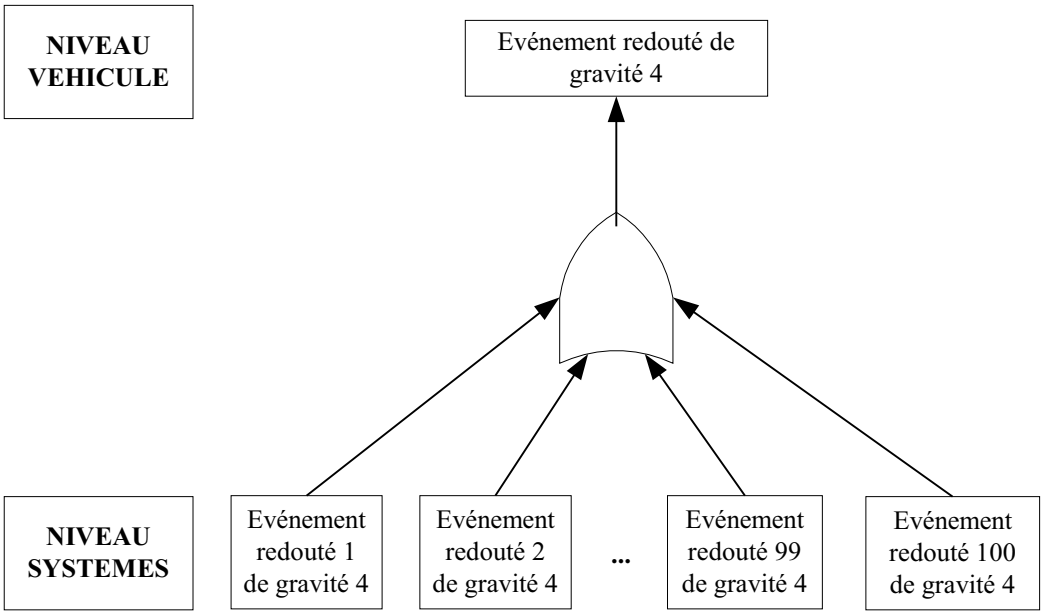

FIG. 1.1 – Evénements redoutés de gravité 4 : du véhicule aux systèmes

- l'exigence majeure avancée dès l'introduction du rapport final est que "le système doit être aussi bon qu'un système mécanique remplissant la même fonction" ; le flou relatif au terme "bon" a été par ailleurs éclairci la même année au SAE (Society of Automotive Engineers) par des ingénieurs de la société Daimler-Chrysler qui ont ajouté que "le système doit être aussi fiable, aussi disponible et aussi maintenable qu'un système mécanique remplissant la même fonction" [46],
- si aucune supposition n'est faite sur le mode de défaillance du noeud, alors une unité tolérante aux fautes (ensemble des calculateurs redondés censés fournir la même fonction) doit être composée de 4 noeuds ; ces 4 noeuds doivent exécuter un protocole d'accord tolérant aux fautes byzantines (pour plus de détails sur la problématiques des fautes byzantines, le lecteur pourra se référer au papier fondateur de Lamport : [69]) pour converger en cas de défaillance d'un des noeuds ; il est précisé par ailleurs dans [29] que, pour une architecture complétement maillée, 2 calculateurs à silence sur défaillance sont suffisants pour former une unité tolérante aux fautes byzantines,
- le système doit être capable de tolérer une faute pendant un temps suffisamment long pour que le conducteur puisse placer le véhicule dans un état sûr,
- la probabilité de rencontrer n'importe quel mode de défaillance critique pour la sécurité du conducteur ne doit pas excéder 5.10^{-10} par heure de fonctionnement. *Si une analyse de sûreté de fonctionnement montre que cette exigence n'est pas respectée, le système ne doit pas être certifié.* Cette exigence est le point d'entrée de nos travaux.

1.6.1.2 Projet PALBUS

Le projet PALBUS, qui a pris fin en avril 2001, avait des objectifs semblables à ceux du projet Brite Euram 111, avec une orientation plus nette vers les méthodologies de conception et d'implémentation de bus de données pour les systèmes distribués à haut niveau de criticité. Des industriels, des instituts de recherche et des universités, tous implantés en Suède, ont coopéré à ce projet. Certaines recommandations intéressantes ont pu être extraites :

- le système doit tolérer un nombre spécifié de fautes arbitraires (ou byzantines, voir [99]), et dans l'éventualité où il doit faire face à ces fautes arbitraires, il doit être en mesure de continuer à fournir le service,
- dans l'éventualité où il doit faire face à un nombre plus important de fautes (spécifié lui aussi), il peut dégrader le service tout en maintenant une certaine qualité de service, elle aussi spécifiée,
- dans le cas de fautes temporaires, le système doit fonctionner avec les anciennes valeurs aussi longtemps que le résultat est satisfaisant.

En outre, le projet discute l'utilisation des normes existantes pour la conception de systèmes X-by-Wire sûrs de fonctionnement, notamment la norme EN 954 [35] qui propose une approche qualitative et la CEI 61508 [24] qui propose une approche plus quantitative (voir paragraphe 1.6.2).

1.6.1.3 Préconisation de sûreté PSA Peugeot Citroën

Lors de la conférence RTS de l'année 2003, G. Mousty, ingénieur sûreté de fonctionnement de la société PSA Peugeot Citroën, a indiqué dans [79] que, pour les systèmes X-by-Wire, "la probabilité d'occurrence d'un événement de gravité 4 ne doit pas excéder 10^{-9} par heure de fonctionnement". Cette préconisation est aussi celle proposée par Hammett au SAE 2002 dans [45].

1.6.2 Normes et standards

Dans la plupart des domaines reconnus comme critiques (par exemple nucléaire, aéronautique, ferroviaire), les systèmes électroniques embarqués obéissent à des réglementations précises autant en ce qui concerne le processus de conception que pour l'évaluation de leur sûreté de fonctionnement. Il n'existe aujourd'hui rien de similaire dans le domaine de l'automobile pour la certification de ces systèmes. Ce problème est néanmoins crucial, et plusieurs propositions sont actuellement à l'étude.

Parmi les standards existants [88], la norme RTC1.6.1 / DO-178B [98] qui est utilisée pour le logiciel dans l'aéronautique, la norme EN 50129 [26], utilisée dans le ferroviaire, et la norme EN 954 [35] utilisée pour la sécurité des machines, fournissent des directives précises pour le développement des systèmes électroniques embarqués qui requièrent un haut niveau de sûreté. Mais ces standards sont difficilement applicables aux systèmes embarqués dans l'automobile, notamment à cause des différences de contraintes (coût, formation du personnel, ...). Néanmoins, la Motor Industry Software Reliability Association (MISRA), un consortium composé des principaux acteurs du secteur automobile en Angleterre, propose un ensemble de directives pour le développement de logiciels destinés à des systèmes à haut niveau de sécurité embarqués dans l'automobile [78].

Une des normes les plus citées dans les études traitant de systèmes X-by-Wire est la CEI 61508 [25]. Cette norme est annoncée comme un bon candidat pour supporter un processus de certification dans l'industrie automobile. En Europe, et en particulier dans le domaine des transports, la tendance est de passer d'une certification basée sur les règles à une certification basée sur les risques [76]. Or, la CEI 61508 définit des niveaux (Safety Integrity Level ou SIL) qui caractérisent une fonction de sécurité en termes de conséquences de sa défaillance définie comme catastrophique, sévère, mineure ou insignifiante (voir tableau 1.1). Il s'agit par conséquent d'évaluer la "probabilité pour qu'un système relatif à la sécurité exécute de manière satisfaisante les fonctions de sécurité requises dans toutes les conditions spécifiées et dans une période de temps spécifiée" [25]. Pour les systèmes correspondant à ceux embarqués dans l'automobile - notamment en terme de fréquence d'utilisation -, la définition des niveaux de sécurité est la suivante : "mesures cibles de défaillance pour une fonction de sécurité, allouée à un système de sécurité fonctionnant en mode de forte sollicitation" [24]. Dans ce contexte, la table 1.1 donne les exigences quantitatives correspondant à chaque niveau (notons que la norme fait apparaitre pour le niveau SIL4 une exigence sur la probabilité de défaillance dangereuse par heure exprimée ainsi : cette probabilité doit être inférieure à 10^{-8} :

Niveau d'intégrité de sécurité	Mode de fonctionnement à forte sollicitation (Probabilité de défaillance dangereuse par heure)
4	$< 10^{-8}$
3	$\geq 10^{-8}$à $< 10^{-7}$
2	$\geq 10^{-7}$à $< 10^{-6}$
1	$\geq 10^{-6}$à $< 10^{-5}$

TAB. 1.1 – Niveaux SIL - norme CEI 61508

Il est communément admis que les systèmes "X-by-Wire" doivent respecter un niveau maximal d'intégrité de sécurité et sont par conséquent estampillés SIL4. Cependant, l'utilisation de cette norme est surtout intuitive, aucun organisme n'ayant à ce jour indiqué qu'elle pouvait s'appliquer aux systèmes "X-by-Wire".

Par ailleurs, le projet européen AUTOSAR[4] qui regroupe la majorité des constructeurs et des équipementiers

[4]http ://www.autosar.org

européens, ainsi que le FlexRay Consortium[5], ont parmi leurs objectifs la normalisation et la standardisation de certaines composantes de ces systèmes, plus particulièrement la conception d'architectures électroniques embarquées et la spécification du protocole de communication. Ces projets pourraient aboutir à des standards dont l'utilisation est censée réduire considérablement la probabilité d'occurrence des fautes de conception, mais la thèse ne traîte pas cet aspect.

1.6.3 Exigences sur les systèmes de communication

En 1993, le "SAE Vehicle Network for Multiplexing and Data Communications Standards Committee" a identifié 3 classes de protocoles de communication pour systèmes embarqués dans l'automobile (SAE A, B et C) et publié une liste d'exigences relatives aux applications critiques de sécurité. Les protocoles de communication pour les systèmes "X-by-Wire" doivent respecter les exigences dites "de sûreté de fonctionnement et de tolérance aux fautes" de la classe C [46] (pour plus de détails, voir [100]) :

1. Régularité du transfert d'information
2. Latence minimale des messages
3. Tolérance aux fautes
4. Robustesse
5. Détection d'erreurs
6. Acquittement et transmission atomique
7. Testabilité
8. Composabilité

Cette liste décline les exigences impondérables que doit respecter le protocole de communication implanté au coeur d'un système "X-by-Wire". Pour plus de détails sur les services à implémenter pour respecter ces exigences, le lecteur pourra se référer à [119].

1.7 Périmètre des travaux

Ce chapitre montre qu'il est indispensable de développer des techniques et des méthodes pour prouver que le système respecte des exigences de sûreté avant d'être implanté dans un véhicule commercialisé en série. Parmi toutes les contraintes énoncées au cours de ce chapitre, nous avons pris la décision de focaliser nos travaux sur une des recommandation du projet BRITE EURAM 111 : "l*a probabilité de rencontrer n'importe quel mode de défaillance critique pour la sécurité du conducteur ne doit pas excéder* 5.10^{-10}*/heure. Si une analyse de sûreté de fonctionnement montre que cette exigence n'est pas respectée, le système ne doit pas être certifié"*. L'objectif principal de cette thèse est de fournir une méthode pour évaluer la sûreté d'un système "X-by-Wire" et donc, d'étudier comment évaluer quantitativement la probabilité d'occurrence de défaillances catastrophiques d'un tel système et comment confronter le résultat avec la contrainte énoncée ci-dessus.

[5] http ://www.flexray-group.com

Chapitre 2

Etat de l'art

A la fin des année 80, A. Villemeur avait synthétisé l'ensemble de méthodes permettant d'analyser la Sûreté de Fonctionnement d'un système dans ce qui est devenu par la suite un ouvrage indispensable pour tout ingénieur ou chercheur travaillant dans le domaine : "Sûreté de Fonctionnement des Systèmes Industriels" [117]. Une petite dizaine d'années plus tard, J-C. Laprie et toute son équipe du LAAS (Laboratory for Analysis and Architecture of Systems) publiait un ouvrage devenu l'ouvrage de référence en Sûreté de Fonctionnement des systèmes électroniques/informatiques : "Guide de la Sûreté de Fonctionnement" [71]. La figure 2.1, extraite de ce dernier, présente les moyens, entraves et attributs de la Sûreté de Fonctionnement. Dans la suite du document, nous nous appuierons sur les concepts et les définitions introduits dans cet ouvrage.

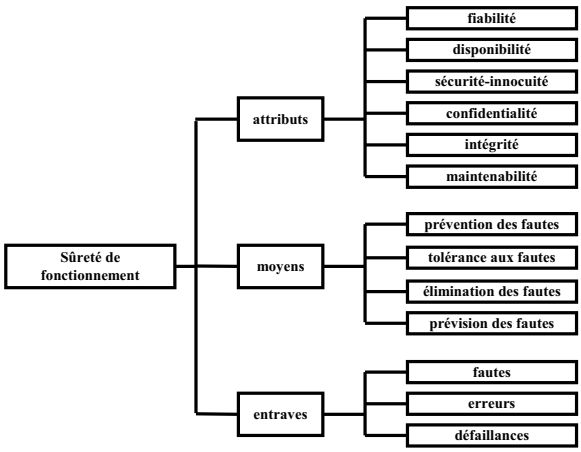

FIG. 2.1 – Les moyens, entraves et attributs de la sûreté de fonctionnement

Si l'on respecte la terminologie de la figure 2.1, nos travaux se situent dans le cadre de la *prévision de fautes*, avec pour objectif la quantification de la *sécurité-innocuité* (appelée *sûreté* dans la suite du document). Certaines techniques sont aujourd'hui devenues des standards en terme de prévision de fautes. Cependant, ces techniques peuvent s'avérer rapidement insuffisantes dans le cadre de l'analyse des systèmes distribués. En effet, pour ces systèmes, la prévision de fautes passe aussi, entre autres, par l'évaluation qualitative et quantitative du ou des protocoles de communication utilisés sur le réseau. Par ailleurs, les automaticiens ont depuis longtemps mis en lumière le problème de l'influence des retards variables sur la stabilité de ces systèmes. L'analyse de la stabilité

(au sens automatique du terme) et du protocole de communication sont donc des techniques de prévision de fautes à part entière.

Ce chapitre décrit les différentes approches utilisées aujourdhui pour la vérification du respect des contraintes de sûreté de fonctionnement par prévision de fautes et les techniques incluant les critères de l'automaticien et /ou l'influence du réseau de communication dans un objectif de vérification du respect des contraintes temps réel. Ainsi, la première section sera consacrée aux techniques de prévisions de fautes standards (section 2.1), statiques et dynamiques. L'influence du réseau sur la sûreté de fonctionnement sera étudiée dans la section 2.2, et les techniques d'évaluation propres aux automaticiens seront évoquées dans la section 2.3.

2.1 Techniques de prévision des fautes standards

Les méthodes d'évaluations quantitatives de prévision des fautes peuvent être divisées en 2 catégories [123] :
- les méthodes dites *statiques* : le système est étudié sans tenir compte de son évolution possible dans le temps.
- les méthodes dites *dynamiques* : le système est étudié en tenant compte de son évolution dans le temps.

2.1.1 Prévision des fautes : les méthodes statiques classiques

Depuis le développement du Concorde, en France, les principales méthodes utilisées pour la prévision de fautes des systèmes critiques sont l'AMDEC et les arbres de défaillances. Leur utilisation est toujours d'actualité pour fournir une partie des résultats nécéssaires lors de l'étude de la sûreté de fonctionnement d'un système.

2.1.1.1 Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC)

Cette méthode, qui fut employée pour la première fois dans les années 1950 dans le domaine militaire, fait aujourd'hui l'unanimité dans toutes les industries à risque (nucléaire, militaire, énergie,...). Depuis 1988, la norme QS9000 [96] impose aux équipementiers automobiles de fournir les AMDEC des systèmes vendus aux constructeurs.

Il s'agit d'une méthode inductive dont l'objectif est de qualifier les causes et les effets des défaillances qui peuvent affecter les composants (ou sous-systèmes) d'un système [117]. La première étape de la méthode est l'identification de tous les modes de défaillance -et de leurs causes- de chaque composant. La seconde étape est basée sur l'étude des effets de ces modes de défaillances. On juge alors la gravité g de chaque événement que l'on peut quantifier à partir des niveaux de gravité (voir paragraphe 1.3.2). Certaines caractéristiques comme la fréquence d'apparition f de la défaillance et sa détectabilité d peuvent aussi apparaître. Il est alors possible de calculer la *criticité* C de la défaillance donnée par la formule :

$C = f \times g \times d$

Cette technique est généralement couplée à celle des Arbres de défaillances pour la recherche des causes des défaillances.

2.1.1.2 Arbre de défaillances

Au même titre que l'AMDEC, l'arbre de défaillances est une méthode classique dans le domaine de la sûreté de fonctionnement. Appelée aussi Arbre des Causes, Arbre des Fautes ou Arbre des Défauts, elle est née en 1962 dans les bureaux de la société Bell Telephone. Il s'agit là d'une technique déductive (on ne cherche plus les effets d'une défaillance mais ses causes) basée sur la recherche des combinaisons d'événements pouvant conduire à une

défaillance. L'arbre est constitué de niveaux successifs d'événements reliés entre eux par des opérateurs logiques. Chaque événement issu d'un opérateur est obtenu par la combinaison des événements d'entrée de cet opérateur. Il est important de noter que contrairement à l'AMDEC, dont l'objectif est avant tout qualitatif, la méthode des arbres de défaillance est fréquemment utilisé pour des évaluations quantitatives. En effet, des probabilités d'apparition (pour une durée donnée) peuvent être associées à des occurrences d'événements, et des opérations sur ces probabilités peuvent être réalisées à partir des opérateurs qui relient les événements entre eux.

L'exploitation d'un arbre de défaillance repose essentiellement sur l'observation des coupes minimales. Une coupe est un ensemble d'événements susceptibles d'entraîner l'événement redouté situé à la racine de l'arbre. Une coupe est dite minimale lorsqu'elle n'en contient aucune autre. Cette approche permet de mettre en lumière les événements critiques qui peuvent causer l'événement redouté, et d'en évaluer la probabilité d'apparition.

Une illustration de l'application de ces méthodes dites statiques classiques à la problématique de la sûreté des systèmes X-by-Wire a été proposée dans [79].

2.1.2 Prévision des fautes : les méthodes dynamiques classiques

Les méthodes statiques présentées précédemment ne sont pas appropriées pour évaluer la fiabilité des systèmes de contrôle-commande fortement dépendant du temps [103]. En effet, les différents formalismes présentés ne proposent aucune solution pour inclure le temps et les performances temps réel de l'application dans l'analyse. Si le remplacement préventif des composants a fait du vieillissement un paramètre moins dimensionnant pour les systèmes embarqués aujourd'hui dans l'automobile que dans le passé, les différentes phases que peut traverser la vie d'un système sont tout de même primordiales pour l'étude de sa sûreté de fonctionnement : la dynamique du système et ses évolutions au cours du temps doivent être pris en compte par la méthode. Pour ce faire, il est indispensable d'utiliser un modèle capable de formaliser le comportement du système et qui peut se modéliser sous la forme d'un graphe analysable.

La modélisation d'un système s'appuie sur une description graphique ou analytique des états et du comportement de ce système. La complexité du système peut amener le concepteur du modèle à ne pas représenter l'intégralité des états possibles du système, mais plutôt des macro-états suffisamment représentatifs pour l'exploitation du modèle. Le graphe d'état-transition est le modèle le plus utilisé pour la prise en compte de la dynamique d'un système dans l'évaluation de sa sûreté de fonctionnement. Parmi ceux-ci, les deux formalismes les plus rencontrés sont les réseaux de Petri stochastiques et les chaînes de Markov.

2.1.2.1 Chaînes de Markov

Le principal atout de l'analyse des systèmes markoviens est qu'elle ne nécéssite pas la connaissance du passé du système. Ainsi, un système est dit markovien si la probabilité de passer d'un état à l'autre est indépendante du passé du système. On parle de chaine de Markov si le processus est discret. Si les taux de transitions sont constants, on parle de processus homogène. Dans une chaîne de Markov, chaque place représente un état du système, et chaque transition la probabilité (pour une certaine durée) de passer d'un état à l'autre. L'étude d'une chaîne de Markov nécéssiste la résolution d'équations différentielles linéaires. De nombreuses méthodes analytiques sont aujourd'hui disponibles pour résoudre ces équations et obtenir des informations telles que la fiabilité, la disponibilité ou la maintenabilité. Un outil tel que Moca RP [6] permet de simuler et analyser des chaînes comprenant un nombre d'états important pour l'évaluation de mesures de sûreté de fonctionnement d'un système. Dans sa thèse, F. Jumel a démontré, entre autres, par une modélisation sous forme de chaîne de Markov des états d'un système commandé

[6] Distribué par la société GFI Consulting

en réseau à retards variables, que les mécanismes de tolérance aux fautes qui prennent en compte la possibilité de défaillance au niveau de la conception de l'architecture fonctionnelle et/ou opérationnelle (ex : suréchantillonnage ou garantie de fail-silence sur les calculateurs) donnent de meilleurs résultats que des solutions de plus bas-niveau (ex : blindage du câble).

2.1.2.2 Réseaux de Petri

Le problème majeur issu de la construction d'une chaîne de Markov est l'explosion du nombre d'états et le manque de représentativité. Une des réponses à cette problématique dans le cadre de l'évaluation de la sûreté de fonctionnement d'un système complexe est l'utilisation des réseaux de Petri.

Réseaux de Petri stochastiques : les réseaux de Petri stochastiques (RdPS) [38] proposent une description du système plus lisible que les chaînes de Markov, et en déduisent directement la chaîne de Markov associée à partir des taux affectés aux transitions. Il est aussi possible d'associer des durées aux transitions dans les réseaux de Petri stochastiques temporisés [8]. De nombreux outils d'évaluation (SURF-2 [60], UltraSAN [31], Moebius [32] ou MOCA-RP) implémentent aujourd'hui les RdPS. Ces outils sont certainement ceux qui offrent le niveau de raffinement le plus riche pour la modélisation de systèmes complexes et l'évaluation des mesures de sûreté de fonctionnement. Les travaux de thèse de C. Ziegler [122] sont un excellent exemple d'utilisation des réseaux de Petri stochastiques pour la modélisation des systèmes embarqués dans l'automobile. Deux systèmes sont modélisés, le coussin gonflable et la direction assistée. L'auteur prouve à l'aide d'une évaluation quantitative de la sécurité, que pour le système de déclenchement du coussin gonflable, l'utilisation d'un calculateur TMR (Triple Modular Redundancy) n'est pas très avantageuse en terme de sécurité par rapport à un calculateur Duplex (redondance double). En ce qui concerne le système de direction assistée, par contre, cette même méthode prouve qu'il est préférable d'utiliser un calculateur TMR.

Réseaux de Petri interprétés : ce formalisme permet de représenter les phénomènes hybrides combinant les aspects discrets et continus. Contrairement aux réseaux de Petri stochastiques, les transitions sont étiquetées par un couple événement/condition : le franchissement d'une condition s'effectue si la condition est vraie, sur occurrence de l'événement. Sur la base des travaux de thèse de D. Jampi [57], R. Schoenig a proposé dans [103] une méthode pour modéliser les systèmes à contrôle-commande hybrides embarqués dans l'automobile sous forme de réseaux de Petri interprétés. Le modèle obtenu est exploité par "stochastisation" des transitions puis génération des graphes de Markov associés. Un exemple d'application est donné dans [103], où quatre architectures plus ou moins tolérantes aux fautes sont modélisées. L'étude des modèles permet de quantifier la fiabilité de chaque architecture et de comparer les résultats entre eux. S'il est prouvé quantitativement que l'architecture disposant du plus grand nombre de mécanismes de tolérance aux fautes est la plus fiable, le problème du coût n'est qu'évoqué.

2.1.2.3 Modélisation orientée objet

Le projet HIDE avait pour objectif l'utilisation d'UML (Unified Modelling Language) pour la modélisation orientée objet des systèmes en vue de la vérification du respect des contraintes de sûreté de fonctionnement [12]. L'idée est de générer automatiquement des chaînes de Markov à partir du modèle UML. La transition est réalisée par la transformation du modèle UML en StateCharts. L'outil PANDA [3] peut alors générer les chaînes de Markov correspondantes et procéder à l'évaluation. Cependant, à notre connaissance, aucun résultat concret obtenu grâce à cette méthode n'est disponible à ce jour.

2.1.2.4 Arbres de défaillance "étendus"

[18] propose d'utiliser des arbres de défaillances étendus, c'est à dire des arbres dont les opérateurs qui relient les événements sont des opérateurs plus complexes que des simples portes logiques. Il est ainsi possible de générer plusieurs réseaux de Petri stochastiques à partir d'un arbre. On peut alors profiter de tous les avantages d'une modélisation en réseaux de Petri. L'applicabilité du processus est montrée avec la modélisation de l'arbre de défaillance étendu correspondant à un système de refroidissement classique. Les réseaux de Petri stochastiques correspondants sont générés automatiquement. L'analyse quantitative de ces modèles présentée dans [18] montre que la disponibilité du système de refroidissement se stabilise au bout de quelques dizaines d'années.

2.1.3 Quantification et mise en oeuvre des techniques

L'évaluation quantitative de la sûreté de fonctionnement d'un système ne peut être effectuée sans injection de valeurs justifiées. Ainsi, le retour d'expérience et les statistiques sont des informations primordiales pour les études de sûreté de fonctionnement. Dans le cadre d'études d'avance de phase, comme c'est le cas pour l'étude des systèmes X-by-Wire, la quantité d'informations disponibles en terme de retour d'expérience n'est pas suffisante. Il faut par conséquent recourir à l'injection de fautes pour évaluer le comportement du système en présence de fautes.

2.1.3.1 Statistiques, retour d'expérience et Mean Time To Failure (MTTF)

Sans mesures, il est impossible d'évaluer la probabilité d'occurrence d'un événement. Les statistiques nous renseignent efficacement sur les paramètres qui caractérisent les variables aléatoires (par exemple : durée de vie, durée de maintenance...) observées lors de l'étude du système. Par exemple, elles sont indispensables à l'évaluation quantitative de la fiabilité R(t), dont [117] donne la définition :

R(t) = P [E non défaillante sur [0,t]]

Le taux de défaillance est un des paramètres les plus utilisés dans l'évaluation de la fiabilité et de la disponibilité des systèmes. Le taux de défaillance λ d'un système embarqué dans l'automobile est considéré comme constant et on fait l'hypothèse que le processus est aléatoire et ergodique - et donc en particulier stationnaire -. Dans ce contexte, [117] nous donne deux hypothèses fondamentales :

- le taux de défaillance est obtenu à partir du Mean Time To Failure (MTTF) du système : $\lambda = \frac{1}{MTTF}$
- on peut utiliser la loi exponentielle pour calculer R(t) : $R(t) = e^{-\lambda t}$ [7]

Etant donné que la grandeur recherchée est une probabilité de défaillance par heure, on étudie le système sur une heure de fonctionnement (t=1 heure), on peut alors donner la formule de la fiabilité dite "statique" :

$R = e^{-\frac{1}{MTTF}}$

2.1.3.2 Injection de fautes

L'injection de fautes est une technique complémentaire à la modélisation. Elle permet de tester le comportement, en présence de fautes, des mécanismes de tolérance aux fautes du système évalué [71]. Un grand nombre de techniques -et les outils associés- sont aujourd'hui disponibles [5]. Les techniques d'injection de fautes varient en fonction du système cible (système physique ou modèle) et de la forme de faute appliquée (altération physique, électrique, ou des informations "bit flip")

[7] Il est important de noter que la notion de fiabilité est fréquemment utilisée pour décrire la défiabilité du système ($R(t) = 1 - e^{-\lambda t}$).

2.1.4 Conclusion sur les méthodes standards de prévision quantitative de faute

Si les graphes d'état-transition sont aujourd'hui le moyen le plus sûr de modéliser des systèmes à fortes contraintes de sûreté, leur exploitation dans le monde de l'industrie est réservée à certains types de systèmes dans des domaines bien précis tels que l'aéronautique ou le nucléaire. Les réticences de certains industriels face à ces méthodes se fondent sur les arguments suivants :

1. Explosion du nombre d'états : même en utilisant les RdPS, la modélisation des systèmes complexes aboutit encore à des modèles contenant parfois plusieurs milliers d'états. Ces modèles sont par conséquent difficile à manipuler, et les moteurs de calculs associés doivent être suffisamment puissants pour donner des résultats en un temps raisonnable. Plusieurs techniques de traitement des modèles permettent une exploitation optimisée de ces derniers. La technique la plus fréquemment utilisée est la simulation de Monte-Carlo, dont la force est que l'erreur de calcul ne dépend pas du nombre de variables [42].
2. Taux de couverture des mécanismes de tolérance aux fautes : certains mécanismes de tolérance aux fautes sont particulièrement complexes à modéliser par des graphes d'état. En outre, la prévision de fautes n'a pas d'intérêt - autre que les études de sensibilité - sans des quantifications réalistes. Or, plus les modèles sont précis, plus les caractéristiques en termes de probabilités et autres taux de défaillances associés aux transitions ou aux opérateurs représentés sont nombreux. Ces taux, qui correspondent fréquemment aux taux de couverture des mécanismes de tolérance aux fautes, sont particulièrement complexes à obtenir et doivent fréquemment être intuitivement approchés (voir travaux de [45] et [122]). Seule l'injection de fautes (voir paragraphe 2.2.2) semble aujourd'hui offrir des résultats concluant quant à l'obtention des taux de couvertures de certains mécanismes de tolérance aux fautes [71]. Cependant, elles ne peuvent que très rarement quantifier tous les taux de transition d'un RdPS affiné. En outre, les RdPS ne permettent pas d'associer une durée déterministe à une faute transitoire. Il est par conséquent nécessaire d'utiliser les RdPS temporisés [8] pour inclure la durée de la faute dans l'analyse. Cependant, cela reste particulièrement compliqué de modéliser tous les mécanismes de tolérance d'un système aussi complexe qu'un système X-by-Wire.
3. Modes de marche : la notion de mode dégradé est fréquemment utilisée dans le monde de l'automobile et multiplie considérablement le nombre d'états à modéliser. Cependant, ces modes de fonctionnement peuvent être complexes à modéliser, notamment dans le cas où le service tel que perçu par le conducteur reste identique. Les structures de récompense et les calculs de performabilité (voir [77]) associés sont une solution efficace, mais la quantification des récompenses peut être problématique et les limites énoncées précédemment restent identiques. Par ailleurs, le regroupement d'états du système en un macro-état représentatif d'un certain mode de marche a été proposé dans [103].

2.2 Influence du réseau de communication sur la sûreté de fonctionnement du système

Les systèmes X-by-Wire sont des systèmes distribués. Les échanges de données entre composants se font selon un protocole de communication donné. La criticité de ces systèmes font du protocole et du support utilisé pour la communication des éléments indispensables pour la sécurité des occupants du véhicule. L'aspect central du réseau de communication est un atout non négligeable pour la tolérance aux fautes (ex : détection des noeuds défaillants). Cependant, si les mécanismes sous-jacents ne sont pas maitrisés ou s'ils sont mal évalués, ces mécanismes peuvent être générateur de défaillances [75]. Ainsi, si les méthodes de prévision de fautes présentées

précédemment peuvent aussi être utilisées pour l'évaluation de la sûreté du réseau de communication, des méthodes et des modèles d'erreurs plus adaptés ont été développées. Par ailleurs, il est important de noter qu'il est indispensable que les algorithmes implémentés au sein du protocole aient été prouvés[8] (utilisation des méthodes formelles) avant toute autre utilisation de méthode d'évaluation. C'est le cas du protocole TTP/C, notamment dans la thèse de H. Pfeifer [90].

2.2.1 Comparaison de protocoles sur critères

2.2.1.1 Rapport comparatif de John Rushby

Dans [99] (mise à jour d'un premier rapport comparatif daté de 2001), John Rushby décrit et compare 4 protocoles de communication destinés à être implantés au coeur de systèmes critiques : 2 protocoles destinés à l'avionique (SPIDER, développé par la NASA, et SafeBUS, développé par Honeywell) et 2 protocoles destinés à l'automobile (TTP/C et FlexRay). Ce rapport comparatif est le plus complet disponible à ce jour dans le domaine.

Les critères de comparaison principaux sont le partitionnement (pour lesquels les protocoles de communication Time-Triggered sont idéaux) et la composabilité[9]. Avant toute comparaison, Rushby définit une Fault Containment Unit (FCU) comme un "composant qui peut être affecté par des fautes indépendamment des autres composants". Il ajoute qu'aucune faute ne doit pouvoir se propager d'un FCU à un autre FCU. Pour chacun des 4 protocoles étudiés, il donne la liste des FCUs, des modes de faute, et du taux maximal tolérable d'arrivée de fautes, puis les qualités et les failles des services suivants :

- synchronisation dans le temps
- gardien de bus (bus guardian)
- démarrage et redémarrage

Les services de base d'un protocole de communication "fiable" tel que la consistence interactive[10] ou la gestion de groupe sont discutés pour chacun des protocoles. Enfin, les notions de flexibilité et de démonstration de la sûreté sont aussi évoqués.

Comme nous l'avons fait dans nos travaux, les fautes de conception ne sont pas prises en compte. Le modèle de fautes considéré est celui de Thambidurai et Park [109] :

- fautes manifestes : correspond à un comportement de type silence sur défaillance ou "Fail-Silent",
- fautes symétriques : fautes cohérentes,
- fautes arbitraires : i. e. byzantines[11] ou asymétriques.

En conclusion de ce rapport, J. Rushby insiste sur le fait que les 2 propriétés majeures que doivent respecter ces protocoles de communication sont la consistence interactive (Interactive Consistency) de la diffusion de messages, et la bonne gestion du partitionnement. D'après lui, seul FlexRay ne respecte aucune de ces propriétés. Les trois autres protocoles de communication respectent ces propriétés mais avec des latences plus ou moins importantes pour la mise en oeuvre des algorithmes de consensus.

[8] Il est aussi indispensable de prouver que les spécifi cations du protocole sont réalistes. Par exemple, les hypothèses de faute du protocole TTP/C semblent assez éloignées de la réalité.

[9] composabilité : une conception composable est une conception au sein de laquelle les applications individuelles ne sont pas affectées par les choix des autres applications avec lesquelles elles sont intégrées.

[10] Pour que la propriété de consistence interactive sont respectée, il faut prouver que les 2 propriétés suivantes sont respectées :
- Agreement : tous les noeuds non-défaillants reçoivent le même message (même si l'émetteur est défaillant)
- Validity : si l'émetteur est non-défaillant, tous les noeuds non-défaillants reçoivent le message effectivement émis.

[11] Rushby précise que les fautes byzantines ne sont pas des fautes qui "ne se produisent jamais en pratique", elles sont la manifestation d'un comportement arbitraire, et elles ont déjà été observées.

Cependant, les spécifications de FlexRay n'étant pas disponibles au moment de la rédaction du document, la comparaison est inégale. En effet, une grande majorité des services ne sont pas spécifiés dans les documents publiques présentant FlexRay. En outre, ce dernier semble laisser beaucoup de liberté au concepteur de l'architecture opérationnelle complète quant aux services à implémenter dans les couches supérieures. C'est pourquoi aucune des conclusions données dans le rapport ne peut être considérée comme définitive.

2.2.1.2 Comparatifs d'H. Kopetz

H. Kopetz, le "père" du protocole TTP/C, a lui aussi publié quelques comparatifs, notamment entre TTP/C et CAN [64], ou TTP/C et FlexRay [65], et plus récemment une présentation [91] comparative de TTP, FlexRay et TTCAN (voir spécifications du protocole TTCAN [40]) . Kopetz part du principe - justifié - que le déterminisme et la composabilité servent la sûreté de fonctionnement d'un système. Il met ainsi en valeur les services de TTP/C qui participent au déterminisme et à la composabilité face à CAN -qui correspond plus à un protocole idéal pour les systèmes événementiels-, et face à FlexRay qui mise autant sur la flexibilité que sur la sûreté de fonctionnement. Comme pour le comparatif de John Rushby, les spécifications de FlexRay n'étaient pas encore disponibles au moment de la rédaction des documents. Le dernier rapport comparatif entre TTP/C et FlexRay démontre assez aisément et à l'aide de critères précis qu'en terme de sécurité, TTP/C a une avance certaine sur FlexRay. H. Kopetz insiste aussi en conclusion sur le fait que TTP/C a aussi été analysé et discuté par des universitaires et des industriels. Plusieurs versions du protocole ont ainsi vu le jour, ces versions tenant compte de certaines critiques, ce qui est effectivement un avantage considérable.

2.2.2 Injection de faute

Si l'injection de fautes peut être appliquée sur un système ou son modèle à n'importe quel niveau, nous ne traitons dans cette section que les pratiques inhérentes à l'injection de fautes sur les protocoles de communication TTP/C et FlexRay.

2.2.2.1 Injection de fautes sur le système physique

En 1990, l'injection de fautes sur la plateforme MARS (MAintenable Real-time System) donnait les premières quantifications des taux de couvertures des mécanismes de tolérance aux fautes des systèmes à communication Time-Triggered. Cette étude a aussi permis de mettre en lumière l'importance des fautes transitoires et de leurs fréquences sur des systèmes, à haut niveau de criticité, embarqués dans l'automobile [66].

Toujours à partir d'injection de faute réalisée sur cette même plateforme, [6] donne le pourcentage de détection de chaque mécanisme pour une erreur donnée. Les perturbations électromagnétiques, au même titre que d'autres sources de fautes transitoires, sont simulées, mais l'accent est mis sur l'efficacité des mécanismes de détection l'un par rapport à l'autre plus que sur la robustesse globale du système.

En outre, la société TTTECH a aujourd'hui mis sur le marché un noeud physique générateur de fautes "Disturbance Node"[12] qui permet d'injecter des fautes dans un système dont le protocole de communication est TTP/C. A notre connaissance, aucun résultat n'a été communiqué à ce jour.

[12] http ://www.tttech.com

2.2.2.2 Injection de fautes sur modèle

Dans le cas du protocole de communication TTP/C, le projet EU-IST-1999-10748 (voir rapport final du projet [55]), intégralement consacré à l'injection de fautes sur plateforme "Time-Triggered" équipée d'un réseau de communication de type TTP/C, a été un des premiers à proposer de l'injection de fautes sur modèle VHDL de systèmes destinés au X-by-Wire (voir aussi [11]). Ce projet a aussi donné naissance à un modèle en langage C du protocole TTP/C et de l'application Brake-by-Wire associée, ainsi qu'à un logiciel d'injection de fautes (voir [49]) dédié à ce type de modèles. Par ailleurs, les résultats des différentes campagnes d'injection de fautes réalisées au cours de ce projet - et aussi, depuis, sur cette plateforme - nous permettent de disposer aujourd'hui de quantifications quant au taux de couverture des mécanismes de tolérance aux fautes implémentés dans les systèmes X-by-Wire. Entre autres, [43] montre qu'il existe - selon leur protocole d'injection de fautes - des situations où le temps de réintégration des noeuds qui ont subi une faute transitoire détectée peut excéder 1 TDMA round (cycle de communication) (3,13% des cas de réintégration pour 4 noeuds). Dans [44], les résultats montrent que dans certaines situations, le cluster (ensemble des noeuds participant à la communication) peut être en situation de faute permanente (durée de la faute supérieure à 128 TDMA rounds). Pour 189.10^6 fautes injectées sous forme de bit-flip (durée des rafales aléatoire), cette situation s'est produite 4 fois.

Par ailleurs, les outils logiciels distribués avec les équipements des protocoles de communication TTP/C et FlexRay offrent des solutions "toute faites" pour la simulation de fautes dans l'environnement Matlab/Simulink. Ces outils, utilisés pour le prototypage et le dimensionnement des lois de commande, permettent aussi de tester la robustesse d'une architecture opérationnelle en présence de fautes. On pourra citer l'outil SITCAM/FlexRay commercialisé par la société Decomsys pour FlexRay et TTP-Matlink pour TTP/C distribué par la société TTTECH.

2.2.3 Evaluations probabilistes

On regroupe dans cette classe les techniques dont l'objectif est, d'une part, de modéliser les aléas qui "perturbent" les échanges d'information ; et d'autre part, d'évaluer quantitativement l'impact de ces aléas sur le comportement du système.

La perte d'informations peut être source d'instabilité pour un système, et ce, quelle que soit l'activité au sein de laquelle l'information va être altérée ou perdue. La plupart des études probabilistes sur la perte d'informations au sein d'un système sont orientées vers la susceptibilité aux perturbations du médium de communication. En effet, ce dernier est la zone du système la plus sensible aux perturbations. On considére alors une erreur comme l'occurrence de l'événement "bit erroné" sur un médium de communication de type bus.

Dans ce contexte, les premiers à avoir pris en compte les erreurs de communication étaient Tindell et Burns dans [110] pour le protocole de communication CAN. Le modèle d'erreurs proposé correspondait alors à une seule rafale d'erreurs et un nombre borné d'erreurs isolées (séparées par une durée minimale paramétrable) pendant toute la durée de l'étude. On peut alors borner le temps de réponse maximal pour un nombre d'erreurs donné.

N. Navet a fait l'hypothèse dans [81] et [82] qu'il est irréaliste de donner une borne pour le nombre maximal d'erreurs pouvant survenir pendant un intervalle de temps. Il a ainsi proposé un modèle probabiliste d'erreurs dans le but d'obtenir la probabilité qu'une trame ne respecte pas son échéance. Ce modèle permet de prendre en compte la fréquence d'arrivée des erreurs et leurs durées (rafales). La fréquence d'apparition est telle que le nombre d'occurrences suit une loi de Poisson, et la durée de la rafale peut entraîner une seule erreur ou une rafale. D'un point de vue mathématique, ce modèle est décrit par un processus de Poisson généralisé :

$$X(t) = \sum_{i=0}^{N(t)} y_i \text{ avec } y_0 = 0$$

– $N(t)_{t\geq 0}$ suit une loi de Poisson de paramètre λavec $P(k) = \frac{(\lambda t)^k}{k!}e^{-\lambda t}$
– $y_i = \begin{cases} u, \, avec\, une\, probabilite\, :\, \alpha \\ 1, \, avec\, une\, probabilite\, :\, 1-\alpha \end{cases}$

Pour l'application numérique, Navet propose la distribution suivante pour la v.a. u :

$$P(u = k) = kp^2q^{k-1}$$

Ce modèle présente l'avantage considérable de prendre en compte les rafales d'erreurs sans bornes prédéfinies quant à leurs durées. En effet, rien ne prouve aujourd'hui qu'une perturbation altère au plus un nombre borné de bits ou de trames consécutifs donnés, le chapitre 6 atteste même plutôt du contraire.

En 2002, dans [16], puis dans sa thèse , I. Broster a remis en cause le modèle précédent, en raison de son pessisme, et plus particulièrement :

– le fait que Navet fasse l'hypothèse que, si une erreur se produit pendant le temps de réponse maximal d'un message, ce message est perdu. Or, ce temps n'étant qu'une borne sur le temps de réponse, il se peut que le message soit déjà arrivé avant l'occurrence de l'erreur.
– l'hypothèse selon laquelle une rafale d'erreurs peut affecter plusieurs message consécutifs.

Il propose alors d'utiliser un modèle "simplifié" qui ne prend pas en compte les rafales. Le dernier modèle d'erreurs proposé par Broster[13] dans [17] nous donne ainsi le nombre d'erreurs k se produisant pendant une durée t. Ce dernier suivant une loi de Poisson, on a :

$$P(k) = \frac{(\lambda t)^k}{k!}e^{-\lambda t}$$

Borster a proposé d'adapter ce modèle au protocole de communication Time-Triggered TTCAN [40]. Il part du principe que la probabilité pour un message m de taille T_m (temps bit) d'être perdu est la probabilité qu'il soit affecté par au moins une faute pendant T_m. Soit, 1 moins la probabilité de n'être affecté par aucune faute :

$P(k \neq 0) = 1 - \frac{(\lambda T_m)^0}{0!}e^{-\lambda T_m}$
$P(k \neq 0) = 1 - e^{-\lambda T_m}$

Il fait alors l'hypothèse que les fautes sont indépendantes, et que seule la perte des n copies du message entraîne une défaillance. La probabilité de perdre les n copies du messages est donc :

$$P(fail)^n = (1 - e^{-\lambda T_m})^n$$

2.2.4 Conclusion sur ces méthodes

Si chacune de ces méthodes permet d'analyser et de comparer les protocoles de communication en vue de la sûreté de fonctionnement du système, il est important de garder à l'esprit qu'elles sont complémentaires.

2.2.4.1 Comparaisons par critères

Si la comparaison des protocoles de communication par critères est indispensable pour mettre en valeur certains avantages, elle est rarement exhaustive, et il n'existe pas de norme de comparaisons avec une liste de critères prédéfinis. De plus certains protocoles de communication, comme le FTTCAN [36], qui pourraient légitimement être un sérieux candidat dans la "course au X-by-Wire", n'apparaissent jamais dans les comparaisons. Par ailleurs, les critères peuvent parfois être entachés de subjectivité et les services ne sont pas identiques pour chaque protocole. Il faudrait aussi prendre en compte le fait que des services non disponibles au niveau protocolaire pourraient être intégrés aux niveaux supérieurs, proposition appliquée dans une étude comparative présentée à RTS 2003 [119].

[13] Un modèle identique avait été présenté par A. Burns dans [19].

2.2.4.2 Injection de fautes

Avec la prise de conscience relative à la part de plus en plus prépondérante des fautes transitoires sur le système embarqué dans l'automobile, l'injection de fautes est devenue indispensable à l'évaluation quantitative des protocoles de communications. Cependant, la non-exhaustivité des tests sur les systèmes physiques et la granularité du modèle du système étudié en font une méthode d'évaluation limitée.

2.2.4.3 Méthodes d'évaluation probabilistes

Les modèles d'erreurs des méthodes d'évaluation probabiliste disponibles posent plusieurs problèmes. Le modèle de N. Navet a été construit de manière très intuitive. Il n'est basé sur aucun retour d'expérience concret. Cependant la prise en compte des rafales en fait déjà un modèle plus réaliste que celui de I. Broster, qui lui considère que les fautes (messages erronés) sont indépendantes, ce qui, de part la nature même des perturbations et des systèmes affectés semble irréaliste. Ainsi, sous la condition qu'on ait modélisé de manière réaliste les perturbations, la méthode de N. Navet permet d'obtenir plus de résultats.

2.3 La stabilité des systèmes commandés en réseau

L'étude de la qualité de service des systèmes temps réel n'a longtemps été que partielle. Elle était essentiellement orientée vers l'ordonnancement de tâches (voir [73]) et les méthodes d'accès au médium de communication dans les réseaux temps réel (voir [111]). Malgré l"'End to End Argument" de Salzer qui montrait déjà la voie en 1984 [56] - "la fonction ne peut être correctement implantée qu'avec une connaissance complète de ses interactions avec l'environnement" -, l'inclusion des caractéristiques de haut niveau de la fonction dans l'analyse n'était qu'anecdotique. Si du point de vue de l'automatique, les critères majeurs de la qualité de service ont aujourd'hui été identifiés, l'identification de critères au niveau d'une implantation est encore un sujet ouvert.

2.3.1 Influence des performances temporelles sur la qualité de service des systèmes échantillonnés

Historiquement, les premiers travaux importants dans le domaine ont été menés par Ray et Halevi en 1988. Leur objectif était d'explorer les effets de retards variables sur les performances des systèmes de contrôle-commande. La conclusion des travaux était claire et sans ambiguité : les retards variables déteriorent les performances de l'asservissement ou de la régulation et peuvent être cause d'instabilité. Andreff prouve à l'aide d'un exemple simple en 1994 qu'une borne maximale sur les retards n'est pas suffisante pour assurer la stabilité [4]. Dans son exemple, son système devient instable lorsque le retard est trop petit. Il montre ainsi qu'une borne minimale sur le retard peut elle aussi être indispensable pour la stabilité du système. (*Pour un état de l'art complet et détaillé sur les travaux menés dans le domaine avant 1998, nous conseillons au lecteur le papier de synthèse "Fundamentals of Implementing Real-Time Control Applications" [113] de Martin Törngren.)*

C'est ensuite en Suède que sont apparus les travaux majeurs avec les thèses de Nilsson [85] (orienté automatique) et Törngren [112] (plus orienté informatique et réseaux) puis au sein du projet DICOSMOS.

G. Juanole et I. Blum avaient eux aussi ouvert une brèche avec [58] en présentant une méthode à base de réseaux de Petri stochastiques permettant de quantifier l'influence des performances temporelles d'une application (durée des tâches, temps de réponse, retard dû à la perte de messages) sur les performances de l'asservissement[14] et

[14] L'asservissement consiste à fournir au système les capacités de suivre au mieux les variations de la consigne qui lui est appliquée.

plus particulièrement sur la marge de phase. Plus récemment, les travaux de thèse de F. Jumel [59] ont proposé des techniques ayant pour objectif d'établir le lien entre certains choix faits lors de la construction d'une architecture opérationnelle et la qualité de la régulation [15]. Pour ce faire, Jumel propose d'utiliser des méthodes analytiques tant que cela est possible, et la simulation le cas échéant.

Dans ce contexte, l'un des objectifs majeurs de nos travaux est de considérer les perturbations comme des événements probables influant sur les temps de réponses des différentes fonctions du système, et d'étudier l'influence de ces perturbations sur la qualité de service de la fonction. En effet, s'il est évident que les critères cités précédemment sont dimensionnant pour la stabilité (du point de vue de l'automatique) du système, d'autres critères comme par exemple la situation de vie de ce même système -notamment s'il est embarqué dans un véhicule- sont tout aussi dimensionnant.

2.3.2 Conclusion sur l'étude analytique des critères de stabilité de l'automaticien

Les techniques proposées pour donner les conditions de stabilité des systèmes à retards variables sont, généralement, difficilement exploitables analytiquement en raison de l'absence de formes closes. Les travaux, présentés dans [59], montrent en outre que, s'il est possible de prouver qu'un système est stable pour un retard τ tel que $\tau \in [\tau_m, \tau_M]$, ceci n'est qu'une condition suffisante et, en particulier, dans certains cas de figure, le système peut rester stable pour un retard $\tau > \tau_M$. Evaluer la stabilité - au sens automatique du terme - du système de contrôle-commande étudié est donc une voie complexe à mettre en oeuvre.

[15] La régulation consiste à maintenir le système dans un certain état quelles que soient les variations de l'environnement.

Conclusions et présentation des contributions

Le chapitre 1 a montré qu'il était indispensable de prouver que les systèmes "X-by-Wire" embarqués dans un véhicule assure la sûreté de celui-ci. Sans remettre en cause l'intérêt - qui n'est plus à démontrer- de chacune de ces méthodes dans des contextes d'application qui leurs sont propres, nous avons décidé de proposer une nouvelle méthode de prévision de fautes quantitative qui évalue l'influence des fautes transtoires et des performances temps réel du système sur la qualité de service (et par extension la sûreté) de la fonction. Notre objectif est d'observer l'impact d'une architecture distribuée ainsi que des phénomènes transitoires directement sur le service tel que perçu par le conducteur et donc directement sur le comportement du véhicule.

Pour ceci, nous introduisons le terme de *Fiabilité Comportementale* (voir définition au chapitre 5) qui pourrait être un nouvel attribut de la sûreté de fonctionnement de système embarqué. Nous définissons la *Fiabilité Comportementale* comme l'aptitude du système à assurer un service en prenant en compte la dynamique de l'application embarquée (performances temporelles, tolérances aux défaillances). Elle se mesure par la probabilité d'occurrence de défaillance au niveau du véhicule qui est causée par des altérations du comportement du système "Steer-by-Wire" dues à des fautes transitoires (par exemple, à des perturbations électromagnétiques). Ces mesures sont associées à une zone entièrement perturbée ou à un trajet suivi par le véhicule.

La contribution de ce travail est une méthode pour évaluer la Fiabilité Comportementale en nous attachant particulièrement aux perturbations électromagnétiques comme sources de fautes transitoires. Nous utilisons partiellement certains des moyens et certaines des méthodes présentés précédemment (injection de faute, modèle d'erreur, critère de stabilité de l'automaticien) dans le but final de quantifier la probabilité d'occurrence de défaillance catastrophique du système. La méthode proposée repose sur plusieurs activités : application de techniques d'injection de fautes sur modèle Simulink pour évaluer l'influence de la durée pendant laquelle des messages sont perdus, sur les critères de qualité ; construction d'un modèle d'erreur probabiliste qui repose sur des rélévés réels caractérisant l'environnement électromagnétique routier pour un trajet donné ; projections des résultats obtenus par l'injection de fautes sur le modèle d'erreur construit afin d'obtenir la Fiabilité Comportementale. Au préalable, nous proposons une technique qui permet de vérifier qu'en l'absence de perturbations affectant le comportement du système (mode nominal), celui-ci assure que le véhicule répond aux critères de qualité définis par PSA Peugeot Citroën.

L'ensemble de la méthode est détaillée en partie 2 de ce document.

Nos travaux ont été appliqués sur les systèmes de direction "Steer-by-Wire" et nous utiliserons un tel système comme exemple pour illustrer, mais les méhodes d'évaluation proposées sont génériques. Une étude de cas est présentée en partie 3.

Partie 2

Introduction

Cette deuxième partie présente les contributions principales du travail réalisé au cours de la thèse. En particulier, ainsi que nous l'avons dit précédemment, la méthode d'évaluation de la sûreté d'un système "X-by-Wire" repose sur une étude de ce système sous une hypothèse d'absence de fautes physiques externes, puis sur l'analyse de ce même système en prenant en compte l'occurrence de perturbations.

Dans un premier temps (chapitre 3), nous introduisons les *critères de qualité* sur lesquels repose l'évaluation de la qualité d'un véhicule chez PSA Peugeot-Citroën. Une qualité minimale, fixée par cet industriel pour chaque type de véhicule, est requise avant mise en production de tout véhicule de ce type. Ces critères sont fixés de telle manière que si la qualité minimale est atteinte, on peut conclure sur le respect des contraintes de sûreté par tous les sous-systèmes composant le véhicule. Notons que, si les critères de qualité présentés dans ce document et leurs modes de calcul sont propres à l'industriel partenaire, la démarche suivie pour leur utilisation dans l'objectif de cette thèse peut être appliquée à d'autres types de mesures de qualité d'un véhicule.

Etude du système en mode nominal.
La conception des lois de commande n'est pas l'objet de cette thèse. Néanmoins, l'étude des systèmes et la détermination des lois de commande à appliquer, telles qu'elles sont réalisées actuellement par des automaticiens, chez PSA Peugeot-Citroën, se font sous l'hypothèse de retard constant ("systèmes à retard") ; en particulier, par une suite de simulations sous Matlab / Simulink, complétées par des tests sur un système réel, les valeurs que peut prendre ce retard et qui sont admissibles pour la qualité requise du véhicule sont évaluées. *Les modèle disponibles chez PSA Peugeot Citroën au moment des travaux et les critères de qualité associés étant ceux des systèmes de direction, nous détaillerons nos travaux en prenant comme illustration les systèmes Steer-by-Wire*. En fait, cette étude fournit une borne supérieure de ce retard pour un système fonctionnant en mode dit *nominal*, à savoir sans perturbations physiques externes pouvant potentiellement altérer le fonctionnement des capteurs/actionneurs, l'exécution des algorithmes sur des micro-contrôleurs ou la transmission des informations sur les réseaux. Un des objectifs de notre travail est d'évaluer le retard induit par une implantation et de chercher sous quelles conditions ce retard est inférieur à la borne fournie. Ce problème est traité au chapitre 4.

Etude du système en mode perturbé
Les systèmes auxquels nous nous intéressons sont soumis, de manière inéluctable pendant toute leur durée de vie, à des perturbations qui peuvent avoir une influence sur leur comportement, et augmenter le retard mesuré précédemment pour le mode nominal. L'injection de fautes lors de simulations sous Matlab/Simulink nous permet d'évaluer, pour une architecture opérationnelle donnée, les valeurs admissibles que peut prendre l'intervalle entre l'arrivée de 2 instances valides du même signal (par exemple, la consigne de direction fournie par le conducteur) consommées par la loi de commande qui élabore les consignes à fournir aux actionneurs (par exemple, la consigne à donner aux moteurs d'entrainement de l'axe de direction) afin de garantir un comportement admissible du véhicule

(par exemple, l'écart de la trajectoire obtenue par rapport à une trajectoire de référence doit être inférieur à un seuil spécifié). L'évaluation de la probabilité d'occurrence de défaillances du système "X-by"Wire" nécessite alors de modéliser les occurrences des perturbations, leur durée et la génération d'erreurs associées. Nous développons au chapitre 5 la notion de fiabilité comportementale d'un système et montrons comment l'évaluer analytiquement. Nous concluons sur la technique d'analyse développée, montrons quelles propriétés de sûreté, exprimées au niveau véhicule, peuvent être garanties et confrontons ce résultat aux préconisations présentées au chapitre 1.

Chapitre 3

Les critères de qualité des systèmes de direction

Ainsi que nous l'avons mentionné en introduction de cette partie, PSA Peugeot Citroën a identifié des "critères de qualité" qui sont propres à ce constructeur et aux types de véhicules considérés. Ces critères correspondent à des mesures représentatives de la "qualité" du véhicule dans des situations de vie particulières qui représentent, en fait, des conditions extrêmes de conduite. En particulier, deux situations de vie du véhicule sont considérées comme référence pour la détermination du pire retard tolérable. Il s'agit de :

- l'*inscription en courbe* qui se traduit par un virage pris à grande vitesse,
- le *sinus balayé* qui représente une séquence d'évitement de plots à amplitude croissante.

Avant de présenter la procédure de tests et les grandeurs significatives à observer dans chacune de ces situations, nous fournissons ci-dessous quelques définitions.

3.1 Définitions

Pour comprendre la philosophie des différents critères de qualité des systèmes de direction utilisés chez PSA Peugeot Citroën, nous présentons ici certaines notions, et le vocabulaire associé, correspondant au mouvement d'un véhicule dans l'espace (voir la figure 3.1 extraite du cours de E. Naudin sur l'ESP (Electronic Stability Protocol) - document interne PSA Peugeot - Citroën).

Le référentiel utilisé pour décrire le mouvement du véhicule est défini par le repère orthonormé (O, X, Y, Z) lié au véhicule. O désigne le centre de gravité du véhicule. La caractérisation du mouvement en translation et rotation est donnée ainsi :

- *accélération* : le vecteur d'accélération est décrit par sa projection sur chaque axe du repère (O, X, Y, Z) ce qui donne les composantes suivantes : accélération longitudinale selon l'axe (O, X), accélération latérale selon l'axe (O, Y), accélération verticale selon l'axe (O, Z),
- *angle de roulis* : le roulis décrit le mouvement de la caisse autour de l'axe (O, X),
- *angle de tangage* : le tangage décrit le mouvement de la caisse autour de l'axe (O, Y),
- *angle de lacet* : le lacet décrit le mouvement de la caisse autour de l'axe (O, Z).

On s'attache généralement à observer plus particulièrement l'angle de tangage lors d'un coup de freinage brusque, tandis que, angles de roulis et de lacet sont observés lors d'une demande de braquage et, en ce qui concerne le

roulis, dans le cas d'un virage serré.

Enfin, l'*empattement* désigne la distance entre les axes des deux essieux tandis que la *démultiplication variable* traduit le fait que les lois de commande prennent en compte la vitesse de lacet et l'accélération transversale pour interpréter la valeur de la consigne d'angle volant de butée à butée.

3.2 Inscription en courbe

L'objectif d'étudier le comportement du véhicule dans ce type d'essai, est double :

- d'une part, il s'agit d'évaluer quantitativement le retard du roulis stabilisé par rapport au lacet stabilisé. On étudie, pour ceci, le comportement d'un véhicule en virage à vitesse et angle de braquage constant.
- d'autre part, il s'agit de quantifier la manière dont le véhicule s'écarte de la trajectoire visée.

Processus de test. La situation de vie étudiée, dans ce cas, correspond à un processus précis qui doit être suivi par l'essayeur et qui obéit aux prescriptions suivantes (les prescriptions qui figurent dans ce document sont données à titre d'exemple mais elles ne sont pas formellement celles appliquées au sein de l'entreprise ; notons que la méthode développée ne dépend pas de la forme du processus de test) :

- Le test est réalisé à 100km/h, avec maintien de la vitesse longitudinale, c'est-à-dire suivant (O, X), en virage (l'essayeur doit donc compenser la décélération du véhicule en accélérant légérement durant le virage pour maintenir cette consigne).
- Le braquage demandé doit correspondre à une accéleration transversale, c'est-à-dire suivant (O, Y) de $0,6g$, soit $5,9m/s^2$; de plus, le volant dispose d'une butée, ce qui permet de limiter l'amplitude.
- Le temps pour aller de 10% à 90% de l'amplitude finale doit être inférieur à $0,15s$.

Mesures. Les enregistrements débutent dés que la valeur d'angle volant atteint 20 degrès. Les grandeurs à observer pendant l'essai sont le lacet et le roulis jusqu'à ce qu'ils soient stabilisés (c'est-à-dire, dés que leur vitesse et leur accélération sont nulles). De cette observation, on déduit quatre valeurs :

- T_p : le temps mis, à partir du temps 0 d'observation, pour atteindre la vitesse de lacet maximale,
- $V_{0,9R}$: la vitesse moyenne pour atteindre 90% du roulis stabilisé,

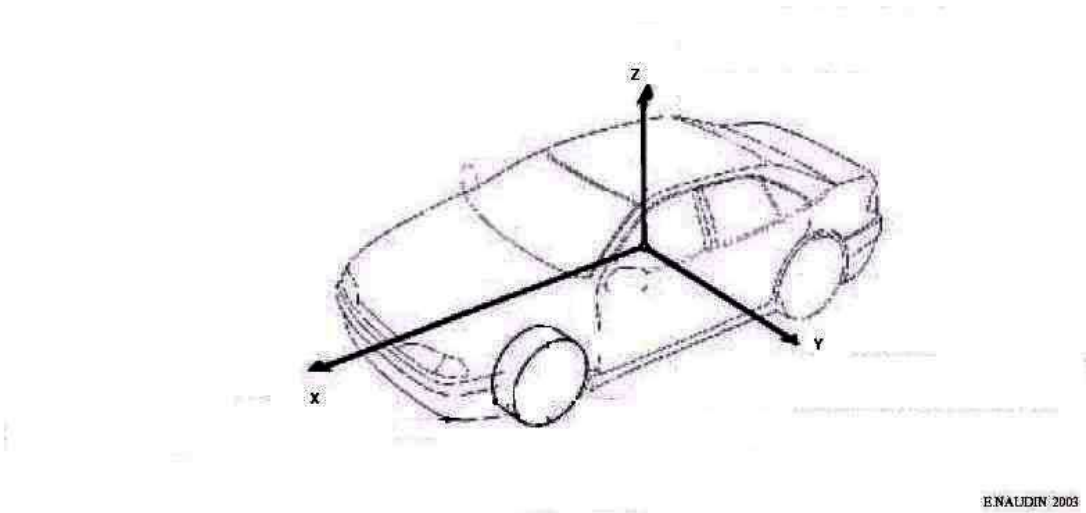

FIG. 3.1 – système de référence d'un véhicule dans l'espace

- $T_{0,9R}$: le temps mis, à partir du temps 0 d'observation, pour atteindre 90% du roulis stabilisé,
- E_V : le pire écart en mètres, obtenu au cours de la campagne de mesures, entre la trajectoire théorique visée (calculée pour un retard nul) et la trajectoire réelle.

3.3 Sinus balayé

Cette situation de vie du véhicule est un cas limite qui permet d'évaluer la facilité à placer le véhicule suivant une certaine trajectoire, ce qui se traduit par la relation entre la vitesse de lacet et l'angle volant.

Processus de test. Il s'agit de réaliser une séance d'évitement de plots à amplitude croissante sur au moins 1 km. L'essayeur, dans ce cas également doit observer un processus de référence précis :

- La vitesse doit être de 90 km/h sur 1 km.
- Le volant doit osciller entre -20° et +20° à une fréquence variant, suivant une fonction parabolique, de 0 Hz à 5Hz, du début à la fin de l'essai.

Mesures. Les grandeurs qui sont observées lors d'une telle campagne de test sont :

- R_L : retard en secondes de la vitesse de lacet par rapport à l'angle volant pour une fréquence d'oscillation du volant de 0,5 Hz.
- G_{mes} : gain mesuré de la vitesse de lacet par rapport à l'angle volant pour une fréquence de rotation du volant de 0,5Hz. (Unité °/s/°). En fait, $\frac{G_{mes}}{G_{th}}$permet de caractériser le comportement sous-vireur d'un véhicule où G_{th}, gain "théorique" (véhicule neutre, modèle bicyclette) de la vitesse de lacet théorique par rapport à l'angle volant, est égal à :
$$\frac{Vitesse\_Vehicule}{Empattement * Demultiplication}$$
- N_g : note obtenue par le véhicule selon une grille de cotation propre à PSA Peugeot Citroën attribuée au rapport gradient / niveau d'effort ; cette note caractérise la précision de la voiture en courbes.

3.4 Fonction "qualité du véhicule"

Pour chacune des deux situations de vie du véhicule vues précédemment, une fonction propre à PSA Peugeot-Citroën, permet de calculer, en fonction des grandeurs observées, une valeur appelée :

- "*note de calage*" dans le cas de l'inscription en courbe,
- "*note de réponse / précision*" dans le cas du sinus balayé.

Cette note représente la qualité globale du véhicule dans cette situation de vie. Les deux fonctions définies pour évaluer ces notes ne sont pas fournies dans ce document pour des raisons de confidentialité. Il s'agit de :

- la fonction $Q_{inscription-courbe}$, dont les variables sont T_p, $V_{0,9R}$, $T_{0,9R}$,
- la fonction $Q_{sinus-balaye}$, dont les variables sont R_L, G_{mes}, N_g.

De plus, dans le cas de l'inscription en courbe, un critère de qualité intéressant est fourni par la mesure de l'écart à la trajectoire de référence (trajectoire désirée et imposée par le cahier des charges de l'essai). Nous verrons comment appliquer ces fonctions et utiliser la valeur de l'écart de trajectoire pour la détermination du pire retard tolérable d'une instance d'un signal consommée par une loi de commande (voir chapitre 4) en l'absence de perturbations ainsi que pour la détermination du pire intervalle d'interarrivée entre deux instances correctes d'un même signal, dans le cas où le véhicule peut être soumis à des perturbations.

Chapitre 4

Méthode d'évaluation du pire retard tolérable

4.1 Présentation du problème

La démarche que nous proposons sera illustrée, ainsi que nous l'avons dit précédemment, sur un exemple de système "X-by-Wire". Fonctionnellement, le contrôle du système de direction d'une automobile est réalisé sous la forme d'un algorithme de contrôle-commande qui enchaîne les actions suivantes de manière itérative :

- Acquisition des valeurs de sortie du système et conversion analogique / numérique de ces valeurs,
- Elaboration de la consigne à appliquer sur les équipements de direction en fonction de la consigne conducteur courante,
- Conversion numérique / analogique de la consigne calculée et application du résultat en entrée du système à contrôler.

Cette chaine d'actions est activée périodiquement à une fréquence F_E déterminée lors de l'identification du système [16]. A chaque activation, le calcul de la consigne pour les actionneurs de direction prend en compte idéalement la consigne conducteur courante.

L'architecture opérationnelle implantant cette application de contrôle-commande est distribuée pour des raisons d'éloignement des organes concernés (volant, axe de direction). L'acquisition et la conversion analogique / numérique de la consigne conducteur (angle volant, couple) est réalisée sur un calculateur (site 1) tandis que les autres traitements sont réalisés sur un autre calculateur (site 2). Les sites 1 et 2 communiquent par l'intermédiaire d'un réseau de communication.

De plus, l'acquisition de la consigne conducteur se fait à une fréquence supérieure à F_E. Chaque valeur acquise est convertie numériquement. Filtrage et formatage des valeurs sont des fonctions réalisées également sur le site 1. Nous détaillerons au paragraphe 4.3.1 le comportement exact de cette activité.

Globalement, sans entrer dans les détails, on peut constater que l'activation i de l'algorithme sur le site 2 à un instant $t_i = (i-1)\frac{1}{F_E}$ consomme en entrée un consigne conducteur qui a été acquise à un instant $t < t_i$. Nous appellerons Retard Pur T_{PD}, la durée qui sépare la consommation d'une consigne conducteur par l'algorithme de contrôle-commande de l'acquisition de sa valeur (voir figure 4.1). La figure 4.1 illustre la durée qui sépare

[16] La fréquence d'échantillonnage peut être obtenue par le théorème de Shannon (la fréquence d'échantillonnage doit être 2 fois supérieure à la plus grande fréquence signifi cative) si l'on connait toutes les caractéristiques fréquentielles du système, ou par la règle d'Aström (la période d'échantillonnage doit être 4 à 5 fois inférieure au temps de "montée" attendu du système) [86].

l'aquisition d'une consigne conducteur et la réalisation de l'ordre correspondant par le système phyisque. Le cas de figure représenté sur cette figure correspond à un système reparti sur 2 sites, cependant, on peut aussi imaginer un troisième site "central" qui, par exemple, calculerait une "consigne sécurisée" à partir de la consigne provenant du site 1 et d'autres informations auxquelles il a accès, et transmettrait cette "consigne sécurisée" au site 2. Notons que cette étape peut être également incluse dans l'élaboration de la consigne.

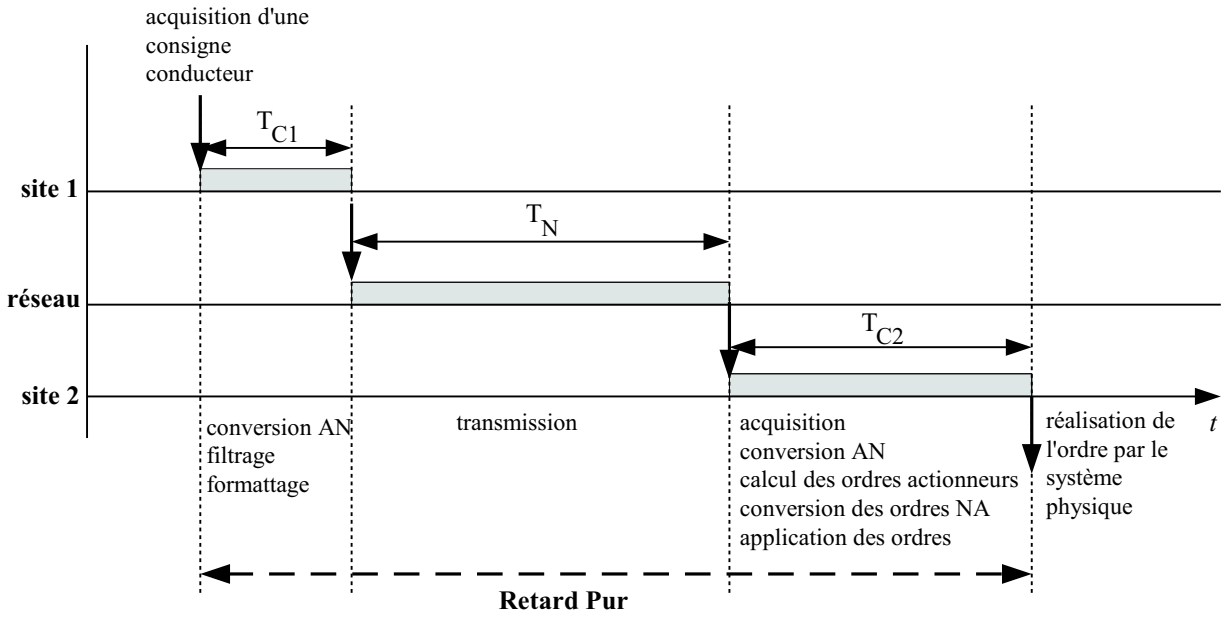

FIG. 4.1 – décomposition des temps par action élémentaire

Les techniques proposées pour donner les conditions de stabilité des systèmes à retards variables sont, généralement, difficilement exploitables analytiquement en raison de l'absence de formes closes (voir section 2.3.2). Une alternative est d'étudier le comportement du véhicule pour des caractéristiques particulières d'une implantation (en particulier, pour des retards de la consigne conducteur différents). Ceci passe par l'observation du véhicule, au cours d'une situation de vie donnée (environnement, vitesse...), et, en particulier, de l'impact de son comportement sur la sécurité des passagers. Dans le cas d'application que nous traitons dans ce travail, des tests sur véhicules ont montré qu'il existe une valeur τ_{max}, que nous appellerons le *pire retard tolérable*, telle que tout retard de la consigne conducteur, constant, τ, supérieur à τ_{max}, pris en compte dans la loi de commande du système Steer-by-Wire a pour conséquence que le véhicule n'est plus pilotable dans certaines de ses situations de vie [30]. Partant de cette remarque, la technique utilisée pour évaluer la borne supérieure du retard admissible repose sur l'observation du comportement du véhicule et non sur l'analyse du système de contrôle-commande que ce véhicule intégre. Nous avons présenté, dans le chapitre 3, quelques situations de vie qui servent de référence chez PSA Peugeot-Citroën et, pour chacune d'elles, quelles sont les variables observées sur le véhicule. Dans le présent chapitre, nous montrons comment, à l'aide de ces informations, il est possible, grâce aux fonctions, introduites à la section 3.4 et propres à ce constructeur automobile, de déterminer la valeur de τ_{max}. Ainsi que nous l'avons vu, les situations de vie qui servent de références à l'étude sont des situations limites au sens où :

> *Si, pour un retard dû à l'implantation donnée, sous une hypothèse d'absence de perturbations, la sécurité n'est pas affectée dans ces situations, elle ne le sera dans aucune autre situation de vie du*

véhicule.

Dans ce contexte, l'objectif est le calculer le retard pur pire cas (pire retard possible entre la production d'un échantillon et sa mise à disposition de l'actionneur) du système étudié, et de le comparer avec le pire retard tolérable. La section 4.2 sera ainsi consacrée à l'évaluation du pire retard tolérable introduit précédemment en fonction de critères propres à la société PSA Peugeot Citroën, et la section 4.3 au calcul du retard pur pire cas (noté par la suite T_{WCPD}).

4.2 Evaluation du pire retard tolérable

Rappelons que les fonctions

- $Q_{inscription-courbe}$, de paramètres T_p, $V_{0,9R}$ et $T_{0,9R}$,
- et $Q_{sinus-balaye}$, de paramètres R_L, G_{mes} et N_g,

permettent d'obtenir deux notes : la "*note de calage*" dans le cas de l'inscription en courbe et la "*note de réponse / précision*" dans le cas du sinus balayé qui représentent la qualité du véhicule dans les situations de vie correspondantes (voir chapitre 3). Malheureusement, dans aucun de ces deux cas, il n'est possible d'exhiber une expression de la fonction qui exprime directement la "*note de calage*" (respectivement, la "*note de réponse / précision*") en fonction de la valeur du retard τ, introduit dans le contrôle de la direction du véhicule.

Aussi, dans le cas de l'inscription en courbe (respectivement, du sinus balayé), pour chaque valeur du retard τ^i, un essai devra être réalisé, un triplet $(T_p^i, V_{0,9R}^i, T_{0,9R}^i)$ évalué (repectivement, un triplet (R_L, G_{mes}, N_g)) et une "*note de calage*" $Calage^i$ (respectivement, une "*note de réponse / précision*" $Reponse\_Precision^i$) obtenue par application de la fonction $Q_{inscription-courbe}$ (respectivement, $Q_{sinus-balaye}$). Nous obtenons donc une suite (τ^i, $Calage^i$) (respectivement, (τ^i, $Reponse\_Precision^i$)) avec $\tau^i < \tau^j$ si $i < j$. Nous faisons, ici, l'hypothèse que la "*note de calage*" (respectivement, la "*note de réponse/précision*") décroit toujours quand le retard τ augmente [17] c'est-à-dire que, pour deux valeurs de retard τ^i et τ^j, telles que $\tau^i > \tau^j$, alors $Calage^i < Calage^j$ (respectivement, $Reponse\_Precision^i < Reponse\_Precision^j$).

Pour chaque véhicule, une note minimum, $Calage_{min}$ (respectivement, $Reponse\_Precision_{min}$) à obtenir pour garantir la sécurité et la qualité du véhicule est fournie par décision de l'entreprise. La valeur du "Retard Pur Maximal Tolérable", pour le critère considéré, $\tau_{max,Calage}$ (respectivement, $\tau_{max,Reponse\_Precision}$) est donc donnée par le dernier τ^i tel que $Calage^i > Calage_{min}$ (respectivement, $Reponse\_Precision^i > Reponse\_Precision_{min}$).

Enfin, nous évaluons, pour l'inscription en courbe, la valeur du plus grand délai conduisant à un *écart de trajectoire* admissible, c'est-à-dire inférieur à l'écart maximal admissible $E_{V,max}$ (dans les expériences menées, fixé à 0,5 m.) de la manière suivante : pour chaque valeur du retard τ^i, un essai est réalisé, l'écart de trajectoire E_V^i est mesuré. Nous obtenons donc une suite (τ^i, E_V^i) avec $\tau^i < \tau^j$ si $i < j$. Nous faisons, ainsi que précédemment, l'hypothèse que l'écart de trajectoire croit toujours quand le retard τ augmente. Aussi, le Retard Pur Maximal Tolérable, selon le critère "*écart de trajectoire*", $\tau_{max,Ecart\_Trajectoire}$ est donc donné par le dernier τ^i tel que $E_V^i < E_{V,max}$.

[17] Cette hypothèse, intuitive, a été vérifi ée par l'expérience.

Le *Pire Retard Tolérable*, τ_{max}, est donc le plus petit Retard Pur Maximal Tolérable évalué pour chacun des critères. Dans le cas traité ici, on obtient :

$$\tau_{max} = min(\tau_{max,Calage}, \tau_{max,Reponse\_Precision}, \tau_{max,Ecart\_Trajectoire}) \tag{4.1}$$

Nous avons réalisé un modèle Simulink et l'avons exécuté dans un environnement véhicule "SimulinkCar" fourni par PSA Peugeot Citroën (voir Annexe A pour les informations sur le simulateur). Cependant, comme expliqué dans l'Annexe A, les résultats donnés par le modèle d'environnement véhicule SimulinkCar pour le critère de réponse-précision ne sont pas satisfaisants. Néanmoins, sur la base de retour d'expériences, il est communément admis que $\tau_{max,Calage} \simeq \tau_{max,Reponse\_Precision}$. Ainsi, dans le cadre d'une évaluation a priori, nous n'utiliserons dans la suite du document que les critères de calage et d'écart de trajectoire sur inscription en courbe :

$$\tau_{max} = min(\tau_{max,Calage}, \tau_{max,Ecart\_Trajectoire}) \tag{4.2}$$

4.3 Détermination du "Retard Pur Pire Cas ", τ_{WCPD}, dans une architecture opérationnelle donnée

On désigne par le terme d'architecture opérationnelle une projection de l'architecture fonctionnelle / logicielle du système (fonctions, liens de données, contrôle) sur une architecture matérielle donnée. Elle représente donc l'ensemble des tâches et des trames véhiculées sur les réseaux, leurs attributs et ceux relatifs aux politiques d'ordonnancement et aux protocoles. Notons que notre étude est illustrée sur une architecture opérationnelle correspondant à un système "X-by-Wire". Ce système assure ses services par exécution d'un ensemble d'activités interdépendantes. La chaîne d'activité correspondant à un de ces services est présentée au paragraphe suivant.

4.3.1 Un exemple de chaîne d'activités dans une architecture opérationnelle de type Steer-by-Wire

La figure 4.2 montre une architecture opérationnelle de référence pour les systèmes Steer-by-Wire, et plus particulièrement, pour assurer la fonction qui consiste à piloter l'axe de direction en fonction de la consigne fournie par le conducteur (par l'intermédiaire du volant). La partie de l'architecture opérationnelle qui réalise la fonction donnée fait apparaître une chaîne d'activités :

- acquisition : les consignes du conducteur sont lues (couple et angle volant) à l'aide de capteurs, de manière périodique ; après chaque acquisition, la dernière valeur lue est mise à disposition pour d'autres activités (variable partagée).
- traitement de mise en forme de la consigne conducteur : un traitement des informations est réalisé périodiquement par un calculateur (calculateur "volant") ; aprés chaque traitement de mise en forme, la dernière valeur de la consigne conducteur est mise à disposition pour d'autres activités (variable partagée). Ce traitement peut être redondé sur n calculateurs.
- transmission : la dernière valeur produite par le traitement décrit précédemment est transmise, également périodiquement, par chaque calculateur sur les n canaux de communication (redondance de la communication).
- traitement de calcul de la consigne actionneur : périodiquement (selon la période de transmission), le traitement implantant l'asservissement de l'axe de direction est exécuté ; il reçoit la valeur transmise par les

canaux de communication, calcule la consigne à appliquer aux actionneurs de l'axe de direction puis l'applique. Ce traitement est implanté sur un calculateur (calculateur "actionneur").

– Actionnement : l'actionneur met en oeuvre la consigne qui lui est appliquée.

En fait, ainsi que nous le verrons dans la section suivante, les données consommées et produites par chaque activité relèvent de concepts différents (voir section 4.3.2). De plus, ces activités observent des périodes différentes (voir section 4.3.3).

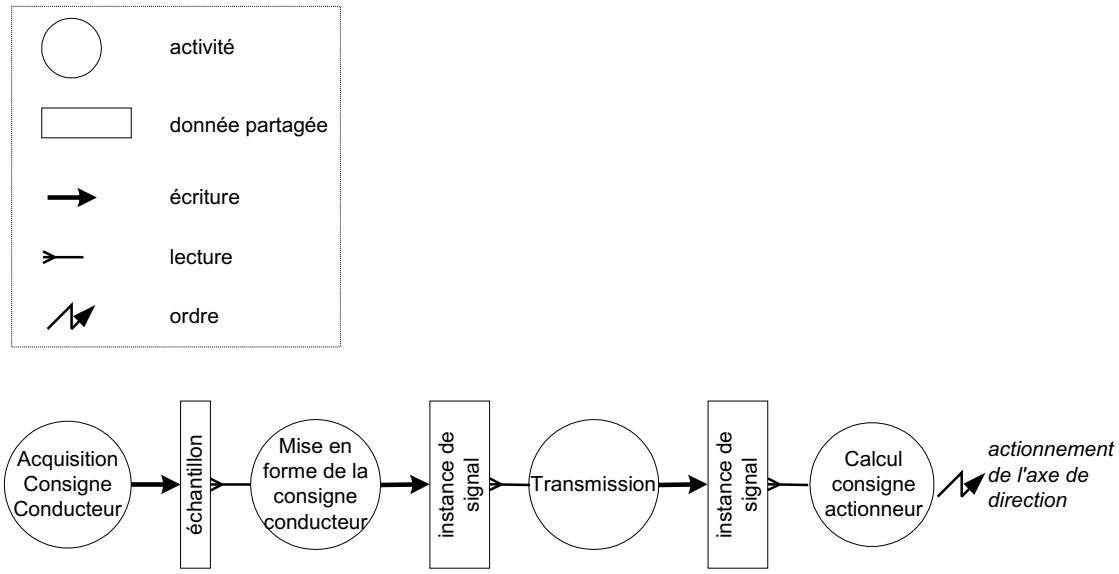

FIG. 4.2 – Chaîne d'activités de la fonction "pilotage de l'axe de direction"

4.3.2 Problématique de la mise à jour de l'information

Cette section a pour objectif de préciser le vocabulaire concernant toutes les entités associées à une information au cours de la durée de fonctionnement du système (voir figure 4.3).

Point de vue de l'information applicative

– Nous appelons "information" une entité qui représente un état de l'environnement. Par exemple, la *consigne d'angle volant* est une information.

– Une information, à un instant donné, peut être composée de plusieurs "informations élémentaires" qui correspondent, chacune, à une variable mesurable par un capteur. Nous appellons chacune de ces informations élémentaires, une "variable". Par exemple, l'information "*consigne d'angle volant*" est composée des variables "*angle volant*" et "*couple volant*".

– Les applications qui nous intéressent fonctionnent en effectuant, au cours du fonctionnement du système, des lectures successives et, dans le cas des systèmes X-by-Wire, périodiques, de chaque variable. Un "échantillon" correspond à une lecture d'une variable à un instant donné. Une variable est donc matérialisée par une suite d'échantillons. Chaque échantillon est décrit par un couple (*valeur,numéro*). La périodicité de création des échantillons est une caractéristique de l'"information".

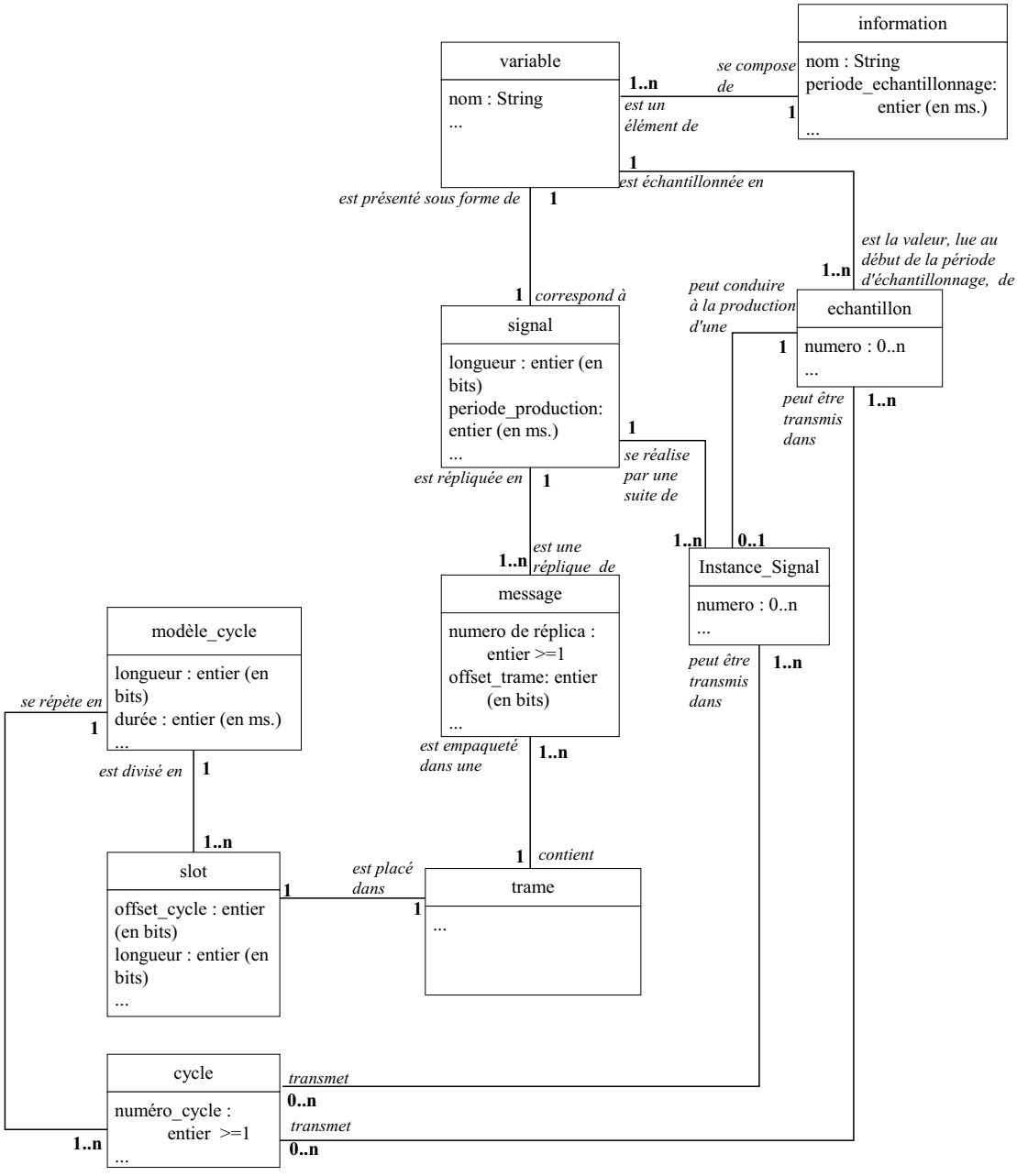

FIG. 4.3 – de l'information au slot

Point de vue de la communication

- La communication des informations sur le réseau relève d'un "modèle de cycle" qui définit, hors ligne, précisémment, une suite de "slots" qui se répète périodiquement. Un "modèle de cycle" est caractérisé par sa longueur en bits et sa période en millisecondes.
- Au cours de la vie du système, le temps, du point de vue du réseau, peut être vu comme une séquence de "cycles".

Des informations applicatives aux régles de communication

- Lors de la conception du système, à chaque "variable" correspondra un "signal" qui représente la régle de présentation de la variable (en particulier le nombre de bits nécessaires pour la coder). L'entité "signal" est l'élément de base qui sera manipulé lors de la configuration des cycles de transmission (par exemple, sur TTP/C). Un "signal" est caractérisé par sa période de production et l'offset appliqué sur la première production.
- De plus, pour des questions de tolérance aux fautes un même "signal" peut être transmis plusieurs fois dans un cycle par des calculateurs différents. On désigne par "message" un exemplaire du signal dans un cycle. Ainsi, une "instance de signal", lorsqu'elle est transmise, est répliquée sous forme de "messages" au sein du "cycle" concerné.
- Les "messages" sont groupés au sein de "trames".
- A chaque "trame" correspondra un "slot" dans chaque "cycle" de communication.

Ainsi que nous pouvons le voir dans le diagramme UML présenté en figure 4.3, les différentes activités du système sont périodiques. Nous montrons, dans le paragraphe suivant, l'impact du choix des différentes périodes sur le comportement d'une application.

4.3.3 Relation entre les périodes des différentes activités

Dans ce qui suit, nous noterons :

- ε_c : la période d'échantillonnage d'une information,
- dt : la durée d'exécution d'un traitement sur un calculateur "volant". Cette durée est supposée constante au cours de la vie du système et identique sur chacun des calculateurs redondés (voir hypothèse 3 ci-dessous).
- ε_t : la période d'activation des traitements sur un calculateur "volant". Il s'agira également de la période de production associée à un signal.
- ε_n : la durée d'un cycle de transmission sur le réseau.
- d : l'intervalle de temps entre la fin du dernier réplica concernant le signal dans tout cycle de transmission et la fin du cycle.

4.3.3.1 Echantillonnage périodique des variables - Production périodique des instances de signaux

Hypothèse 1 : Nous considérons, dans la suite des travaux, que les "informations" sont sur-échantillonnées. Ceci signifie que la période de lecture des échantillons est plus petite que la période de traitement de mise en forme de la consigne conducteur (construction d'une instance de signal). Soit $\varepsilon_c < \varepsilon_t$.

Hypothèse 2 : Une "instance de signal" est produite *en fin* de chaque traitement de mise en forme de la consigne conducteur. On considère que la gigue sur la fin des traitements est nulle. Cette hypothèse est réaliste pour un calculateur dédié hebergeant un nombre restreint de fonctions, ce qui est les cas des systèmes Steer-by-Wire actuels. Cependant, dans le cadre d'un système plus complexe, il serait nécessaire de prendre en compte

l'ordonnancement des activités et l'éventuelle gigue induite sur la fin de la tâche de production d'instances de signaux.

Hypothèse 3 : Tous les producteurs du même signal (réplication des producteurs sur des calculateurs redondés au sein d'une FTU (une FTU est un ensemble de plusieurs stations qui assurent la même fonction et émettent leurs messages dans des fenêtres temporelles différentes) et réalisent leurs traitements selon la même période (ε_t) et le même temps de traitement (d_t). Par ailleurs, nous supposons qu'ils sont synchronisés.

Transmission périodique des trames - Règles de consommation des trames

Hypothèse 4 : La période d'exécution des traitements de calcul de la consigne actionneur est égale à la durée d'un cycle et le début d'exécution est "calé" sur la réception de la dernière réplique du cycle.

Production périodique des signaux - Transmission périodique des trames

Plusieurs cas de figures sont possibles :

– la période de production d'un signal est inférieure à la durée d'un cycle (voir figure 4.4). Certaines instances de signaux ne seront pas transmises.

la période de production d'un signal est supérieure à la durée d'un cycle. Dans ce cas, la même instance de signal correspondant donc au même échantillon peut être transmise dans plusieurs cycles successifs (voir figure 4.5). Remarque : Le cas limite qui a été implanté dans le projet PSA Peugeot Citroën étudié est celui où les périodes sont égales.

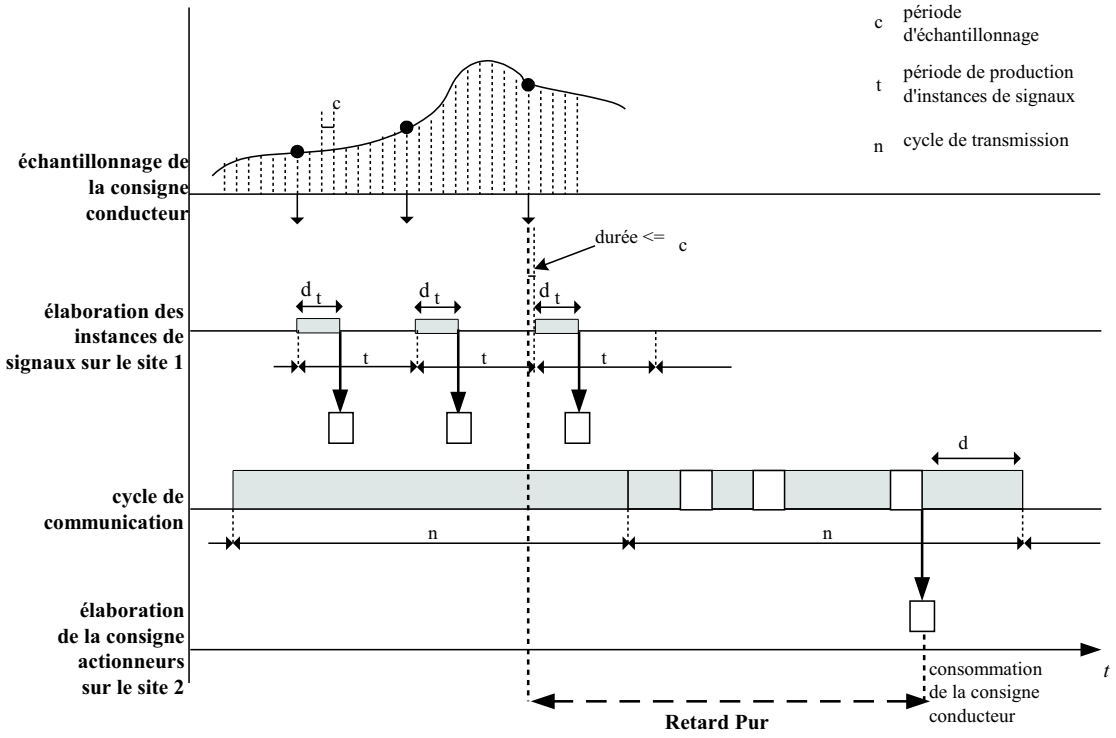

FIG. 4.4 – Retard Pur dans le cas $\varepsilon_t < \varepsilon_n$ (cas 1)

Hypothèse 5 : l'instance de signal consommée par l'algorithme d'élaboration de la consigne actionneur est représentative de l'évolution de la consigne conducteur depuis la dernière instance de signal consommée.

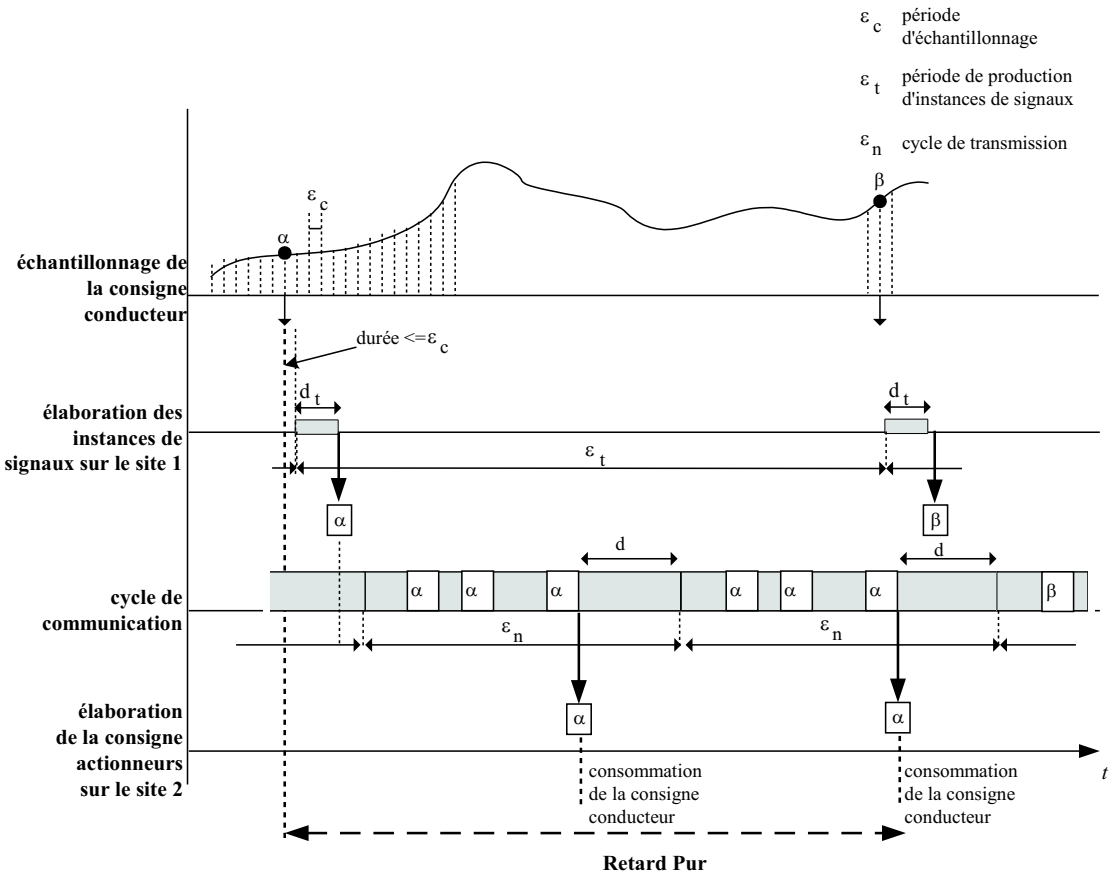

FIG. 4.5 – Pire Retard dans le cas $\varepsilon_t > \varepsilon_n$ (cas 2)

4.3.3.2 Formulation générale du Retard Pur Pire Cas

Cas 1 : $\varepsilon_n > \varepsilon_t$

Le Retard Pur Pire Cas T_{WCPD} d'une consigne conducteur traitée lors d'une exécution de l'élaboration de la consigne actionneur (site 2) est défini ainsi :

- L'instance de signal considérée est celle qui était disponible au début du cycle de communication correspondant à l'exécution de l'élaboration de la consigne actionneur ; ceci signifie que le retard inclut $\varepsilon_n - d$.
- Dans le cas $\varepsilon_n > \varepsilon_t$, cette instance de signal a pu, au pire, être produite à $\varepsilon_t - dt$
- Enfin, toute instance de signal a été produite, à partir d'un échantillon ; le temps de production s'ajoute systématiquement au retard ; il est constant (voir hypothèses 2 et 3) et égal à dt.
- Quant au dernier échantillon, à partir duquel l'instance de signal considérée a été produite, il précède au pire le début de production de cette instance de la durée ε_c.

Donc, le Retard Pur Pire Cas est égal à :

$$T_{WCPD} = (\varepsilon_n - d) + (\varepsilon_t - dt) + (dt) + (\varepsilon_c)$$

soit, si on néglige ε_c qui est toujours trés inférieur à ε_t :

$$T_{WCPD} = \varepsilon_n - d + \varepsilon_t \tag{4.3}$$

Cas 2 : $\varepsilon_n < \varepsilon_t$

Dans ce cas, la même instance de la consigne conducteur peut être transmise dans des cycles de communication successifs et donc, traitée lors d'exécutions successives des traitements d'élaboration de la consigne aux actionneurs. Si l'on considère que le Retard Pure Pire Cas T_{WCPD} est obtenu pour la dernière réplique de l'instance de signal sur le site 2, cette condition est suffisante, mais pas forcément nécessaire. En effet, il est possible que la loi de commande implantée au niveau de l'actionneur ait été conçu pour l'arrivée de plusieurs instances de signal identiques consécutives, et que seule la première d'entre elles soit nécessaire. Cependant, si aucune information n'est disponible sur cette loi de commande, on considère que le Retard Pur Pire Cas T_{WCPD} est obtenu pour la dernière réplique de l'instance de signal arrivée sur le site 2. Il est défini ainsi :

- L'instance de signal considérée est celle qui était disponible au début du cycle de communication correspondant à la dernière utilisation de cette instance ; ceci signifie que le retard inclut $\varepsilon_n - d$.
- Dans le cas $\varepsilon_n < \varepsilon_t$, cette instance de signal a pu, au pire, être produite à :
$$\left\lfloor \frac{\varepsilon_t}{\varepsilon_n} \right\rfloor \varepsilon_n + \varepsilon_t - dt$$
- Enfin, toute instance de signal a été produite, à partir d'un échantillon ; le temps de production s'ajoute systématiquement au retard ; il est constant (voir hypothèses 2 et 3) et égal à dt.
- Quant au dernier échantillon, à partir duquel l'instance de signal considérée a été produite, il précède au pire le début de production de cette instance de la durée ε_c.

Donc, le Retard Pur Pire Cas est égal à :

$$T_{WCPD} = (\varepsilon_n - d) + (\left\lfloor \frac{\varepsilon_t}{\varepsilon_n} \right\rfloor \varepsilon_n + \varepsilon_t - dt) + (dt) + (\varepsilon_c)$$

soit, si on néglige ε_c qui est toujours trés inférieur à ε_t :

$$T_{WCPD} = (\left\lfloor \frac{\varepsilon_t}{\varepsilon_n} \right\rfloor + 1)\varepsilon_n - d + \varepsilon_t \tag{4.4}$$

4.3.4 Conclusion : vérification du respect des contraintes temps réel et optimisation de l'architecture opérationnelle

Nous avons vu dans ce chapitre comment déterminer le pire retard tolérable, τ_{max}, appliqué à la consigne conducteur, tel que la sécurité du véhicule n'est pas impacté. En mode nominal (sous une hypothèse d'absence de perturbations), l'architecture opérationnelle du système X-by-Wire garantit cette sécurité, si et seulement si :

$$T_{WCPD} \leq \tau_{max}$$

où T_{WCPD} est le Retard Pire Pur Cas, dont nous avons fourni un moyen d'évaluation dans le paragraphe 4.3.3.2.

Cependant, la comparaison entre T_{WCPD} et τ_{max} ne permet pas uniquement de valider les performances temps réel de l'architecture opérationnelle, elle permet aussi d'avoir une idée de la qualité de service du système telle

que perçue par le conducteur. En effet, d'après le chapitre 3, plus T_{WCPD} est petit, et plus la qualité du système de direction est élevée. Le concepteur peut donc utiliser la méthode pour valider l'architecture opérationnelle en mode nominal, mais aussi évaluer ses performances. Par ailleurs, le concepteur peut aussi profiter de la marge entre T_{WCPD} et τ_{max} pour augmenter la durée des cycles de communication ou les périodes de production si le besoin s'en fait ressentir.

Il est tout de même important de noter que tant que le mode perturbé n'a pas été étudié, les conclusions concernant la validation de l'architecture opérationnelle étudiée sont temporaires.

Chapitre 5

Verification du respect de la contrainte de sûreté en cas de fautes transitoires dues à l'environnement (mode perturbé)

Comme expliqué en introduction, les systèmes Steer-by-Wire sont soumis à des perturbations qui peuvent avoir une influence néfaste sur leur comportement et entraîner des défaillances catastrophiques. Après avoir donné les caractéristiques de ces perturbations (section 5.1), nous définissons une terminologie claire et précise pour les notions de fautes, d'erreurs et de défaillances, d'abord au niveau du système Steer-by-Wire, puis au niveau du véhicule (section 5.2). Ayant défini une défaillance de niveau véhicule comme l'événement correspondant au cas où l'intervalle entre l'arrivée de 2 échantillons valides au niveau des actionneurs en cas d'erreurs est supérieur à l'intervalle maximal tolérable, nous évaluons alors le nombre maximal de cycles de communication consécutifs erronés tolérables (section 5.3). La probabilité de perdre toutes les instances du même signal étant fonction de la qualité de la conception du système, notamment en terme de redondance et de diversification, nous proposons à la section 5.4 quelques méthodes pour évaluer l'influence de la redondance et de la diversification sur la probabilité de perdre toutes les instances du même signal. Ces grandeurs étant identifiées, on est alors en mesure de calculer les 2 métriques qui quantifient la Fiabilité Comportementale : la probabilité d'occurrence de défaillance dans une zone perturbée (section 5.5) et la probabilité d'occurence de défaillance pour un trajet donné (section 5.5.3). Enfin, la dernière section de ce chapitre est consacrée à l'analyse de la correspondance entre les probabilités définies dans les sections précédentes et la contrainte de sûreté telle que définie à la section 1.3.3.

5.1 Source de perturbations et fautes transitoires

Comme expliqué précédemment, nous consacrons notre étude en mode perturbé à l'influence des fautes transitoires sur le comportement du système Steer-by-Wire et du véhicule au sein duquel il est embarqué. Or, les fautes transitoires sont exclusivement causées par des perturbations de tous genres. Le dictionnaire Larousse donne pour le terme *perturbation* la définition suivante : "trouble qui entraîne une altération, un dérangement". La susceptibilité aux perturbations des systèmes électroniques constitue une des différences majeures avec les systèmes mécaniques/hydrauliques. En effet, on imagine mal une colonne de direction déformée par un passage aux abord d'un radar militaire puissant ou par une hausse de température brutale dans le compartiment moteur. Les systèmes

électroniques embarqués sont par contre susceptibles d'être "dérangés" ou "altérés", pour reprendre les termes de la définition, par ces situations. Cette réalité est devenue un nouveau paramètre de poids, particulièrement pour la conception et l'évaluation de la sûreté de fonctionnement du système. Dans ce contexte, nous avons fait le choix de consacrer exclusivement notre analyse à la quantification de l'influence des perturbations sur la sûreté du système. Les perturbations étudiées auront pour sources la pollution électromagnétique et les variations de températures. D'autres sources, telles que les particules alpha, les neutrons ou les décharges électrostatiques sont susceptibles de perturber les systèmes électroniques, notamment les équipements à base de nanotechnologie [13, 115, 84, 105], mais le manque de renseignements disponibles sur les occurrences et les pathologies de ces perturbations nous a amené à ne pas en tenir compte dans notre étude. Cependant, dans l'éventualité où une analyse qualitative et quantitative de l'environnement radiatif routier verrait le jour, la méthode proposée pour l'évalution de l'influence des perturbations électromagnétiques sur la sûreté serait applicable.

5.1.1 La température

Les composants embarqués dans l'automobiles doivent être résistants à une plage de température allant de -30° à 120° Celcius. Cependant, lorsqu'ils sont soumis à une température élevée proche de ses limites pendant une durée assez longue, des composants tels que les diodes ou les transistors peuvent avoir un comportement qui se dégrade [50]. De plus la surchauffe du compartiment moteur est un événement dont la probabilité d'occurrence n'est pas nulle. C'est pourquoi nous considérons que ce type de perturbation a une influence sur la sûreté du système. Pour un modèle d'erreur focalisé sur les perturbations dues à la température, le lecteur pourra se référer au modèle décrit dans [63]. Un exemple d'application de ce modèle aux évaluations de la sûreté des systèmes X-by-Wire a été présenté à la conférence Convergence 2004 [21].

5.1.2 Les perturbations électromagnétiques

Elles représentent le coeur de notre étude, même si l'approche proposée est, sous certaines hypothèses, applicable à d'autres formes de perturbations. En effet, même si le rapport de cause à effet reste encore aujourd'hui complexe à établir, certains travaux tendent à montrer que les perturbations électromagnétiques peuvent être la cause d'accidents graves. En 1998, Elaine Scarry avait été jusqu'à affirmer dans un prestigieux journal New Yorkais que les perturbations électromagnétiques étaient la cause des crash des vols TWA 800 et Swissair 111 [102], et que l'aéroport JF Kennedy de New York pouvait être un "Triangle des Bermudes". Même si ses travaux sont discutés par la NASA et quelques universitaires [67], elle a mis en lumière une problématique encore loin d'être maitrisée aujourd'hui. En outre, plusieurs témoignages attestent du fait qu'en présence de sources perturbantes, certains véhicules ont des comportements inattendus, voire dangereux[18].

Les principales sources de pollution électromagnétique sont essentiellement les émetteurs de radiocommunication et de radiodiffusion et autres radars (y compris les émetteurs servant la téléphonie et toute autre forme de télécommunication), la foudre, les décharges électrostatique humaine (par exemple lors d'un contact sol-véhicule), les lignes aériennes à haute tension, les machines domestiques et industrielles, et les véhicules eux-même (par exemple les véhicules d'intervention d'urgence équipés d'émetteurs puissants) [89, 94] .

[18] Pour des exemples, des forums de discussion, des avis sur le sujet, voir :
- http ://www.forum-auto.com/sqlforum/section4/sujet123065.htm
- http ://membres.lycos.fr/corruptn/10-81.htm
- http ://www.metatechcorp.com/URSI.htm
- http ://www.globalsecurity.org/org/news/2002/021216-secure01.htm
- http ://archive.infopeace.de/msg01934.html

Le domaine de l'électromagnétisme est un domaine où les incertitudes de mesures peuvent être importantes, ce qui amène les concepteurs de systèmes embarqués dans l'automobile à soumettre leurs composants à des niveaux de champs très élevés en phase de test. Trois dimensions sont à prendre en compte pour la spécification de composants robustes aux perturbations électromagnétiques : la fréquence, la puissance, et le niveau du champ. Cette problématique est aujourd'hui mal maîtrisée, et la seule véritable limite imposée par la règlementation est que le composant doit être robuste à un certain niveau de champ pour une certaine plage de fréquence. PSA Peugeot Citroën respecte cette réglementation en imposant une classe de fonctionnement à respecter pour un certain niveau de champ rayonné et une certaine plage de fréquence (voir norme véhicule confidentielle [95]). La norme à respecter est la norme NF R1308-2 [83], elle même inspirée de la norme ISO 11451-2 [53]. Les directives européennes sont quant à elles réunies dans un seul et même document : la CEI 61000-4-2 [22]. Cependant, des études telles que [97] indiquent que des résultats positifs ne constituent qu'une "présomption de conformité", et qu'il est très difficile de prévoir si un équipement sera sensible ou non à une perturbation donnée. De même, [62] indique que la caractérisation de l'environnement électromagnétique n'est basée que sur des valeurs moyennes. De plus, certains appareils non conformes tels que des radios CB (Citizen Band radio) et autres émetteurs utilisant des bandes de fréquence et des puissances interdites sont aujourd'hui en circulation, et sont potentiellement en mesure de perturber les systèmes électroniques embarqués dans l'automobile. C'est pourquoi la probabilité de rencontrer un pic de perturbation susceptible d'altérer le bon fonctionnement du système est non nulle, et un des objectifs majeurs de ce document est d'apporter une méthode permettant de la calculer.

5.1.2.1 Quelle dégradation pour le système

A notre niveau, la plus petite dégradation détectable et observable est l'inversion de bit (aussi communément appelé "Bit Flip" ou "Soft Error"). Cette inversion peut se produire dans n'importe quelle couche du système : mémoire, traitement, réception, émission ou transmission. Ainsi, nous considérerons qu'un champs électromagnétique est en mesure de perturber le système lorsqu'il est susceptible d'inverser au moins un bit.

5.1.2.2 Bande de fréquences et niveau de champs

Une étude japonaise réalisée à la fin des années 80 sur la caractérisation de l'environnement électromagnétique routier utilisait la bande de fréquence suivante pour ses relevés : de 10KHz à 1 GHz. La norme véhicule PSA Peugeot Citroën élargit le spectre et prévoit deux séries d'essais. Le comportement des composants au cours de ces essais est observé. En fonction de la criticité du système et de son comportement, on peut déduire une classe de fonctionnement et un niveau de fonctionnement. Les hautes et les basses fréquences font tous deux l'objet d'une série de tests. Même s'il est clairement indiqué dans le document que "l'équipement ou le système est conçu de manière à ce qu'aucune perturbation électromagnétique ne puisse entrainer un effet catastrophique", il est aussi important de noter qu'au dessus de 100V/m, une dégradation du service est tolérée. Or, sur un système de type X-by-Wire, une simple dégradation de service peut rapidement se transformer en événement catastrophique. La criticité du système nous amène donc à adopter l'approche "pire cas" suivante : n'ayant aucune preuve du contraire, nous ferons l'hypothèse qu'un niveau de champ supérieur à 100V/m est susceptible de perturber un système X-by-Wire. Plusieurs arguments pourraient avoir tendance à minimiser le pessimisme de l'approche "pire cas" :

- seules certaines fréquences pour certaines puissances données sont susceptibles d'influencer le fonctionnement d'un système électronique,
- la notion de dégradation n'est pas clairement expliquée mais pourrait éventuellement être transparente pour l'utilisateur du véhicule.

Cependant, comme exprimé précédemment, la criticité des systèmes, la connaissance grossière de l'environnement routier et les quelques événements révélateurs d'une réalité quant à la mise en cause de la sécurité du conducteur nous amènent à conserver cette approche "pire cas" pour notre modèle d'erreur du paragraphe 5.5.4 .

5.1.2.3 La CEM et l'avenir

De la micro à la nanotechnologie : Si tout le monde s'accorde sur le fait que la nanotechnologie va s'imposer dans la conception de systèmes électroniques embarqués, cette innovation n'est pas sans risque. En effet, ces circuits sont beaucoup plus sensibles aux perturbations, et la quantité de soft-errors ou bit-flips (inversion de bits) risque d'augmenter considérablement si toutes les précautions requises ne sont pas prises en amont [13, 115, 84, 105]. Les mondes de l'aérospatiale et de l'aéronautique, pourtant connus pour mettre beaucoup de moyens aux services de la sûreté de fonctionnement, sont aujourd'hui confrontés à des problèmes de ce type avec leurs systèmes électroniques embarqués de conception sous-microniques[19] [115].

Le 42 Volts : De même que pour l'avénement de la nanotechnolgie, l'implantation de sources d'alimentation capable de fournir jusqu'à 42 Volts ne fera qu'accentuer les problèmes de compatibilité électromagnétique. En effet, certains des composants requis pour fournir une tension de 42 Volts - par exemple de nouveaux commutateurs - fonctionnent à des fréquences et des niveaux de puissance particulièrement importants (voir [70]) qui sont susceptibles de perturber les autres systèmes. Si ces problèmes concernent plutôt la compatibilité des systèmes intra-véhicule, ils sont tout de même révélateurs d'une réalité : la perturbation CEM doit, aujourd'hui plus que jamais, être pensée comme une entrave conséquente à la sûreté de fonctionnement des systèmes embarqués.

5.1.3 Notion de zone et de durée de perturbation

Dans la suite du document, nous focaliserons donc notre étude sur les perturbations électromagnétiques. Une perturbation de ce type ne pourra avoir une influence sur la sûreté du système - et donc du véhicule - que si le véhicule est en mouvement. Si l'on considère qu'une perturbation CEM est causée par une source fixe (ex : un radar) ou en mouvement (ex : un radio-émetteur embarqué) dont le champs d'émission est limité à une certaine zone, on peut alors associer la notion de zone traversée par le véhicule à la notion de perturbation, et plus particulièrement à la notion de durée de perturbation. Pour ce faire, nous serons amenés à faire l'hypothèse - que nous considérons ici comme pire cas - que la vitesse du véhicule est constante et égale à la vitesse utilisée pour l'évaluation des critères de qualité : 100km/h.

Comme détaillé au paragraphe 5.1.2.2, les composants implantés au sein des systèmes embarqués dans l'automobile sont testés jusqu'à un niveau de champ n_c pour des fréquences données. Néanmoins, chaque zone au sein de laquelle le niveau de champ est supérieur à n_cV/m peut générer des erreurs au sein du système (voir figure 5.1).

On utilise alors l'hypothèse de vitesse constante sur l'ensemble du trajet pour déterminer la distribution des périodes passées dans des zones potentiellement perturbantes. Les erreurs n'étant susceptible de se produire que dans ces zones, nous considérons que l'action "pénétrer dans une zone perturbante" est une faute dont la durée correspond à la taille de la zone. La figure 5.2 est par conséquent notre *modèle de faute* pour le système.

[19] Dont la taille est inférieure à 1 micromètre.

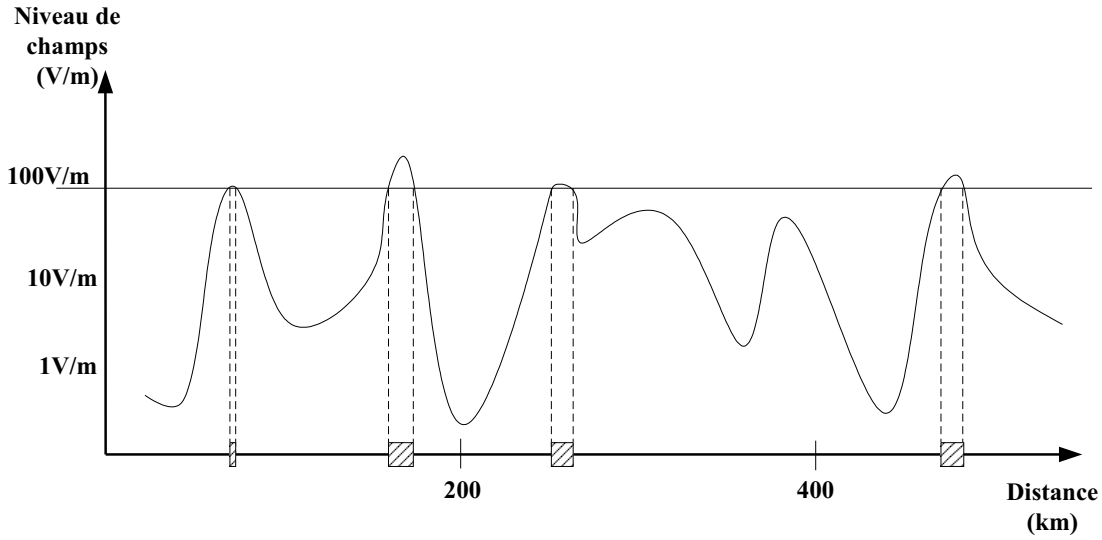

FIG. 5.1 – Extraction des zones dont le niveau de champs est supérieur à celui imposé en phase de test

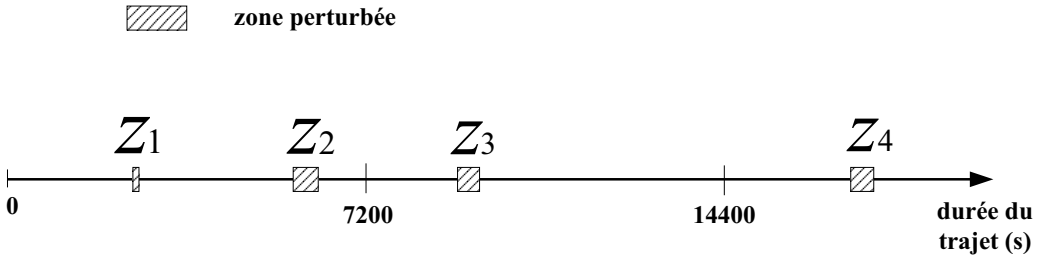

FIG. 5.2 – Distribution temporelle des zones dont le niveau de champs est supérieur à celui imposé en phase de test : *modèle de fautes*

5.2 De la faute transitoire à la défaillance de niveau véhicule

L'objectif de cette section est de montrer comment évaluer les occurrences de défaillances, considérées au niveau d'un véhicule, en fonction de défaillances d'un de ses systèmes embarqués. Pour ce faire, il est indispensable, dans un premier temps, de préciser quel est le système étudié (le véhicule, le système X-by-Wire, le réseau,....), puis, pour chaque système, quelles sont les fautes considérées, quelle est la durée pendant laquelle la faute affecte le système et sous quelles formes elles apparaissent au sein de ce système. Dans un deuxième temps, il s'agit d'identifier comment une faute donnée au niveau d'un système peut être causée par une ou des défaillances d'un autre système. Dans cette étude, comme nous nous préoccupons essentiellement de l'impact du système de communication sur la qualité d'un véhicule, nous considérons que :

– le système "véhicule" intégre et dépend du système embarqué étudié, par exemple du système "Steer-by-Wire",
– le système "Steer-by-Wire" intégre et dépend du système de communication.

5.2.1 Défaillance de niveau système

Nous analysons alors selon quelles régles, les fautes qui affectent le système de communication font qu'une défaillance est perçue au niveau du véhicule. Nous montrons le raisonnement suivi en prenant plusieurs hypothèses ; de plus, nous observons, pour illustrer le propos, uniquement le service σ_{FA} "entrainement de l'axe de direction en fonction de la consigne conducteur et de l'état du véhicule" et au niveau de ce service, nous considérons la consigne du conducteur sous la forme d'un signal *s* dont une instance est transmise dans un cycle de communication ; les hypothèses sont les suivantes :

1. les calculateurs sont silencieux sur défaillance ("fail-silent", voir paragraphe 6.1) (une valeur transmise et non erronée lors de sa transmission est supposée correcte),
2. le taux d'erreurs résiduelles des CRC est faible pour les protocoles de communication considéré dans un système "X-by-Wire" (TTP/C, FlexRay ou CAN ; pour le protocole de communication CAN, par exemple, il est indiqué que des erreurs multiples supérieures à 6 bits différents dans tout le contenu d'un message ne sont pas détectées avec une probabilité d'erreur résiduelle de 3×10^{-5}) et nous supposons qu'il est compensé par le fait que les consommateurs d'une instance de signal intégrent des algorithmes pour maintenir une cohérence des informations reçues (algorithmes reposant par exemple sur les dernières instances reçues),
3. la période d'activation de la loi de commande chargée de calculer les consignes pour l'entrainement de l'axe de direction est égale à un cycle de communication ; l'instance du signal est consommée par cette loi de commande, en début d'activation de la loi et à la fin du dernier slot contenant un réplica de ce signal à l'intérieur du cycle,
4. il suffit d'avoir un réplica correctement transmis dans un cycle pour considérer que la valeur de l'instance du signal reçue dans ce cycle est correcte.

Sous les deux premières hypothèses, on peut raisonnablement considérer, par la suite, que la *probabilité qu'une information erronée soit délivrée et reconnue correcte (erreur résiduelle non détectée par le CRC et non détectée par les algorithmes de cohérence) à un consommateur sur une suite de cycles est négligeable.*

De plus, pour faciliter le raisonnement, nous considérons des signaux pour lesquels la période de production (désignée par ε_t dans les chapitres précédents) des instances d'un signal est inférieure ou égale à la durée d'un

cycle de communication (ε_n) ; dans le cas où $\varepsilon_t > \varepsilon_n$, le raisonnement est un peu plus complexe puisque une même instance de signal est transmise dans plusieurs cycles consécutifs ; ce cas sera abordé au paragraphe 5.3.2.

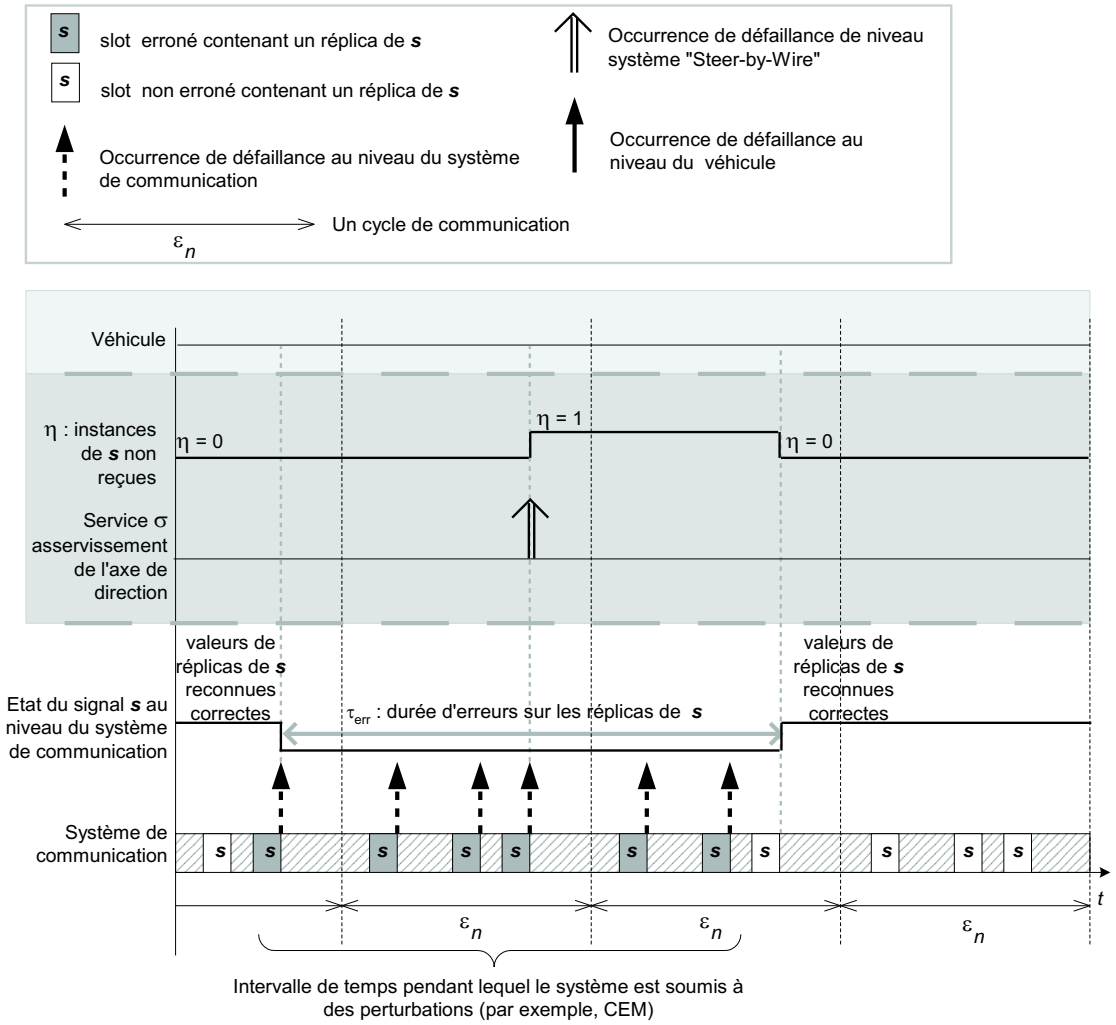

FIG. 5.3 – Propagation de fautes sans défaillance de niveau véhicule

De manière plus précise, nous définissons les niveaux suivants :

– Une faute au niveau du système de communication est un événement extérieur à ce système (par exemple, une perturbation électro-magnétique) qui peut affecter un slot de transmission contenant un réplica d'une instance du signal *s* ; l'occurrence de la défaillance se produira à la fin du slot "erroné" (détection de valeur erronée par le contrôleur de communication de la station réceptrice. On note par τ_{err} la durée pendant laquelle tout slot attribué au signal *s* est détecté incorrect (l'intervalle de durée τ_{err} commence toujours aprés un slot attribué à *s* et finit toujours aprés un slot attribué à *s*).

– Les défaillances du système de communication peuvent être considérées comme des fautes au niveau du système "Steer-by-Wire" ; ces fautes, sous l'hypothèse 4, peuvent être tolérées par ce système (redondance spatiale, par redondance de bus, et temporelle, par réplication de la même instance de signal dans plusieurs slots du cycle). Par contre, compte-tenu de l'hypothèse $\varepsilon_t \leq \varepsilon_n$, il faut que dans chaque cycle, la ou les

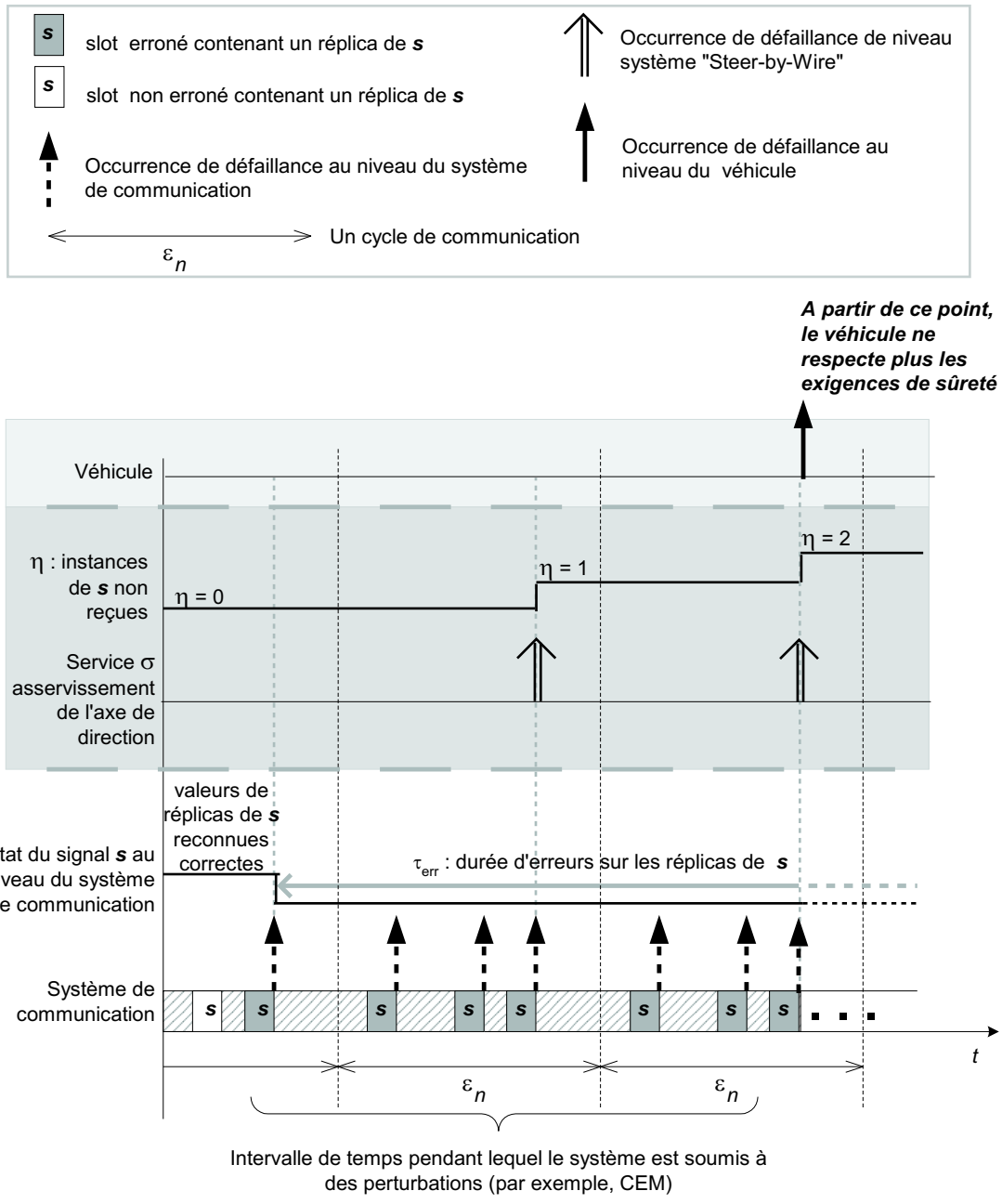

FIG. 5.4 – Propagation de fautes avec occurrence d'une défaillance au niveau du véhicule

stations réceptrices reçoivent au moins une valeur correcte du signal *s*. Il y aura occurrence d'une défaillance du système "Steer-by-Wire" chaque fois que, lors d'un cycle de communication, tous les slots attribués au signal *s* sont erronés. Cette défaillance ne peut se produire qu'à la fin du dernier slot contenant un réplica de s dans le cycle. On note η le nombre de cycles pendant lesquels tous les slots correspondants à *s* sont erronés.

– L'occurrence d'une défaillance du système "Steer-by-Wire" devient une faute au niveau du véhicule car, pour l'exécution concernée de la loi de commande, l'actionnement des moteurs d'entrainement de l'axe de direction se fait en fonction de valeurs non représentatives de l'état courant du système. Cependant, compte-tenu de la robustesse intrinsèque aux lois de commande embarquées, cette faute peut ne pas conduire à une situation telle qu'elle affecte la sécurité des occupants du véhicule et de son environnement. Intuitivement, il faudra certainement plusieurs fautes consécutives pour que le véhicule ne soit plus sûr. La défaillance au niveau du véhicule dépendra donc du nombre η de "cycles perdus".

Les figures 5.3 et 5.4 illustrent les dépendances introduites ci-dessus dans le cas où on ne considère qu'un bus et où le signal *s* est répliqué 3 fois dans chaque cycle. Pour simplifier, nous considérons que $\varepsilon_t = \varepsilon_n$, ainsi une instance du signal *s* est transmise à chaque cycle de communication. Nous supposons dans cet exemple que la sûreté du véhicule n'est plus assurée dés qu'un cycle de communication est perdu, soit η doit être tel que $\eta \leq 1$. Dans le scénario présenté en figure 5.3, la perturbation affecte le dernier slot du premier cycle (partiellement représenté sur la figure), puis tous les slots du cycle suivant et enfin, seulement les deux premiers slots du 3ème cycle. Aussi, il y a défaillance au niveau du système "Steer-by-Wire" à la fin du dernier slot attribué à *s* dans le deuxième cycle. Le nombre de cycles perdus est 1. Sur l'intervalle de temps présenté, il n'y a pas de défaillance au niveau du véhicule. Par contre, à la figure 5.4, la zone perturbée s'étend dans le temps et affecte le dernier slot du premier cycle (partiellement représenté) puis tous les slots des cycles 2 et 3. Deux occurrences de défaillances se produisent au niveau du système "Steer-by-Wire" (fin du dernier slot du cycle 2 et fin du dernier slot du cycle 3). Le nombre de cycles perdus est 2 et est, donc, supérieur à la valeur tolérable. Il y a défaillance au niveau du véhicule en fin du dernier slot attribué au signal *s* dans le troisième cycle.

En suivant un raisonnement similaire à celui employé dans le chapitre précédent, nous partons de la défaillance au niveau d'un véhicule et identifions, dans la section suivante, les conditions au niveau du système "Steer-by-Wire" et de son système de communication qui conduisent à cette défaillance.

5.2.2 Evaluation de la défaillance de niveau véhicule

Nous reposons cette évaluation sur la même approche que celle vue dans le chapitre précédent en appliquant également une technique d'injection de fautes. Nous considérons un véhicule dans les deux situations de vie considérées et présentées au chapitre 4 : l'inscription en courbe et le sinus balayé. Nous avons donc modélisé le service σ "entrainement de l'axe de direction en fonction de la consigne conducteur et de l'état du véhicule" sous Matlab / Simulink ; nous l'exécutons dans l'environnement SimulinkCar qui, comme nous l'avions mentionné, permet de calculer la valeur de certains paramètres (T_p, $V_{0,9R}$, $T_{0,9R}$,R_L, G_{mes}, N_g et E_V). Le modèle prend en compte un retard pur, τ, calculé en mode nominal et donc tel que $\tau < \tau_{max}$ (voir chapitre 4). Par contre, ce modèle introduit, dans ce contexte d'évaluation en mode perturbé, la possibilité pour la loi de commande de ne pas recevoir les consignes du conducteur à chacune de ses activations. Une consigne absente correspond à la perte de tous les slots attribués au signal "consigne conducteur" dans un cycle ; nous appellerons cette situation "perte d'un cycle de communication". En se fondant sur l'expérience chez PSA Peugeot-Citroën, le modèle implante la stratégie selon laquelle, si une valeur de signal n'est pas présente, c'est la valeur consommée à la précédente exécution de la loi

qui est utilisée. De plus, ce modèle part d'un profil de trajectoire, statiquement défini a priori et ne modélise pas le comportement d'un conducteur lors d'un essai (pas de corrections de la trajectoire en ligne).

L'objectif, dans un premier temps, est de déterminer le "pattern d'erreurs", c'est-à-dire la répartition des cycles perdus lors de l'exécution du modèle qui aura le plus d'influence sur le comportement du véhicule. Une série de simulations a montré que le "pattern d'erreurs" le plus dimensionnant est l'erreur continue, c'est-à-dire la perte de cycles consécutifs. Le terme "dimensionnant" signifie celui qui place le véhicule dans le pire cas. En fait, lors des simulations, on a pu observer que, si le véhicule est dans un état sûr (pas encore d'occurrence de défaillance), une seule consigne reçue correctement par la loi de commande suffit pour réaliser un actionnement correct. Nous avons donc choisi de déterminer la plus petite suite de cycles consécutifs perdus conduisant à une défaillance.

Pour chaque situation de vie, nous faisons une série de simulations en faisant varier deux paramètres :

- l'instant t à partir de t_0 et par incrément de ε_n (seule possibilité fournie par le simulateur), qui désigne la date de la première instance de signal qui n'est pas reçue par la loi de commande ; t_0 est relative à la date initiale d'observation $t_{observation}$ ($t_0 \geq t_{observation}$) définie pour chaque type d'essai (inscription en courbe ou sinus balayé) ; compte-tenu de la structure du simulateur, t peut être interprétée comme la date de fin du dernier slot attribué à s dans un cycle,
- la durée δ, à partir de cet instant t pendant laquelle la loi de commande ne reçoit aucune instance du signal ; cette durée est égale à ε_n, $2\varepsilon_n$, ... pour représenter la perte d'une suite de cycles consécutifs, soit de tous les slots attribués au signal dans chacun de ces cycles ; le nombre de cycles perdus est noté η ($\eta = \frac{\delta}{\varepsilon_n}$).

On obtient, pour chaque simulation i (t^i, δ^i), la "*note de calage*" $Calage^i$ (respectivement, la "*note de réponse / précision*" $Reponse\_Precision^i$) obtenue par application de la fonction $Q_{inscription-courbe}$ (respectivement, $Q_{sinus-balaye}$) ainsi que la valeur de l'écart de trajectoire E_V^i. On obtient ainsi :

- la plus grande "*note de calage*" $Calage_{max}$ telle que $Calage_{max} > Calage_{min}$; cette note pouvant correspondre à plusieurs couples (t^i, δ^i), on construit le sous-ensemble E_{Calage} contenant tous les couples (t^i, δ^i) conduisant à $Calage_{max}$; on définit alors $\delta_{max,Calage}$ comme le plus petit des δ^i de l'ensemble E_{Calage}. Soit $\delta_{max,Calage} = min_{(t^i,\delta^i)\in E_{Calage}}(\delta^i)$.
- la plus grande "*note de réponse / précision*" $Reponse\_Precision_{max}$ telle que $Reponse\_Precision_{max} > Reponse\_Precision_{min}$; on construit le sous-ensemble $E_{Reponse\_Precision}$ contenant tous les couples (t^i, δ^i) conduisant à $Reponse\_Precision_{max}$; le plus petit des δ^i de l'ensemble $E_{Reponse\_Precision}$ est $\delta_{max,Reponse\_Precision}$. Soit $\delta_{max,Reponse\_Precision} = min_{(t^i,\delta^i)\in E_{Reponse\_Precision}}(\delta^i)$.
- enfin, le plus grand écart de trajectoire admissible EV_{max}tel que $EV_{max} > EV_{min}$; on construit le sous-ensemble $E_{Ecart\_Trajectoire}$ contenant tous les couples (t^i, δ^i) conduisant à la valeur EV_{max} ;
  $\delta_{max,Ecart\_Trajectoire}$ est le plus petit des δ^i de l'ensemble $E_{Ecart\_Trajectoire}$.
  Soit $\delta_{max,Ecart\_Trajectoire} = min_{(t^i,\delta^i)\in E_{Ecart\_Trajectoire}}(\delta^i)$.

Il est important de noter que nous faisons l'hypothèse que *les critères de qualité utilisés en mode nominal sont valables en mode perturbé*. En effet, au moment de la rédaction du document, aucune information nous permettant de répertorier les situations de vie considérées comme des situations pire cas n'était disponible chez PSA Peugeot Citroën. La proposition de critères propres au mode perturbé est un des axes forts des travaux à venir (voir conclusions générales de la partie 2).

Le plus grand intervalle entre deux consommations valides d'instances d'un signal est δ_{max} défini par :

$$\delta_{max} = min(\delta_{max,Calage}, \delta_{max,Reponse\_Precision}, \delta_{max,Ecart\_Trajectoire})$$

et correspond à un nombre maximal tolérable de cycles perdus $\eta_{max} = \frac{\delta_{max}}{\varepsilon_n}$.

Dans l'exemple illustré aux figures 5.3 et 5.4, nous avions supposé $\eta_{max} = 1$.

On appelle alors défaillance de niveau système une situation telle qu'elle puisse avoir pour conséquence une défaillance de niveau véhicule ; dans le cas où $\varepsilon_t \leq \varepsilon_n$, il s'agit de toute situation où l'intervalle d entre deux consommations valides d'une instance de signal soit telle que $\left(\left\lceil \frac{\tau_{err}}{\varepsilon_n} \right\rceil\right) > \eta_{max}$.

5.2.3 Retour d'effort au volant

Ce service est aussi critique que le pilotage de la crémaillère, mais s'étudie différemment. En effet, les informations transitant sur le réseau ne sont pas nécessaires pour fournir un retour d'effort minimal, d'autant plus qu'un mode dégradé mécanique (ressort, frottements divers...) peut être utilisé en cas de perte totale du service. Par contre, en cas de perte totale du service de pilotage de la crémaillère, cette forme de mode dégradé n'est pas implémentable - sinon il faudrait ajouter une colonne de direction -. Le retour d'effort est essentiellement construit à partir de grandeurs véhicules telles que la vitesse longitudinale ou la vitesse de lacet. La multitude des stratégies disponibles pour proposer un mode dégradé minimal ne mettant pas en cause la sécurité du conducteur nous amènent à penser que les fautes transitoires peuvent être aisément tolérées. C'est pourquoi nous n'étudions pas l'influence des fautes transitoires liées à l'environnement sur ce service dans le présent document.

5.3 Evaluation du nombre maximal de cycles de communication perdus en présence d'une perturbation

Dans la section 5.2.2 nous avons montré qu'une perturbation d'une certaine durée Z peut entraîner la perte consécutive des instances de signal pour le consommateur (calculateur de loi de commande et actionneur), η_{max} est alors donné comme le nombre maximal de cycles de consomation (ou de communication) perdus consécutivement, tolérable au niveau de véhicule. **L'objectif de cette section consiste à évaluer le nombre maximal (pire cas) de cycles de communication (de durée ε_n) perdus, noté par $\eta_{WC}(Z)$, en présence d'une perturbation de durée Z.** Nous faisons l'hypothèse qu'une perturbation à l'instant *t* entraîne systématiquement soit une erreur de slot de communication, soit une erreur de production si la communication ou la production a lieu à l'instant *t*. On verra par la suite comment cette hypothèse sera relachée pour tenir compte de l'apport de la redondance (temporelle et physique). En plus, nous rappelons les hypothèses suivantes sur le fonctionnement de notre système :

- hypothèse 1 : on attend toujours le début d'un nouveau cycle de communication pour transmettre des instances de signal mises à jour. C'est donc toujours la dernière mise à jour juste avant le début du cycle de communication qui est transmise.
- hypothèse 2 : les interarrivées des instances de signal au niveau de l'actionneur (i.e., calculateur de loi de commande) sont périodiques de période ε_n.
- hypothèse 3 : une seule instance de signal valide est suffisante du point du vue du consommateur.
- hypothèse 4 : une erreur ne peut affecter que la production et la transmission des instances des signaux.

Selon l'hypothèse 4, une perturbation peut affecter soit la production, soit la transmission (slot), nous étudions comme dans le chapitre 4 les deux cas : $(\varepsilon_t \leq \varepsilon_n)$ et $(\varepsilon_t > \varepsilon_n)$.

5.3.1 Cas 1 : période de production d'un signal inférieure ou égale à la durée d'un cycle de communication $(\varepsilon_t \leq \varepsilon_n)$

Dans ce cas, il y a une ou plusieurs productions par cycle de communication. Nous cherchons donc le pire placement d'une zone de perturbation de durée Z qui entraîne le nombre maximal de cycles de communication (consommation) perdus. Il est facile de constater que ce pire cas correspond à affecter tous les réplicas et toutes les productions du dernier cycle de communication à la fin de la zone perturbée. La figure 5.5 montre l'existence d'un tel pire cas pour lequel la transmission de 2 instances de signal est erronée (voir figure 5.5).

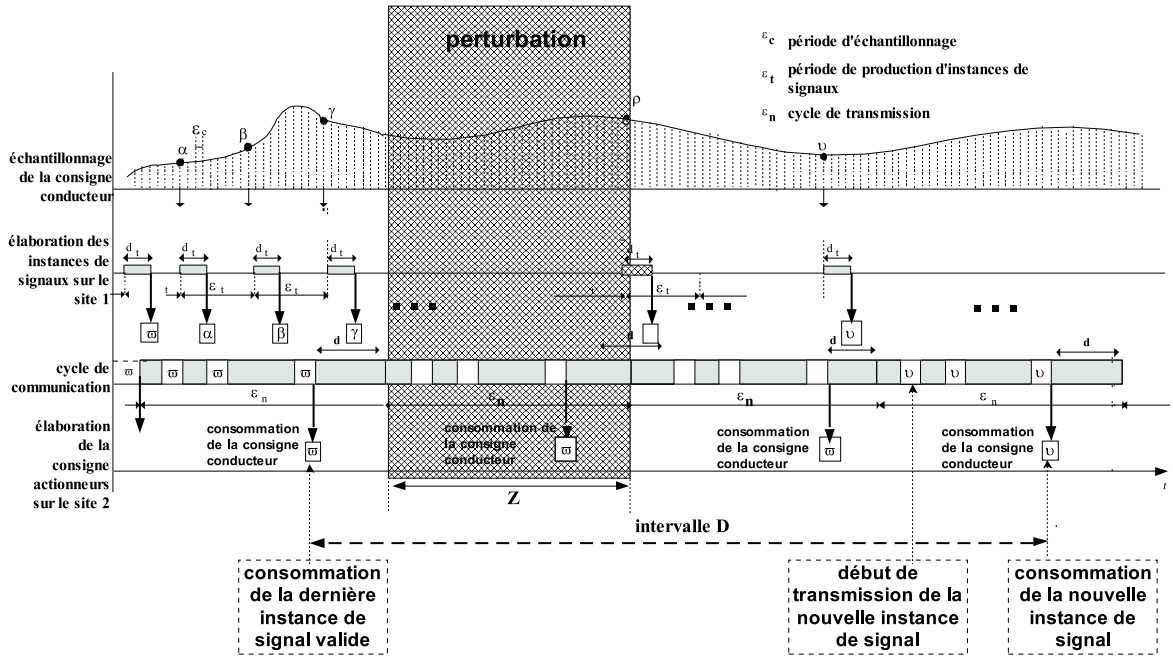

FIG. 5.5 – pire cas - la période de production d'un signal est inférieure à la durée d'un cycle et 2 instances de signal sont erronées

Selon l'hypothèse 1, il n'y a qu'une des productions (si ce n'est pas la dernière) du cycle de communication précédent qui peut être transmise pendant le cycle courant. Si le cycle précédent est complètement perturbé (toutes les transmissions et productions), il n'y aura pas de transmission au cycle courant et la première instance valide n'arrivera qu'au cycle suivant. Ce qui nous donne $\eta_{WC}(Z)$, le nombre maximal (pire cas) de cycles de communication de durée ε_n perdus :

$$\eta_{WC}(Z) = \left\lceil \frac{Z}{\varepsilon_n} \right\rceil + 2 \tag{5.1}$$

On prend toujours la partie entière supérieure qui correspond au nombre maximal de cycle de communication qu'une zone de durée Z peut perturber.

5.3.2 Cas 2 : période de production d'un signal supérieure à la durée d'un cycle de communication $(\varepsilon_t > \varepsilon_n)$

Ce cas est plus complexe à analyser que le cas précédent. En effet, dans ce cas, une perturbation à l'instant de production (i.e. une production perdue) entraînera la perte de plusieurs cycles de consommation (communication). L'évaluation de la relation entre une durée de perturbation Z et le nombre de cycles perdus dépendra de la couverture de la période perturbée (place du début et de la fin). Mais il existe un pire début (respectivement fin) qui entraîne la perte du nombre maximal de cycles de communication $\eta_{WC}(Z)$. En effet, pour la même durée de perturbation, 2 cas extrêmes peuvent se produire : le pire cas et le meilleur cas. Prenons l'exemple d'une durée de perturbation égale à ε_n :

– Pire cas : la transmission de 2 instances de signal est erronée (voir figure 5.6) :

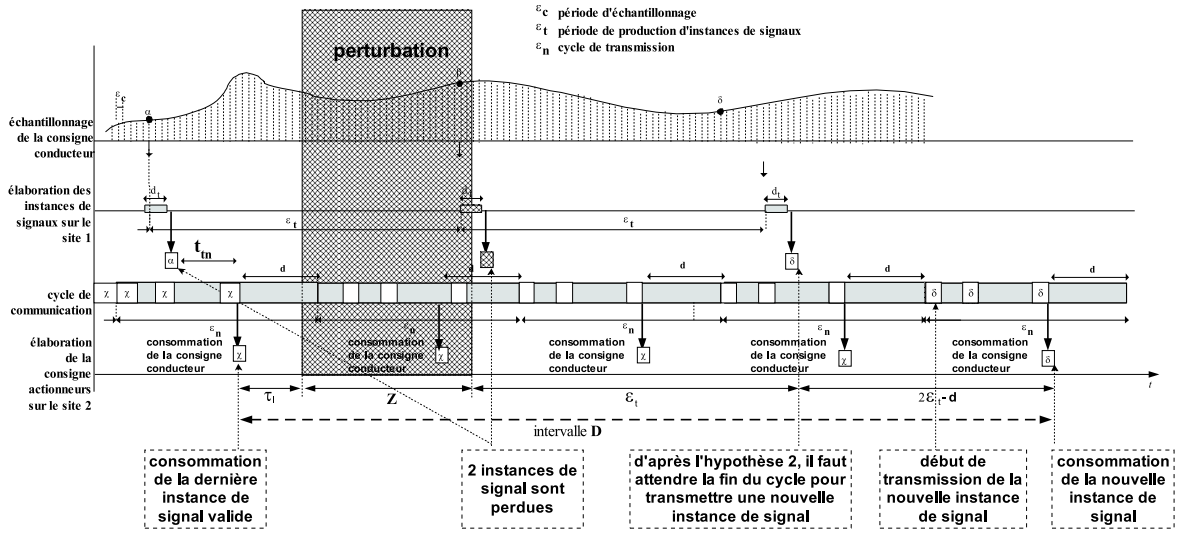

FIG. 5.6 – Pire cas - la période de production d'un signal est supérieure à la durée d'un cycle et 2 instances de signal sont erronées

Dans ce cas de figure, la perturbation affecte le dernier cycle de communication avant la prochaine production ainsi que la prochaine production (pire fin de période de perturbation). Etant donné que $\varepsilon_t > \varepsilon_n$, il n'y a pas d'arrivée des instances valides de signal durant $[0, \varepsilon_t]$, et la prochaine instance de signal valide devra attendre au pire $2\varepsilon_n - d$ pour être livrée à l'actionneur. En notant par D l'intervalle d'interarrivée de deux instances valides de signal, et τ_l l'intervalle de temps entre la dernière instance valide et le début de la perturbation, on peut donc écrire :

$$D = \tau_l + Z + \varepsilon_t + (2\varepsilon_n - d)$$

– Meilleur cas : aucune instance de signal n'est erronée (voir figure 5.7) :

Dans ce dernier cas de figure, une perturbation n'a entraîné aucune erreur au niveau du service car les erreurs au niveau des slots sont tolérées grâce à la redondance temporelle (réplicas).

En conclusion, si l'on désire avoir une approche "pire cas", il faudra considérer le pire cas en maximisant D. τ_l dépend du placement du premier réplica du signal considéré à l'intérieur d'un cycle de communication, τ_l et d sont liés de la façon suivante. Si l'on désigne par l la distance (intervalle de temps) entre le début du premier réplica et

la fin du dernier réplica d'un signal, on a $\varepsilon_n = \tau_l + l + d$. On peut alors réécrire l'expression de D :

$$D = \tau_l + Z + \varepsilon_t + 2\varepsilon_n - (\varepsilon_n - \tau_l - l) = 2\tau_l + Z + \varepsilon_t + \varepsilon_n + l$$

Le maximum est obtenu avec $\tau_l = \varepsilon_n - l$ (ou autrement dit quand $d = 0$). On peut alors donner la formule du pire temps d'interarrivée D_{WC} pour le cas 2 :

$$D_{WC} = Z + \varepsilon_t + 3\varepsilon_n - l$$

On peut discrétiser D_{WC} en fonction du nombre η_{WC} de cycles de communication de durée ε_n perdus qui correspond au rapport entre D_{WC} et la durée d'un cycle de communication ε_n :

$$\eta_{WC}(Z) = \left\lceil \frac{Z + \varepsilon_t + 3\varepsilon_n - l}{\varepsilon_n} \right\rceil \tag{5.2}$$

Bien que, par définition, D_{WC} soit toujours le multiple de ε_n, nous prenons par précaution la partie entière supérieure car aucune information n'étant disponible sur le placement des messages répliqués au sein du cycle, il est impossible de savoir le nombre d'instances du même signal touchées par une perturbation de durée inférieure à un cycle de communication.

Remarque : en absence d'information sur l, nous pouvons aussi majorer le pire cas en supposant que $l = 0$.

On peut finalement écrire :

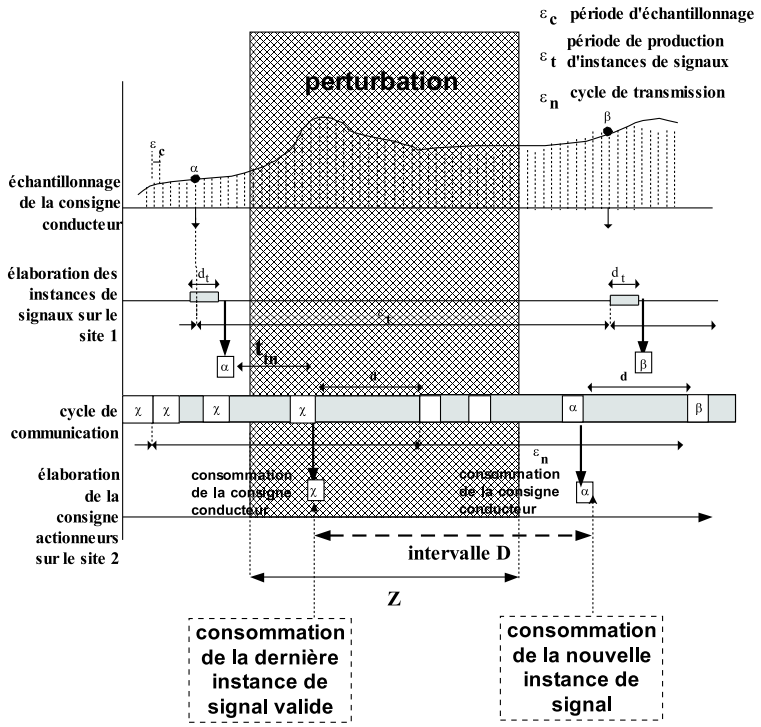

FIG. 5.7 – Meilleur cas - la période de production d'un signal est supérieure à la durée d'un cycle et aucune instance de signal n'est erronée

$$\eta_{WC}(Z) = \begin{cases} \left\lceil \frac{Z}{\varepsilon_n} \right\rceil + 2 \; si \; \varepsilon_t \leq \varepsilon_n \\ \left\lceil \frac{Z+\varepsilon_t+3\varepsilon_n-l}{\varepsilon_n} \right\rceil \; si \; \varepsilon_t > \varepsilon_n \end{cases} \tag{5.3}$$

5.4 Influence de la redondance et modèle d'erreur

Dans les paragraphes précédents, nous avons fait l'hypothèse que, dans une zone perturbée, toutes les instances de signal transmises étaient inéluctablement perdues. Or, la diversité des perturbations électromagnétiques rencontrées et la diversité des méthodes de conception des systèmes, notamment en terme de redondance des composants et des informations transmises au sein du système, nous incitent plutôt à émettre une probabilité sur les occurrences de la perte d'une ou plusieurs instances de signal. Or, d'après l'hypothèse 3 du paragraphe 5.3, on sait qu'une seule instance de signal valide est suffisante du point du vue du consommateur. Ce paragraphe a pour objectif la quantification de la probabilité de perdre toutes les instances du même signal, et donc tous les messages répliqués (donc un cycle de communication si l'on est dans le cas $\varepsilon_n > \varepsilon_t$, voir paragraphe 5.3.1)[20]. Nous nous focalisons uniquement sur l'état de toutes les instances de signal transmises au sein de tous les messages répliqués, du point de vue du consommmateur de l'information. Ainsi, nous ne tenons pas compte de l'état du composant à la source de l'erreur, mais uniquement de l'état de tous les messages répliqués au niveau du consommateur.

5.4.1 La réplication de messages

Comme détaillé au paragraphe 4.3.2, on désigne par "message" un exemplaire d'une instance de signal dans un cycle. Par conséquent, on désignera par "messages répliqués" l'ensemble des messages transportant la même instance de signal (échantillon). La figure 5.8 nous montre un exemple de 4 messages répliqués transmis par 2 ECUs (A et B) sur 2 canaux différents dans un cycle de communication donné.

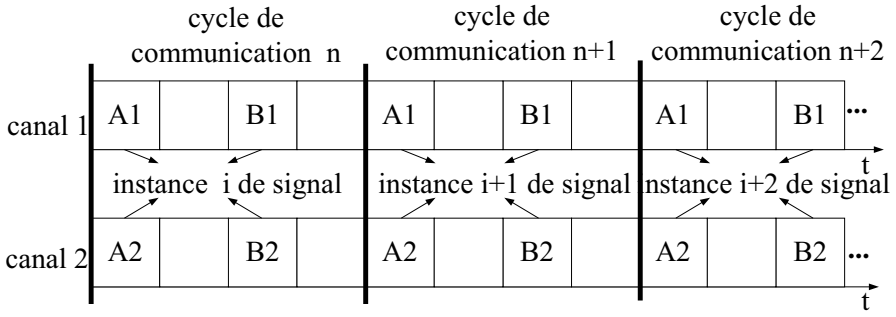

FIG. 5.8 – Exemple : 4 messages répliqués de la même instance de signal S (A1, A2 transmis par l'ECU A ; B1, B2 transmis par l'ECU B) transmis par 2 ECUs (A et B) sur 2 canaux différents dans un cycle de communication donné

On fait l'hypothèse que, du point de vue du consommateur de l'information, la délivrance correcte d'un seul message parmi les messages répliqués suffit pour que le service ne subisse aucune dégradation. Ainsi, si une faute n'affecte qu'une partie de l'ensemble des messages répliqués et qu'il en reste au moins un correct, la faute est tolérée par le système. C'est pourquoi nous considérons qu'une *erreur* correspond à l'événement "perdre tous les

[20] Il est important de noter que cette probabilité n'est pas une probabilité d'occurrence par heure, mais une probabilité brute en cas de perturbation.

messages répliqués". La figure 5.9 illustre cet événement pour l'exemple de la figure 5.8 avec $\varepsilon_t > \varepsilon_n$; On fait l'hypothèse que les ECUs sont fail-silent (voir paragraphe 6.1) dans le domaine des valeurs. Une faute n'entrainera donc pas d'arrivée de messages erroné non détecté au niveau du consommateur.

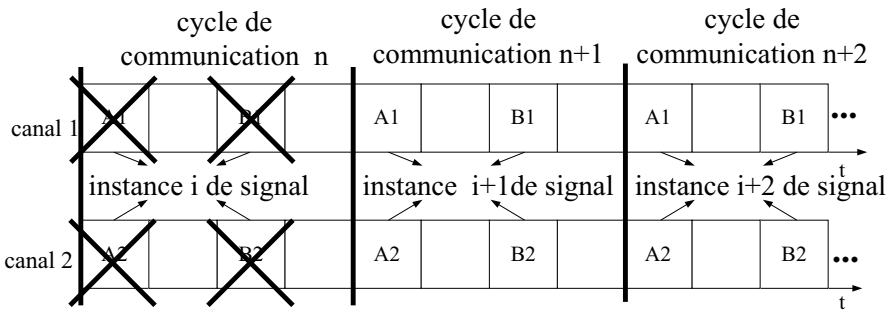

FIG. 5.9 – perte de tous les messages répliqués de la même instance de signal S

5.4.2 Récupération de la probabilité de perdre tous les messages répliqués

La probabilité P_{err} de perdre tous les messages répliqués en cas de perturbation peut être obtenue de plusieurs manières :

- Retour d'expérience fournisseur
- Modélisation analytique
- Injection de fautes (voir paragraphe 2.2.2 pour plus d'informations sur l'injection de faute)

L'injection de faute peut être réalisée sur modèle ou directement sur le système physique.

5.4.2.1 Evaluation de P_{err} par injection de faute

Cette technique peut être réalisée sur des modèles du système à n'importe quelle phase (récupération des statistiques, quantification, test, ...) dans le protocole du réalisation du modèle d'erreur. Plusieurs approches sont disponibles pour obtenir une probabilité de perdre tous les messages répliqués. Celles-ci sont présentées au paragraphe 2.2.2.

5.4.2.2 Evaluation de P_{err} sur un trajet de référence

Cette technique est plus complexe à mettre en oeuvre, mais les résultats obtenus sont plus proches de la réalité. Il s'agit de tester à nouveau le système dans les conditions correspondant aux perturbations auxquelles il a été confronté durant le trajet de référence. Deux approches peuvent alors être proposées :

1. Approche pire cas : on teste le système dans une chambre anéchoidique au sein de laquelle le système sera soumis au pire niveau de champ rencontré pendant le trajet de référence.
2. Approche cas moyen : on teste le système en faisant varier le niveau de champ en fonction des résultats obtenus sur le trajet de référence.

5.4.2.3 Proposition de formule approchée d'évaluation de P_{err}

Nous considérons, ici, qu'un système est formé de composants qui sont les ECUs, les capteurs, les actionneurs et les réseaux. Dans le cas où un composant (par exemple, un ECU) est redondé, si une rafale d'erreur affecte ce composant, elle n'impactera pas forcément toutes ses redondances, notamment si celles-ci sont diversifiées. On peut affirmer que, si 2 composants identiques sont placés exactement au même endroit dans le véhicule, si une perturbation entraîne une défaillance sur un des composants, elle entraînera une défaillance sur le second (les événements ne sont pas indépendants). Plus les composants sont diversifiés et éloignés, plus les rafales d'erreurs impactant des composants pourront être considérées comme des événements indépendants. On appelle λ la probabilité de défaillance d'un composant (notons que la défaillance d'un composant est perçue, dans le contexte de ce travail, comme la perte de message au sein d'un cycle de communication). L'objectif est alors de chercher, à partir de λ, la probabilité P_{err} de perdre tous les messages répliqués (mode commun).

Plusieurs critères peuvent agir sur la probabilité de défaillance commune. L'idée est de fixer une note N_R ($N_R \leq 1$) pour la qualité de chaque critère servant l'indépendance des composants. Plus la qualité de la diversité serait élevée, plus N_R serait proche de 1. Nous proposons, ici, de ne considérer que les ECUs producteurs de messages et le canal de communication. Le tableau 5.10 peut permettre de calculer N_R à partir de critères de diversification primordiaux :

Sous-système	**Nombre de composants redondants**	**Critère de diversification**	**Qualité de la diversification (notée sur 10)**	**Note de diversification**
ECU producteur	n_{ECU}	fournisseur	c_{f_ECU}	$N_{R\_ECU} = \frac{c_{f\_ECU}+c_{t\_ECU}+c_{e\_ECU}}{30}$
		technologie	c_{t_ECU}	
		éloignement physique	c_{e_ECU}	
Canal de communication	n_{BUS}	technologie	c_{t_BUS}	$N_{R\_BUS} = \frac{c_{t\_BUS}+c_{e\_BUS}}{20}$
		éloignement physique	c_{e_BUS}	

FIG. 5.10 – Tableau d'évaluation de critères pour la note de diversification N_R

Sachant que, pour une redondance double d'un composant étudié i, P_{err_i} varie entre λ_i et ${\lambda_i}^2$, on propose la formule suivant pour la quantification de P_{err_i} :

$$P_{err_i} = \lambda_i - N_{Ri}(\lambda_i - \lambda_i^2)$$

que nous généralisons en cas de redondance d'ordre n :

$$P_{err_i} = \lambda_i - N_{Ri}(\lambda_i - \lambda_i^n) \tag{5.4}$$

On propose alors de généraliser la formule à des composants redondés n fois. Considérons un système comportant un ECU, producteur de messages, redondé (ECU) et un canal de communication également redondé (BUS). Nous supposons, dans cet exemple, que le taux de défaillance des capteurs est de $\lambda = 0$. De plus, pour l'étude qui nous intéresse (évaluation de la probabilité de perdre des cycles de communication), le taux de défaillance des

ECUs consommateurs de message peut être pris à 0. Ainsi, nous disposons de :

$$P_{err_{ECU}} = \lambda_{ECU} - N_{R_{ECU}}(\lambda_{ECU} - \lambda_{ECU}^2)$$

$$P_{err_{BUS}} = \lambda_{BUS} - N_{R_{BUS}}(\lambda_{BUS} - \lambda_{BUS}^2)$$

Ce qui donne pour le système :

$$P_{err} = P_{err_{ECU}} + P_{err_{BUS}} - P_{err_{ECU \cap BUS}} \tag{5.5}$$

Remarque : il est important de noter que cette méthode analytique n'apporte aucune preuve quant à la quantification exacte de P_{err}, mais permet seulement de donner une approximation intuitivement réaliste. Pour une évaluation exacte de P_{err}, le lecteur pourra se référer au paragraphe 5.4.2.2.

5.5 Fiabilité comportementale et métriques associées

Dans les sections suivantes, nous établissons les formules nécessaires pour le calcul de la probabilité d'occurence des défaillances, dans un premier temps pour une zone perturbée de durée Z (avec $\eta_{WC}(Z) > \eta_{max}$) au sein de laquelle la probabilité de perdre un cycle est P_{err}, puis pour un trajet suivi par un véhicule traversant une suite de r zones perturbées Z_i (avec $\eta_{WC}(Z_i) > \eta_{max}$ et $i = 1, 2, ..., r$).

5.5.1 Défi nition de la Fiabilité Comportementale

Définition : on appelle fiabilité comportementale l'aptitude du système à assurer un service en prenant en compte la dynamique de l'application embarquée (performances temporelles, tolérances aux défaillances).

Une des mesures de cette fiabilité comportementale est la "probabilité d'occurrence d'une défaillance de niveau véhicule au sein d'une zone perturbée", c'est-à-dire la probabilité d'avoir plus de η_{max} cycles consécutifs perdus pendant la traversée d'une zone Z donnée de perturbations pouvant affecter au plus $\eta_{WC}(Z)$ cycles.

Une autre mesure est la "probabilité d'occurrence d'une défaillance de niveau véhicule au cours d'un trajet", c'est-à-dire la probabilité d'avoir plus de η_{max} cycles consécutifs perdus pendant la traversée de l'ensemble des r zones de perturbations Z_i données pouvant affecter, chacune, au plus $\eta_{WC}(Z_i)$ cycles.

5.5.2 Probabilité d'occurrence des défaillances dans une zone perturbée

On note par $Pd(Z, P_{err})$ la probabilité de défaillance du véhicule dans une zone perturbée de durée Z (avec $\eta_{WC}(Z) > \eta_{max}$) au sein de laquelle la probabilité de perdre un cycle est P_{err}. Comme nous avons déjà montré, dans le pire cas, cette zone peut perturber jusqu'à $\eta_{WC}(Z)$ cycles de communication (ou consommation). Compte tenu que $P_{err} < 1$, la probabilité $Pd(Z, P_{err})$ correspond à celle de perdre plus de η_{max} cycles de communication consécutifs parmi $\eta_{WC}(Z)$. Supposons que la perte d'un cycle est un événement indépendant de ce qui se passe sur des cycles adjacents, posons $k = \eta_{max} + 1$ et $n = \eta_{WC}(Z)$, le calcul de $Pd(Z, P_{err})$ revient à déterminer la probabilité d'avoir au moins k cycles consécutifs perdus dans une suite de n épreuves de Bernoulli indépendantes. C'est un probème étudié depuis fort longtemps et qui a fait l'objet d'une littérature considérable, notamment pour son intétêt dans l'étude de la fiabilité des systèmes connus sous le nom de systèmes "consecutive-k-out-of-n :F" et notés par C(k,n :F), (voir dans [27] pour une synthèse).

On note par L_n la plus longue suite de cycles consécutifs perdus et p (=P_{err}) la probabilité de perdre un cycle. La fiabilité d'un système C(k,n :F), notée par $R(k,n;p) = P(L_n < k)$, a été pour la première fois présentée dans [20], puis simplifiée par [68] et [51]. La formule proposée est la suivante $(q = 1 - p)$:

$$R(k,n;p) = \sum_{m=0}^{\lfloor (n+1)/(k+1) \rfloor} (-1)^m p^{mk} q^{m-1} \left(\begin{pmatrix} n-mk \\ m-1 \end{pmatrix} + q \begin{pmatrix} n-mk \\ m \end{pmatrix} \right) \tag{5.6}$$

Ainsi la probabilité de défaillance du véhicule dans une zone perturbée de durée Z est donnée par :

$$Pd(Z, P_{err}) = 1 - R(\eta_{max} + 1, \eta_{WC}(Z); P_{err}) \tag{5.7}$$

Cependant, il est connu que le temps d'éxecution de la fomule précédente augmente rapidement avec n et k, rendant ainsi peu pratique son exploitation. Face à ce problème, il existe en général deux pistes : proposer des bornes ou trouver une relation de récurrrence premettant de réduire la complexité algorithmique du calcul exact. A notre grande surprise, il existe peu de travaux sur la deuxième piste alors que de nombreux travaux ont été menés suivant la première piste. Par exemple, Muselli a proposé dans [80] des bornes sur ce résultat (déjà étudiée dans [39]) :

$$(1 - p^k)^{n-k+1} \leq R(k,n;p) \leq (1 - qp^k)^{n-k+1}$$

Nous pouvons appliquer directement ces bornes pour l'évaluation de notre $Pd(Z, P_{err})$. Comme par définition :$Pd(Z, P_{err}) = 1 - R(\eta_{max} + 1, \eta_{WC}(Z); P)$, et on ne s'intéresse qu'à la borne supérieure de cette probabilité, on a donc :

$$Pd(Z, P_{err}) \leq 1 - (1 - P_{err}^{(\eta_{max}+1)})^{\eta_{WC}(Z)} \tag{5.8}$$

La deuxième piste a été exploité dans [Rapport de F.Simonot (Institut Elie Cartan - Nancy) en cours de finalisation]. Le point clé pour trouver la relation de récurrence est l'introduction d'une variable aléatoire $T_{k,r}$ qui représente le premier instant où on obtient le *r*ème suite de cycles consécutifs perdus de taille $L_n \geq k$.

Pour la commodité, nous définissons également une variable aléatoire M_n^k qui est le nombre de mots de taille $\geq k$ au cours de *n* épeuves de Bernoulli indépendantes (i.e. *n* cycles), deux mots différents devant être séparés par au moins un cycle correct. Notons par 1 un cycle perdu et 0 un cycle correct.

Exemple 1 : 010111011 donne deux mots de taille ≥ 2 ; 011110000 donne un seul mot de taille≥ 2 et non pas trois.

T_k est le premier instant où on obtient un mot de taille $\geq k$.

Exemple 2 : *k = 3*, dans la suite 010111101, $T_3 = 6$; *k* = 4, dans la suite 11101111111, $T_3 = 8$.

Exemple 3 : *k = 3*, *r = 2*, dans la suite 01011101110, $T_{3,2} = 10$.

On a évidemment $T_{k,1} = T_k$ pour tout $k \geq 1$, et on notera que les $T_{k,r}$ sont des temps d'arrêt. Entre T_k , $T_{k,r}$, L_n et M_n^k on a les relations simples suivantes :

$$P(T_{k,r} \leq n) = P(M_n^k \geq r) \; pour \; r \geq 1 \tag{5.9}$$

En particulier si *r = 1*, on a :

$$P(T_k \leq n) = P(M_n^k \geq 1) = P(L_n \geq k) \tag{5.10}$$

On suppose *k* fixé, $k \geq 1$, la relation 5.9 donne immédiatement :

$$P(T_{k,r} = n) = P(M_n^k \geq r) - P(M_{n-1}^k \geq r) \; pour \; tout \; r \geq 1$$

or on peut constater que

si $r \geq 2$, on a :

$$P(T_{k,r} = n) = qp^k P(M_{n-k-1}^k = r-1) \; pour \; n \geq k+2 \tag{5.11}$$

$$P(T_{k,r} = n) = 0 \; pour \; 0 \leq n \leq k+1 \tag{5.12}$$

si $r = 1$, la situation est légèrement différente, on a :

$$P(T_{k,1} = n) = qp^k P(M_{n-k-1}^k = 0) \; pour \; n \geq k+2 \tag{5.13}$$

$$P(T_{k,1} = k+1) = qp^k \tag{5.14}$$

$$P(T_{k,1} = k) = p^k \tag{5.15}$$

on en déduit donc :

$$P(T_{k,r} = n) - P(T_{k,r+1} = n) = P(M_n^k = r) - P(M_{n-1}^k = r) = qp^k[P(M_{n-k-1}^k = r-1) - P(M_{n-k-1}^k = r)]$$

ce qui fournit finalement la récurrence linéaire par rapport à n :

$$P(M_{n+1}^k = r) = P(M_n^k = r) + qp^k[P(M_{n-k}^k = r-1) - P(M_{n-k}^k = r)] \tag{5.16}$$

Pour simplifier la notation, on écrira $V_r^n = P(M_n^k = r)$(*k* est supposé fixé), la relation 5.16 devient :

$$V_r^{n+1} = V_r^n - qp^k V_r^{n-k} + qp^k V_{r-1}^{n-k} \tag{5.17}$$

Pour démarrer la récurrence il faut connaître :
i) $V_0^m = P(M_m^k = 0) = P(L_m \leq k-1)$
ii) $V_r^m = P(M_m^k = r)$ pour $r \geq 1$ et $0 \leq m \leq k$
V_0^m se calcule par récurrence, car d'après 5.10, on a :
$P(T_k = n) = P(L_{n-1} \leq k-1) - P(L_n \leq k-1) = qp^k P(L_{n-k-1} \leq k-1)$, soit

$$V_0^{n+1} = V_0^n - qp^k V_0^{n-k} \; avec \; n \geq k \tag{5.18}$$

Les conditions initiales de $V_r^m = P(M_m^k = r)$ pour $r \geq 1$ et $0 \leq m \leq k$ se calculent directement sans effort : $V_r^m = 0$ si $r \geq 2$ et $0 \leq m \leq k$; $V_1^m = 0$ si $0 \leq m \leq k$ et $V_1^k = p^k$.

Ainsi les relations 5.17 et 5.18 permettent de calculer facilement et rapidement $P(M_n^k = r)$ pour tous $k \geq 1$ et $r \geq 0$ et en particulier la fonction de répartition de L_n et aussi $P(T_{k,r} = n)$, $r \geq 1$, en utilisant les relations 5.11 - 5.15.

L'algorithme suivant permet le calcul de la distribution de probabilité de L_n. En effet, selon 5.18 et 5.6 , si l'on note par $u_k(n) = P(L_n \leq k-1) = R(k, n; p)$, on peut écrire :

$$u_k(n+1) = u_k(n) - qp^k u_k(n-k) \; pour \; n \geq k$$

avec les conditions initiales : $u_k(n) = 1$ pour $0 \leq n \leq k-1$ et $u_k(k) = 1 - p^k$.

Le but consiste, pour *n* et *p* donnés, à calculer la fonction de répartition de la variable aléatoire L_n , $P(L_n = k)$.

On utilisera deux tableaux :

- un tableau *U(j)* avec $0 \leq j \leq n$, qui servira à travailler et finalement à stocker $P(L_n = k)$

- un tableau *FR(j)* avec $0 \leq j \leq n$ pour stocker $P(L_n \leq k)$

Algorithme de calcul de $P(L_n = k)$ et $P(L_n \leq k)$ **:**

1 - Lire les données :

n entier ≥ 3 et $p \in]0, 1[$

2 - Initialisation :

$q = 1 - p$

$\lambda = q$

$U(1) = q$

$FR(0) = q^n$

3 - Pour $2 \leq k \leq n-1$ faire :

3.1 - construction des conditions initiales

$U(k) = q + pU(k-1)$

$U(k-1) = 1$

$\lambda = p\lambda$

3.2 - pour $k+1 \leq j \leq n$ faire

$U(j) = U(j-1) - \lambda U(j-k)$

3.3 - stockage de la fonction de répartition

$FR(k-1) = U(n)$

4 - Calcul de *FR(n) et U(n)*

4.1 - Compléter la fonction de répartition avec $FR(n-1), FR(n)$

$FR(n-1) = 1 - p^n$

$FR(n) = 1$

4.2 - clacul de $P(L_n = k) = U(k)$

$U(0) = FR(0)$

Pour $1 \leq k \leq n$ faire :

$U(k) = FR(k) - FR(k-1)$

Fin d'algorithme

Nous remarquons que l'algorithme proposé est général dans le sens où il permet de calculer pour tout $k \leq n$. Bien entendu, pour une valeur de *k* fixée, le temps de calcul peut encore être réduit.

5.5.3 Probabilité d'occurrence des défaillances lors d'un trajet

L'idée est de construire, à partir d'une série de mesures réalisées par un véhicule équipé du matériel nécessaire pour relever l'amplitude (niveau), la fréquence et l'intensité du champs électromagnétique ambiant, un modèle de fautes identique à celui proposé à la figure 5.2 du paragraphe 5.1.3 pour les systèmes X-by-Wire en environnement électromagnétique perturbant. Les mesures sont réalisées au cours d'un trajet qui devra être représentatif de l'environnement électromagnétique de la "région" étudiée. On relève, pour une fréquence et une intensité susceptibles de perturber le système étudié, les niveaux de champs supérieurs aux niveaux tolérés et évalués par des procédures de test de robustesse aux champs électromagnétiques. On obtient alors la distribution des zones au sein desquelles les systèmes sont susceptibles d'être perturbés. On utilisera les informations disponibles (obtenues par injection de fautes, retour d'expérience, test...) quant à la probabilité de perte d'information en environnement perturbé pour obtenir un modèle d'erreurs pour les systèmes X-by-Wire en environnement électromagnétique perturbé.

5.5.4 Récupération et exploitation des mesures

Si la technique de récupération et d'analyse des mesures à partir de véhicules équipés est explicitée dans cette section, elle est inspirée du rapport final d'un projet PREDIT, le projet CEERF [94], qui a pour objectif de caractériser l'environnement électromagnétique routier en France. L'essentiel des informations exploitées dans cette section ont été extraites de ce rapport.

5.5.4.1 Le projet CEERF (Caractérisation de l'Environnement Electromagnétique Routier en France)

L'objectif majeur du projet CEERF était d'établir une cartographie de l'environnement électromagnétique sur le réseau routier [94]. Pour ce faire, les points clés avérés du projet étaient les suivants :

1. Etablir une cartographie de l'environnement électromagnétique sur le réseau routier français en terme de :
   - niveau de champs,
   - nature des sources de perturbation,
   - probabilité d'occurence des perturbations d'amplitudes conséquentes.
2. Assurer la pérennité des résultats en développant une méthode innovante de caractérisation de l'environnement afin de :
   - permettre le suivi des évolutions futures de l'environnement,
   - étendre la cartographie au territoire européen.
3. Synthétiser et diffuser les résultats du projet pour :
   - contribuer à l'évolution de la réglementation en CEM, prévue à partir de 2003, notamment le choix des contraintes d'essais d'immunité,
   - fournir au secteur automobile les informations nécessaires lui permettant notamment d'adapter ses cahiers des charges des équipements électroniques, afin d'en assurer la compatibilité au meilleur coût.

5.5.4.2 Déroulement de la phase de mesures

L'objectif de la mission est d'effectuer un trajet précis avec un véhicule équipé du matériel nécessaire pour récupérer la fréquence, l'intensité et l'amplitude du champ électromagnétique ambiant. L'itinéraire du trajet doit être représentatif de l'environnement électromagnétique routier de la région étudiée. On appelera le trajet correspondant *trajet de référence*. Nous proposons un trajet de référence de 600km. Afin de garantir une précision suffisante

des mesures et de couvrir une bande fréquence allant de 100kHz à 3GHz, le véhicule est équipé de plusieurs antennes, et le spectre est sauvergardé sur le disque dur d'un ordinateur embarqué (voir [94] pour plus de détails sur les caractéristiques techniques de la phase de mesure). Les informations collectées à la fin de la phase de mesure sont synthétisées et représentées sur une courbe dont le spectre est donné à la figure 5.11.

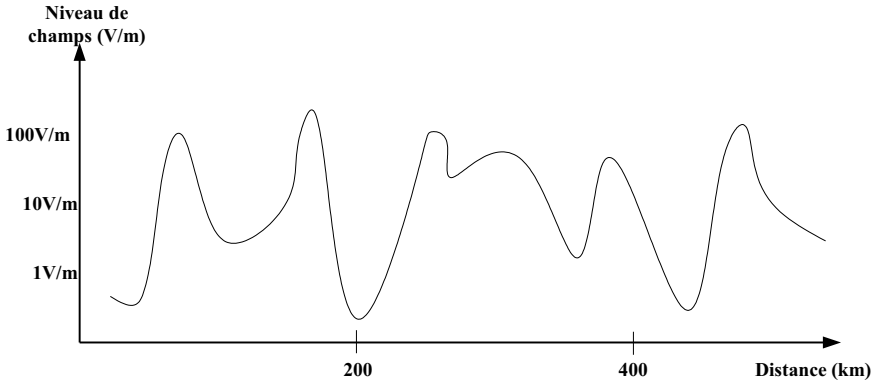

FIG. 5.11 – Exemple de spectre des niveaux de champs rencontrés au cours du trajet de référence

5.5.5 Evaluation de la probabilité d'occurrence de défaillance lors d'un trajet

En appliquant la méthode donnée au paragraphe 5.1.3, le spectre de la figure 5.11 construit à partir de données récupérées au cours du trajet de référence nous a permis de construire un modèle de fautes correspondant à la distribution des zones selon leurs interarrivées et leur durée (voir figure 5.12).

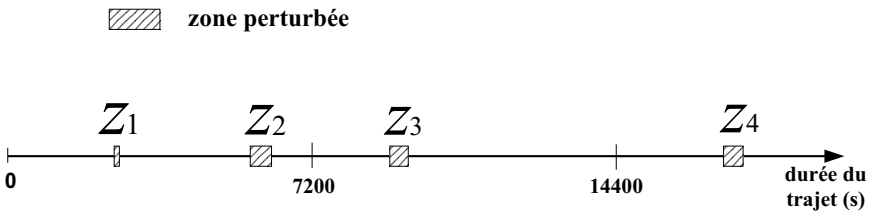

FIG. 5.12 – Distribution temporelle des zones dont le niveau de champs est supérieur à celui imposé en phase de test : *modèle de fautes*

Soit un trajet $T = \{Z_i\}$ composé d'une suite de zones Z_i. On fait l'hypothèse que les arrivées de perturbations sont indépendantes, donc, si pendant l'intervalle d'observation du système, r rafales d'erreurs de durées respectives Z_i surviennent (r est la cardinalité de T), et que la probabilité qu'un cycle de communication soit erroné est toujours de P_{err}, on peut alors donner une borne supérieure pour la probabilité d'occurrence des défaillances du véhicule pendant le trajet, notée par $Pd_{trajet}(T, P_{err})$, qui correspond à la probabilité que le nombre de cycles de communication perdus dépasse η_{max} durant le trajet.

Considérons d'abord la probabilité de ne jamais dépasser la contrainte temporelle η_{max} durant le trajet. Nous avons soit la formule exacte :

$$1 - Pd_{trajet}(T, P_{err}) = \prod_{i=1}^{r} \left[R(\eta_{max}+1, \eta_{WC}(Z_i); P_{err})^{\eta_{WC}(Z_i)} \right]$$

soit la borne :

$$1 - Pd_{trajet}(T, P_{err}) \geq \prod_{i=1}^{r} \left[(1 - P_{err}^{(\eta_{max}+1)})^{\eta_{WC}(Z_i)} \right]$$

Ainsi, la probabilité de dépasser au moins une fois η_{max} pour le trajet est donnée par :

$$Pd_{trajet}(T, P_{err}) = 1 - \prod_{i=1}^{r} \left[R(\eta_{max}+1, \eta_{WC}(Z_i); P_{err})^{\eta_{WC}(Z_i)} \right] \tag{5.19}$$

Elle est aussi bornée par la formule suivante :

$$Pd_{trajet}(T, P_{err}) \leq 1 - \prod_{i=1}^{r} \left[(1 - P_{err}^{(\eta_{max}+1)})^{\eta_{WC}(Z_i)} \right] \tag{5.20}$$

5.5.6 Extension à d'autres sources d'erreurs

Si les perturbations CEM sont les causes de fautes transitoires les plus souvent citées dans la littérature, elles n'en sont pas les causes principales. En effet, il est communément admis que 60% des fautes - transitoires et permanentes - sont dues à des défauts de conception [72]. En outre, comme expliqué dans la section 5.1, la CEM n'est pas la seule source de fautes de transitoires dues à l'environnement. Or, notre modèle d'erreur repose sur 2 éléments :

1. le spectre de perturbations (occurrence et durée) sur un trajet de référence,
2. la probabilité P_{err} de perdre tous les messages répliqués en cas de perturbation.

Il est possible techniquement d'obtenir les mêmes mesures, mais pour l'ensemble des fautes transitoires qui affectent les messages transmis sur le réseau. En effet, il suffit d'utiliser un procédé de diagnostic en ligne qui enregistre chaque occurrence de trame détectée comme erronée ou absente sur un trajet de référence. Il sera alors possible de construire un spectre similaire à celui relevé pour les perturbations CEM. Dans ce cas de figure, la "probabilité P_{err} de perdre tous les messages répliqués en cas de perturbation" serait transformée en "probabilité P_{err} de perdre tous les messages répliqués sachant qu'au moins un message est perdu". De la même manière, on pourrait relever par diagnostic en ligne les occurrences de pertes de tous les messages répliqués. La distribution des perturbations peut alors être analysée avec $P_{err} = 1$. On couvre alors l'ensemble des sources de fautes transitoires, mais aussi intermittentes (voir paragraphe 1.4.2). Cependant, les contrôleurs de communication disponibles à l'heure actuelle ne permettent pas de mettre en oeuvre ces stratégies.

5.6 Correspondance entre la probabilité d'occurrence de défaillance lors d'un trajet et la sûreté

5.6.1 Respect des contraintes

Nous avons donné aux paragraphe 1.6.1 les préconisations en terme de contraintes sur la sûreté pour les systèmes X-by-Wire. Or, dans l'intégralité des cas, cette contrainte est exprimée en probabilité d'occurrence de défaillance par heure.

La Fiabilité Comportementale que nous avons introduite précédemment est mesurée par des probabilités d'occurrence de défaillance par zone ou par trajet ; ceci signifie que si on sait prouver que la probabilité d'occurrence de défaillance de niveau véhicule sur une zone Z donnée est telle que :

$$Pd(Z, P_{err}) < P_{véhicule} \tag{5.21}$$

et pour un trajet T donné :

$$Pd_{trajet}(T, P_{err}) < P_{véhicule} \tag{5.22}$$

il n'est pas possible d'en conclure que :

$$P(occurrence\ de\ défaillance\ critique\ en\ une\ heure) < P_{véhicule} \tag{5.23}$$

Il est néanmoins possible d'étendre la propriété 5.21 si la durée de traversée de la zone Z est supérieure à une heure à :

$$5.21 \Rightarrow P(occurrence\ de\ défaillance\ critique\ en\ une\ heure/zone\ Z) < P_{véhicule}$$

et 5.22 si la durée pendant laquelle est effectué le trajet de référence T est supérieure à 1 heure, à :

$$5.22 \Rightarrow P(occurrence\ de\ défaillance\ critique\ en\ une\ heure/trajet\ T) < P_{véhicule}$$

De plus, d'aprés la méthode proposée, ces propriétés 5.22 et 5.21 sont établies sous des hypothèses données (vitesse constante, pire situation de vie, etc.). Il n'est pas possible, avec les informations dont nous disposons à l'heure actuelle (rapport CERF de 2003 et modèles Matlab / Simulink du système et SimulinkCar du véhicule) d'affirmer que :

$$5.22 \Rightarrow 5.23$$

ni que :

$$5.21 \Rightarrow 5.23$$

Enfin, du point de vue de l'évaluation de la sûreté, il est important de garder à l'esprit que les conditions données pour vérifier les propriétés 5.21 et 5.22 sont nécessaires, mais elles ne sont pas suffisantes, car seules les fautes transitoires d'interaction dues à l'environnement sont traitées.

Néanmoins, l'approche que nous avons proposée montre qu'il est possible d'apporter des évaluations quantitatives à la fiabilité comportementale relativement à des trajets réalisés sous des conditions donnés. Il serait alors intéressant d'identifier la pire trajectoire d'un véhicule qui serait définie par un trajet et une situation de vie, pire trajectoire qui garantirait que si la propriété est respectée sur cette trajectoire, elle est respectée sur toute trajectoire.

5.6.2 Quelles contraintes pour les réglementations à venir

Alors que les acteurs industriels et scientifiques du monde de l'électronique embarquée dans l'automobile se posent aujourd'hui la question de l'applicabilité des normes types CEI 61508 pour certifier le développement de systèmes critiques sûrs de fonctionnement (voir paragraphe 1.6.2 pour plus de détails) et de l'éventuelle création d'une norme dédiée, ces travaux peuvent apporter certains éléments de réponse à la problématique de l'évaluation a priori de l'occurrence des défaillances de gravité 3 ou 4 causée par des fautes transitoires (voir paragraphe 1.4.2). Les fautes intermittentes étant intégralement dues à des défauts de conception, cet aspect, non abordé dans ces travaux, pourra être traité par des processus qualité d'ordres méthodologiques. Même si la robustesse des équipements vis à vis des perturbations peut aussi être améliorée par des processus qualité, il reste une part d'aléatoire qu'aucun processus de développement ne peut maîtriser. Cette part d'aléatoire est aujourd'hui paramétrée par des niveaux de sûreté qui s'expriment en probabilité d'occurence de défaillance par heure, comme celui proposé pour les SILs de la CEI61508 (voir paragraphe 1.6.2). Plusieurs arguments démontrés dans ces travaux pourraient nous amener à remettre en cause cette approche. En effet, les taux de défaillances des systèmes sont renseignés à partir du retour d'expérience des constructeurs d'automobiles. Les chiffres sont obtenus grâce aux statistiques réalisées par les réparateurs en cas de retour de véhicule pour cause de défaillance permanente d'un composant. Si certains défauts transitoires sont enregistrés pour alimenter ces statistiques, les causes des défauts ne sont pas signalables. Par conséquent, les constructeurs n'ont aujourd'hui à leur disposition aucun taux de défaillance relatifs aux fautes transitoires. En outre, l'environnement étant en perpétuel mouvement, le retour d'expérience à t_0 ne permet pas forcément d'alimenter une modélisation fine de cet environnement à t_0+ 1 an, surtout pour un véhicule qui devrait être vendu au public à t_0+ 5 ans. La vitesse du développement des télécommunication est un bon exemple pour illustrer le dynamisme de l'environnement au sein duquel circulent les automobiles d'aujourd'hui. Si nos travaux n'apportent aucune réponse définitive à cette problématique, ils donnent des pistes à exploiter, notamment avec l'inclusion des contraintes temps réel dans les exigences de sûreté de fonctionnement, et l'alimentation continue des modèles d'erreurs au moyen de trajets de référence. De même, si une contrainte probabiliste devait être imposée, son expression poserait un réel problème (voir paragraphe 5.6.1). En effet, si nos travaux proposent un taux de défaillance par trajet, cette notion est trop réductrice pour une réglementation dont le champs d'application se voudrait national, ou même européen. On pourrait éventuellement imaginer un retour à partir de tests réalisés sur une multitude de trajets, mais quelle serait alors la méthode statistique à utiliser : moyenne, pire cas ? La criticité des systèmes pourrait inciter les ingénieurs en sûreté de fonctionnement à utiliser une approche pire cas, mais le surcoût inhérent à cette approche pourrait être un frein à cette solution.

Aucune réponse n'a aujourd'hui été apportée à la problématique de l'évaluation quantitative de l'influence des fautes transitoires sur la sûreté de fonctionnement dans le monde l'automobile, et c'est certainement entre autres pour cette raison qu'aucune norme dédiée n'a encore vu le jour. Si ça devait être le cas prochainement et que le problème discuté ici n'était pas traité, la réglementation ferait l'impasse sur 40% de 90% = 36%[21]- soit un tiers - des causes de défaillance des composants électroniques et/ou informatiques.

[21] 90% des fautes affectant un système élecronique/informatique sont transitoires, et 40% ne sont pas dues à des défauts de conception [72].

Bilan des contributions

La partie 2 décrit intégralement la méthode d'évaluation proposée dans ces travaux de thèse, selon les deux étapes que sont l'étude du système Steer-by-Wire en mode nominal et en mode dégradé. L'étude du système en mode nominal repose sur des modèles et des techniques disponibles actuellement chez PSA Peugeot Citroën. Nous avons enrichi ces techniques par la discrétisation du modèle Simulink du système Steer-by-Wire selon la durée des cycles de communication. De plus, en complément des pratiques industrielles actuelles, nous proposons de placer l'étude non plus seulement dans une démarche propre aux automaticiens, mais aussi dans une démarche d'évaluation de la sûreté de fonctionnement d'une architecture opérationnelle donnée. Le pire retard pur tolérable évalué au paragraphe 4.2 devient alors une exigence de sûreté de fonctionnement au même titre que le MTTF ou la fiabilité. La paragraphe 4.3, consacré à l'évaluation du retard pur pire cas, décrit la méthode qui va permettre au concepteur du système de vérifier que cette exigence est respectée ou non par l'architecture opérationnelle étudiée. La méthode utilisée est représentée à la figure 1.

Le résultat de l'évaluation du retard pur pire cas donne aussi une indication sur la qualité de service et les performances temps réel du système (voir le paragraphe 6.4 de l'Etude de Cas qui sera présentée dans la partie 3 de ce document).

L'étude du système en mode perturbé constitue l'apport majeur de cette thèse. Elle repose sur l'objectif d'évaluer l'impact des phénomènes transitoires sur la sûreté de fonctionnement du système. Dans ce contexte, l'originalité de l'approche est d'étudier non plus le comportement du système en cas de fautes transitoires, mais l'influence du système sur le comportement du véhicule au sein duquel il est embarqué. L'idée était de calquer l'approche utilisée par PSA Peugeot Citroën en mode nominal sur le mode dégradé en incluant un modèle d'erreur pour les évaluations probabilistes. Comme détaillé au paragraphe 2.2.3 de l'Etat de l'Art, plusieurs modèles analytiques de l'influence des perturbations CEM sur la qualité de service d'un réseau de communication ont déjà été proposés, mais aucun d'entre eux n'était construit à partir de données réelles. Ceci étant, nous proposons ici une méthode d'évaluation basée sur des statistiques réelles quant à la probabilité d'apparition des perturbations électromagnétiques sur un trajet donné et à leur durée, ainsi que le protocole à respecter pour récolter ces mesures et les exploiter. Le modèle est ainsi tout à fait paramétrable en fonction des spécifications des réseaux implémentés, mais aussi des normes et autres réglementations à venir en matière de CEM. En effet, il a été créé pour utiliser des données provenant d'un document de travail - le rapport du projet PREDIT CEERF [94] - qui doit être mis à jour régulièrement en fonction de l'environnement électromagnétique routier. La méthode utilisée est résumée à la figure 2.

Cependant, il est important de garder à l'esprit qu'un modèle de faute unique n'est représentatif que d'une seule région. Or, à l'heure où la notion de plateforme se globalise dans le monde de l'automobile, on imagine mal une spécification de système pour une région donnée. En conséquence, pour tirer des conclusions généralistes sur une architecture donnée, il faudra utiliser une multitude de modèles et, en fonction de l'approche choisie (pire cas, moyenne...), réaliser des évaluations statistiques sur l'ensemble des résultats. Cette solution n'est pas présentée

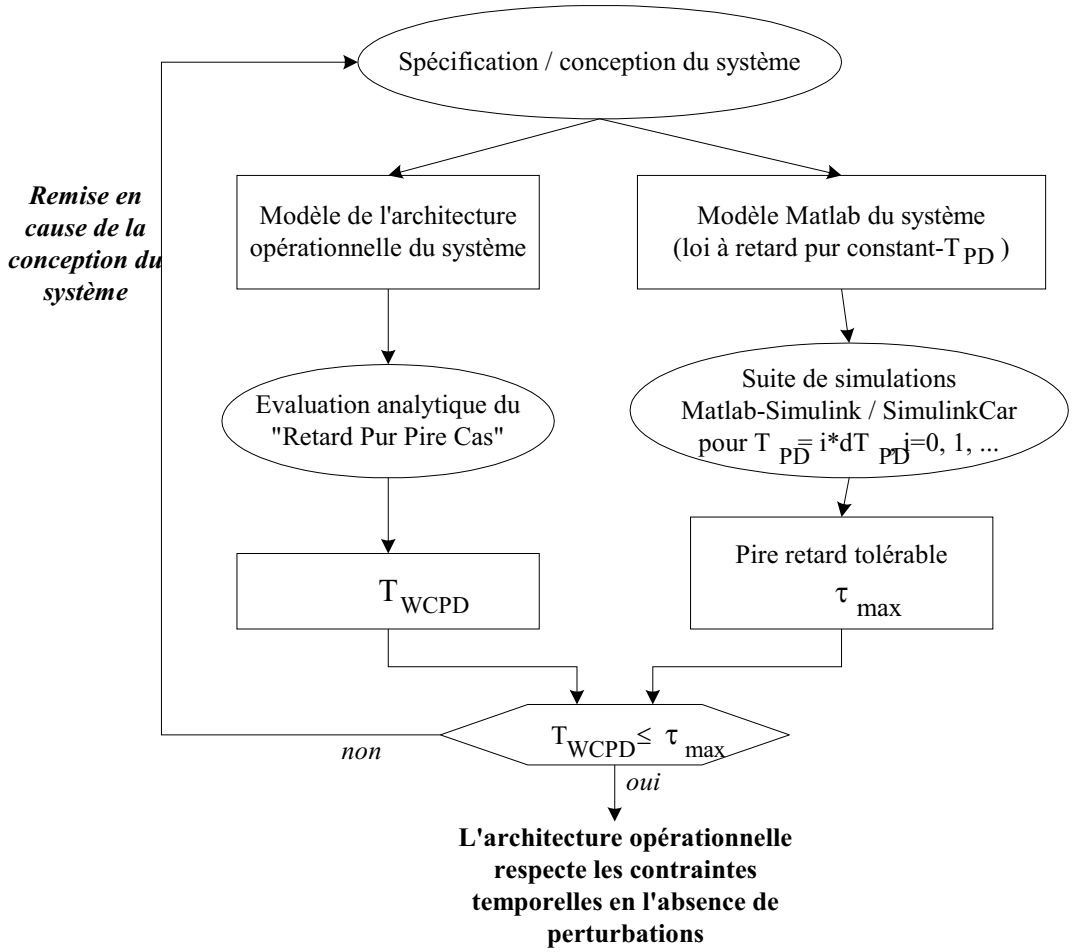

FIG. 1 – Méthode de vérification en mode nominal

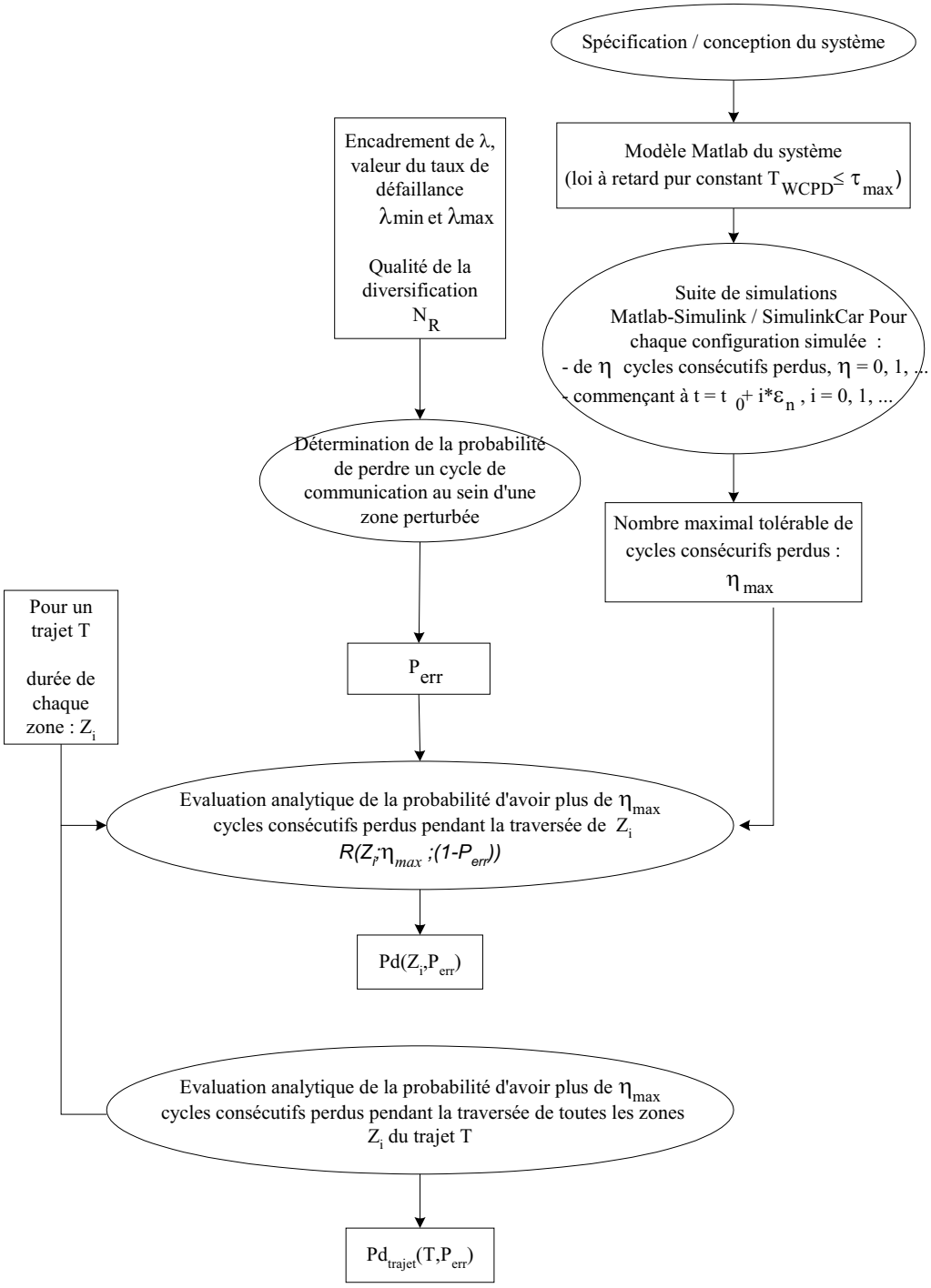

FIG. 2 – Méthode d'évaluation de métriques de la Fiabilité Comportementale en mode perturbé

dans ce document - nous nous intéressons dans ces travaux de thèse à la probabilité de défaillance pour une zone et un trajet donnés -, mais sera rappelée dans les perspectives.

Par ailleurs, si la majeure partie des difficultés techniques inhérentes à cette approche ont été traitées (pattern d'erreur, modélisation sous Simulink, modèle d'erreur réaliste,...), plusieurs hypothèses fortes - et discutables - sont imposées, et notamment :

- le plus petite durée d'une défaillance au niveau du système correspond à un cycle de communication (voir paragraphe 5.2),
- les critères de qualité de service utilisés pour le mode nominal sont valable pour le mode dégragé (voir paragraphe 5.2.2).

Les informations disponibles au moment de la rédaction de ce document ne nous permettaient pas de relacher ces hypothèses. Si la problématique du relachement de ces deux hypothèses doit constituer un axe fort pour les travaux à venir sur l'évaluation de Fiabilité Comportementale (voir Perspectives), cela ne retire rien à l'apport méthodologique de ces travaux qui constitue dorénavant un cadre rigoureusement balisé pour l'évaluation quantitative du comportement des systèmes en cas de fautes transitoires. Cet apport repose aussi sur la non exclusivité des exemples choisis ici pour caractériser les systèmes (Steer-by-Wire) et les perturbations (CEM).

Enfin, la problématique de la correspondance entre les quantifications associées à la Fiabilité Comportementale et les contraintes de sûreté a soulevé le problème crucial de la quantification des réglementations à venir, et mis en évidence le piège d'une quantification en défaillance par heure qui pourrait ne pas avoir de sens.

Partie 3

Chapitre 6

Etude de cas : application à une architecture opérationnelle Steer-by-Wire

Cette section a pour objectif de rappeler en section 6.1 les méthodes présentées aux chapitres 4 et 5 à une architecture opérationnelle Steer-by-Wire réaliste en termes de coût, de taille et de technologie utilisée. Après avoir decrit les services d'un tel système et les aspects opérationnels (section 6.2) de son architecture, nous appliquerons la méthode de vérification du respect des contraintes temps réel en mode nominal (sections 6.3), puis nous évaluerons la Fiabilité Comportementale du système selon le modèle d'erreurs présenté au chapitre 5, pour trois trajets de référence différents : en région très perturbée (section 6.7), moyennement perturbée (section 6.8) et peu perturbée (section 6.9). Dans chaque cas, nous réaliserons une étude de sensibilité sur la Fiabilité Comportementale du système en faisant varier la durée d'un cycle de communication et la robustesse du système. Enfin la dernière section (6.10) de l'étude de cas sera consacrée à l'influence du protocole de communication sur la Fiabilité Comportementale, mais aussi sur la disponibilité du véhicule.

6.1 Rappel de la méthode

La méthode proposée dans ce document a pour objectif principal d'évaluer l'influence des performances temps réel et des fautes transitoires sur la sûreté du véhicule (absence de défaillance catastrophique). On rappelle ici l'approche méthodologique proposée dans la thèse :

Le détail des différentes étapes est le suivant :

1. Dans un premier temps, par exécution d'un modèle Matlab / Simulink du système interagissant avec un modèle SimulinkCar du véhicule, nous évaluons le retard pur maximal tolérable pour la fonction "actionnement de la crémaillère" entre la consigne conducteur et le traitement de cette consigne par la loi de commande pilotant l'actionneur de crémaillère ; puis, nous validons une architecture opérationnelle de ce système en évaluant analytiquement le pire retard et vérifiant que ce pire retard est inférieur au retard pur maximal tolérable (voir chapitre 4). Cette étude se fait sous une hypothèse d'absence de perturbations susceptibles d'affecter le fonctionnement du système de communication.
2. Lorsqu'un système est dimensionné de telle sorte que son fonctionnement respecte les contraintes de sûreté en mode nominal (sans perturbation), nous pouvons analyser son comportement face à des perturbations

pouvant affecter ses composants, plus particulièrement les échanges d'informations via un réseau ; pour ceci :

- nous évaluons, par simulation du système dans son environnement véhicule (Matlab / Simulink et SimulinkCar), le pire intervalle tolérable séparant deux arrivées d'échantillons valides en entrée de la loi de commande de la position crémaillère,
- puis, nous déterminons, en fonction de caractéristiques intrinsèques des composants matériels et de l'architecture opérationnelle (redondance, diversification), la probabilité, qu'en zone perturbée, un cycle de communication soit affecté,
- enfin, ces informations nous permettent d'évaluer la probabilité d'occurrence d'une défaillance critique lors de la traversée d'une zone perturbée donnée ou sur un trajet de référence ; ceci nous donne des mesures permettant de quantifier la Fiabilité Comportementale d'un système.

6.2 Architecture opérationnelle du système 'Steer-by-Wire"

L'étude de cas présentée ici repose sur un système "Steer-by-Wire" dont des parties ont servi d'illustrations dans la partie 2 de ce document. Fonctionnellement, ce système doit fournir, à tout instant, deux services :

- σ_{FA} : braquer les roues selon la requête conducteur,
- σ_{HW} : fournir un retour d'effort au volant cohérent avec la situation de vie du véhicule.

6.2.1 Architecture informatique support

La figure 6.1 est une illustration de l'architecture physique sur laquelle sont implantés les services décrits précédemment. Elle inclut 4 calculateurs communément appelés ECU (Electronic Control Unit) ou noeud. Deux ECUs en redondance active traitent les même signaux en entrées, fournissent les mêmes signaux en sorties et sont implantés géographiquement près du volant : HW ECU1 (Hand Wheel ECU1) et HW ECU2 (Hand Wheel ECU2). Deux autres ECUs en redondance active sont implantés géographiquement près de la crémaillère : FAA ECU1 (Front Axle Actuator ECU1) et FAA ECU2 (Front Axle Actuator ECU2). Chaque ECU est connecté à 2 canaux de communication redondants (BUS1 et BUS2). Les canaux de communication obéissent à un protocole TDMA (la configuration des cycles TDMA pour cette application sera précisée au paragraphe 6.2.2.4). 3 capteurs (as1, as2 et as3), connectés par des liaisons point à point aux HW ECU 1 et HW ECU 2, mesurent les requêtes du conducteur. De même, 3 capteurs (rps1, rps2 et rps3), connectés par des liaisons point à point aux FAA ECU 1 et FAA ECU 2, mesurent la position crémaillère, l'effort bielette (interface entre la crémaillère et la roue), et éventuellement d'autres informations relatives à la situation de vie du véhicule. 2 moteurs (ou actionneurs) en redondance active, connectés par liaison point à point au noeud HW ECU 1 pour l'un et HW ECU 2 pour l'autre, fournissent un retour d'effort au volant. Enfin, 2 moteurs en redondance active, connectés par liaison point à point au noeud FAA ECU 1 pour l'un et FAA ECU 2 pour l'autre, actionnent la crémaillère pour permettre le braquage des roues.

Les ECUs redondés sont regroupés au sein d'Unités Tolérantes aux Fautes (FTU). Une FTU est un ensemble de plusieurs stations qui assurent la même fonction et émettent leurs messages dans des fenêtres temporelles différentes. Dans l'étude de cas, une première FTU comprend les ECUs HW ECU1 et HW ECU2, tandis que les ECUs FAA ECU1 et FAA ECU2 forment une deuxième FTU. Le rôle d'une FTU est double (voir [120]), puisqu'elles augmentent la robustesse du système en cas de faute transitoire de durée inférieure à 1 cycle de communication (redondance temporelle d'information à l'intérieur d'un cycle), et qu'elles permettent aussi aux noeuds récepteurs de tester la cohérence des informations reçues et aux noeuds émetteurs de détecter les erreurs

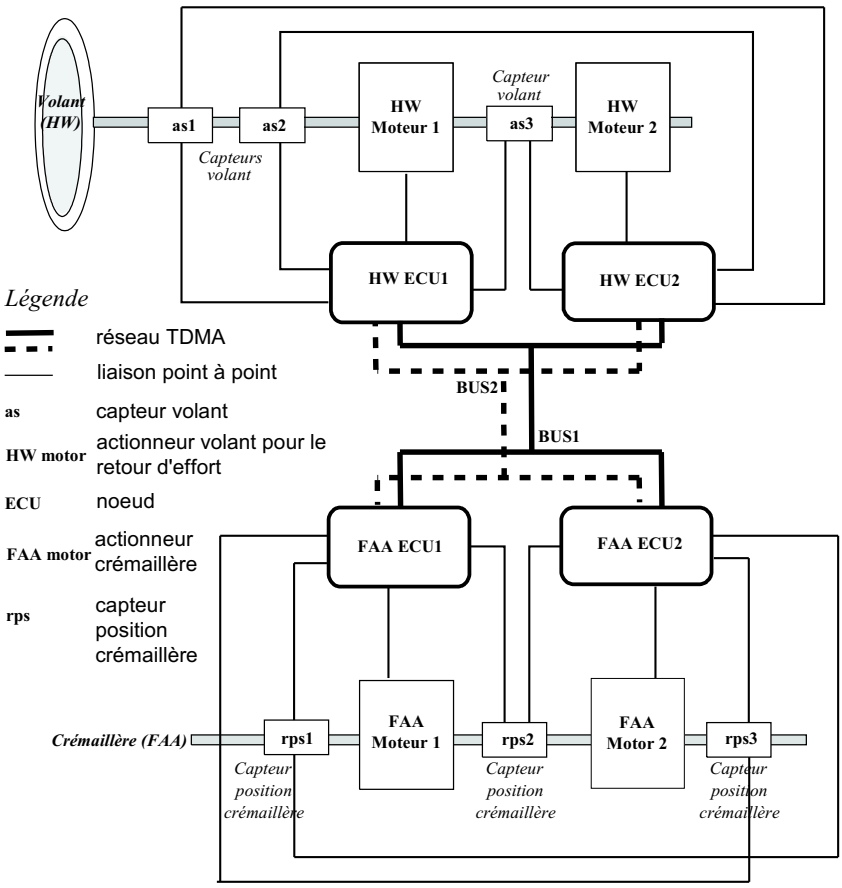

FIG. 6.1 – Architecture Steer-by-Wire

de calcul commises avant l'émission.

Nous considérons, de plus, que les ECUs sont à silence sur défaillance (fail silent). Un ECU est dit fail-silent si :

- 1.
  - a) il transmet ses trames au bon moment,
  - b) il transmet la bonne valeur.
- 2. il transmet une trame erronée mais dont l'erreur est détectable (exemple : CRC erroné).

L'utilisation d'ECUs "fail-silent" simplifie grandement la construction d'architectures tolérantes aux fautes. En effet, si les noeuds sont "fail-silent" à 100%, le nombre minimum d'ECUs par FTU pour tolérer k ECUs défaillants est de k+1 (voir[34]). Notons que la propriété sur le nombre maximal d'ECUs défaillants dans une architecture opérationnelle est généralement complexe à vérifier. Dans l'éventualité où le taux de couverture n'est pas de 100%, Hammett a montré à la conférence SAE 2002 [45] qu'il est possible d'inclure une évaluation de ce taux de couverture dans des calculs de sûreté et que son influence est non-négligeable.

Les exigences 1.a) et 2) doivent être respectées par le protocole de communication, alors que le respect de l'exigence 1.b) incombe à l'application. Pour plus d'information sur la notion de silence sur défaillances, le lecteur pourra se référer à [34], [108], [92] et [120].

6.2.2 Architecture opérationnelle

6.2.2.1 Implantation du service σ_{FA}

Les requêtes du conducteur sont mesurées par les 3 capteurs répliqués as1, as2 et as3 et envoyées aux applications implantées dans les ECUs redondants HW ECU 1 et HW ECU 2. Chaque application réalise un vote sur les 3 valeurs reçues et produit une donnée dite "sécurisée". Cette donnée est transmise via les deux bus de communication BUS1 et BUS2 . Les applications localisées sur les noeuds redondants FAA ECU 1 et FAA ECU 2 consomment, à chaque activation, cette donnée ainsi que la situation de vie du véhicule et la dernière position de la crémaillère (fournie par les capteurs rps1, rps2 et rps3) pour élaborer la consigne à donner à l'actionneur de la crémaillère. Les activités de ces applications sont donc synchronisées sur le cycle de communication (et plus particulièrement sur la fin du dernier réplica du message consommé).

6.2.2.2 Implantation du service σ_{HW}

Le couple volant est mesuré par les 3 capteurs répliqués as1, as2 et as3 et envoyé à des applications localisées dans les ECUs HW ECU 1 et HW ECU 2. Chaque application réalise un vote sur les 3 valeurs reçues et construit une valeur de couple à fournir au volant à partir de ces 2 valeurs, de la situation de vie du véhicule et de la position courante de la crémaillère reconstruite à partir des informations fournies par rps1, rps2 et rps3.

6.2.2.3 Caractéristiques temporelles

Ces caractéristiques ont été établies dans le cadre de la construction d'une architecture "Steer-by-Wire" chez PSA Peugeot Citroën. La loi de commande élaborant les consignes à l'actionneur de la crémaillère doit être activée périodiquement selon une période définie par une étude amont d'automatique. Cette période et la taille des données à transmettre à chaque cycle fixe la longueur du cycle de communication ε_n. Dans cette étude de cas :

$$\varepsilon_n = 6ms$$

Les périodes de production des instances de signaux par les applications émettrices sont les suivantes :

- l'application localisée sur l'ECU HW ECU1 (respectivement, sur l'ECU redondant, HW ECU2) produit les instances des signaux Angle_HW et Couple_HW regroupées au sein d'une trame de nom HW_Trame_ECU1 (respectivement HW_Trame_ECU2) ; les signaux sont produits ainsi :
  - Angle_HW toutes les 2 ms,
  - Couple_HW toutes les 4 ms.

- l'application localisée sur l'ECU FAA ECU1 (respectivement, sur l'ECU redondant FAA ECU2) produit les instances des signaux Position_FAA et Effort_Biellette_FAA regroupées au sein d'une trame de nom FAA_Trame_ECU1 (respectivement FAA_Trame_ECU2) ; les signaux sont produits ainsi :
  - Position_FAA toutes les 2 ms,
  - Effort_Biellette_FAA toutes les 4 ms.

Nous focalisons plus particulièrement notre étude de cas sur le service σ_{FA} (braquer les roues selon selon la requète conducteur) et, pour ce service, sur la variable Angle_HW, et nous considérerons donc dans la suite de l'étude que la période de production considérée est le minimum des périodes de production des instances de signaux (Angle_HW, Couple_HW) regroupées dans les trames supportant Angle_HW (HW_Trame_ECU1, HW_Trame_ECU2) :

$$\varepsilon_t = min(2, 4) = 2ms$$

Cette étude de cas relève donc de la situation où $\varepsilon_n > \varepsilon_t$.

6.2.2.4 Configuration du cycle de communication

Comme indiqué précédemment, l'accès au médium de communication est contrôlé par un protocole de type Time Division Multiple Access (TDMA). L'intégralité de la bande passante est allouée à chaque station au cours d'une tranche horaire (time slot). L'atomicité d'observation des erreurs étant le cycle de communication dans la méthode que nous avons proposée, le placement des messages au sein de cycle de communication n'a pas d'influence sur la probabilité d'occurrence de défaillance et les caractéristiques temporelles du paragraphe. Néanmoins, pour mettre en oeuvre des techniques d'évaluation plus fines, il serait important de pouvoir analyser l'influence du placement d'un des réplicas au sein d'un cycle. Le lecteur pourra se référer à [41] pour un placement optimal des réplicas au sein du cycle du communication.

Par contre, la configuration d'un cycle a une incidence directe sur la quantification de T_{WCPD} (voir paragraphe 4.3.3.2). Dans cette étude de cas, nous avons $\varepsilon_n > \varepsilon_t$; aussi, toutes les instances de signal sont transmises dans un seul et unique cycle. Nous proposons, par exemple, l'allocation de la figure 6.2 :

Nous conservons l'hypothèse adoptée aux chapitres précédents selon laquelle la livraison de l'instance de signal à l'actionneur est réalisée à la fin du dernier slot contenant un réplica de l'instance dans le cycle. Soit d, la distance entre la fin du dernier slot au sein duquel est véhiculé le signal observé et la fin du cycle (voir paragraphe 4.3.3.2), on peut écrire : $d = 1,5\,ms$.

- Si le protocole de communication implémenté est TTP/C, la configuration est complétée par les choix suivants :
  - le nombre de TDMA Rounds par ClusterCycle est 1,
  - la taille d'un TDMA Round est 5 ms,

  - l'intégralité de l'instance de signal est placée dans le slot correspondant,
  - la taille de chaque fenêtre (slot) est identique et vaut 1,5 ms.
- Si le protocole de communication implémenté est FlexRay, cette configuration repose sur les choix suivants :
  - le cycle de communication est intégralement statique (pas de partie dynamique),
  - la taille d'un cycle de communication est 5 ms et tous les slots ont une durée de 1,5 ms,
  - l'intégralité de l'instance de signal est placée dans 1 seul slot de durée 1,5 ms,
  - le placement des slots est le même sur chaque canal (BUS1 et BUS2).

Remarque : le choix du protocole de communication est réalisé en amont, et a une incidence certaine sur les critères régissant le placement et la taille des slots au sein d'un cycle de communication. Cependant, notre objectif est de proposer une méthodologie relativement indépendante de ce même protocole. D'où l'idée de considérer le cycle entier comme unité d'erreur. Nous essaierons de montrer l'influence du protocole de communication au paragraphe 6.10, mais plutôt en terme de mécanismes de détection d'erreurs.

6.3 Evaluation du retard pur pire cas T_{WCPD} en mode nominal

Le chapitre 4 est consacré à l'évaluation du pire retard pur T_{WCPD} et à la vérification des contraintes temps réel en mode nominal. D'après la formule 4.3, dans le cas où $\varepsilon_t < \varepsilon_n$, on peut écrire :

$$T_{WCPD} = \varepsilon_n - d + \varepsilon_t \tag{6.1}$$

soit, pour le signal Angle_HW répliqué dans les trames HW_Trame_ECU1 et HW_Trame_ECU2 :

$$\boxed{T_{WCPD} = 6,5\,ms}$$

6.4 Evaluation du pire retard pur tolérable

Comme présenté aux paragraphes 4.2 et 5.2.2, l'évaluation des bornes maximales tolérables sur le retard pur et sur l'intervalle de temps entre les arrivées de deux instances valides du même signal est réalisée à l'aide des outils Matlab/Simulink et SimulinkCar par une suite de simulations reposant sur des situations de vie prédéfinies par le constructeur. Le lecteur pourra consulter l'annexe A pour une description détaillée du simulateur.

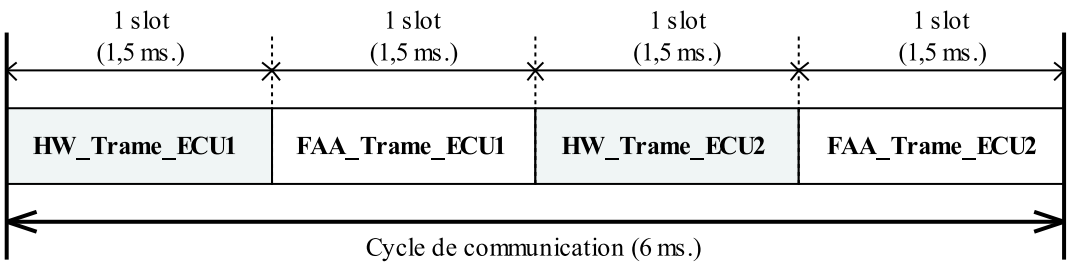

FIG. 6.2 – Placement des slots au sein du cycle de communication (identique sur BUS1 et BUS2)

En mode nominal, c'est-à-dire, sous une hypothèse d'absence de perturbations, on doit donc évaluer la valeur du pire retard tolérable, τ_{max}, pour le service σ_{FA} "actionnement de la crémaillère en fonction des consignes conducteur". Néanmoins, dans cette étude, la qualité des modèles de véhicule font que les simulations en situation de "sinus balayé" ne fournissent pas de résultats significatifs. Nous ne les prenons pas en compte ; notons que le retour d'expérience chez PSA Peugeot-Citroën, montre que les configurations compatibles avec les exigences de sûreté et de qualité des véhicule dans la situation de vie "inscription en courbe" satisfont également les exigences dans la situation de vie "sinus balayé". Aussi, nous utilisons par la suite :

$$\tau_{max} = min(\tau_{max,Calage}, \tau_{max,Ecart\_Trajectoire}, \tau_{max,Reponse\_Precision}) = min(\tau_{max,Calage}, \tau_{max,Ecart\_Trajectoire})$$

Les résultats obtenus, à l'issue de la série de simulation sont dans le cadre de cette étude sont :

Ecart de trajectoire : $\tau_{max,Ecart\_Trajectoire} = 18\,ms$

Calage : $\tau_{max,Calage} = 24\,ms$ Soit :

$$\boxed{\tau_{max} = 18\,ms}$$

Pour que les exigences de sûreté soient respectées, le Pire Retard Pur T_{WCPD} du système doit être tel que $T_{WCPD} < \tau_{max}$, ce qui est vérifié dans cette étude de cas.

Notons qu'il existe une marge de $12,25$ ms entre le retard pur pire cas T_{WCPD} et la contrainte imposée τ_{max}. Cette marge, relativement conséquente au regard des grandeurs étudiées, révèle, intuitivement, que le système pourrait éventuellement être optimisé tout en respectant les exigences imposées. Cette marge peut être un atout de taille pour le concepteur du système qui peut apporter un peu de souplesse dans la périodicité des tâches et des messages, et éventuellement agrandir la taille de son cycle de communication pour transmettre plus d'informations, ou encore ajouter une partie dynamique si le protocole de communication offre cette possibilité. Sinon, le concepteur peut introduire des exigences plus sévères pour proposer un système à haut-niveau de prestation en terme de réactivité. Cette dernière alternative peut être primordiale pour convaincre le public du bien fondé des systèmes "Steer-by-Wire".

6.5 Evaluation du pire intervalle tolérable entre les arrivées de deux instances valides du même signal

On recherche par ici, toujours par une suite de simulations, le pire intervalle tolérable entre les arrivées de deux instances valides du même signal δ_{max}. De la même manière que précédemment, nous n'utilisons le modèle de véhicule sous SimulinkCar que pour la situation de vie "inscription en courbe". Nous obtenons alors les deux résultats suivants :

Ecart de trajectoire : $\delta_{max,Ecart\_Trajectoire} = 36\,ms$

Calage : $\delta_{max,Calage} = 42\,ms$

Pour les mêmes raisons que celles évoquées en section 6.4, les résultats obtenus pour la situation de vie "sinus balayé" ne sont pas significatifs, on peut alors écrire :

$$\delta_{max} = min(\delta_{max,Calage}, \delta_{max,Ecart\_Trajectoire}) = 36\,ms$$

$$\eta_{max} = 6$$

6.6 Modèle d'erreur

Nous instancierons dans cette section le modèle d'erreur présenté au chapitre 5.

6.6.1 Probabilité d'erreur

Plusieurs méthodes existent pour quantifier P_{err}. Celles-ci sont détaillées au paragraphe 5.4.2. Nous proposons dans notre exemple d'utiliser la méthode analytique d'approximation de P_{err} présentée au paragraphe 5.4.2.3.

Peu d'information sont aujourd'hui disponibles quant à la quantification de P_{err}. Cependant, certaines campagnes d'injection de fautes menées sur des architectures ou des modèles d'architectures baties autour du réseau de communication TTP/C nous permettent d'avoir une idée de la robustesse de ces systèmes en environnement très perturbé. On peut citer les études de Grillinger [43] qui nous donne des renseignements intéressants sur le temps de réintégration d'un noeud défaillant en fonction de la durée de la faute (supérieure ou égale à un TDMA Round). Le processus physique d'injection de faute est le Bit Flip au niveau de informations stockées dans le CNI. Il montre que dans environ 3% des cas (3.10^{-2}), le temps de retour à la normale peut excéder 1 TDMA round même si la durée de la faute est largement inférieure à la durée d'un TDMA Round, ce qui conforte nos choix en terme de modèle d'erreur. Par ailleurs, dans le rapport du projet "Fault Injection for TTA" [54], la campagne d'injection de fautes par radiation (Heavy-Ion Radiation) donne les résultats suivant : pour le noeud étudié, une erreur est enregistré toutes les 4 secondes, et cette fréquence peut diminuer jusqu'à 3 à 5 erreurs par minute. Ainsi, si l'on considère que le durée d'un cycle est de 5 ms, le taux d'erreur ira environ de 1.10^{-3} à 1.10^{-4} pour un seul noeud. Donc, selon la notation du paragraphe 5.4.2.3 on peut quantifier approximativement λ et écrire : $1.10^{-4} < \lambda < 1.10^{-2}$.

Le sous-système le plus sensible aux perturbations CEM est le canal de communication [81], aussi nous faisons l'hypothèse, ici, que λ est nul pour les ECUs producteurs de signaux concernant le serviceσ_{FA}.

Sous-système	Nombre de composants redondants	Critère de diversification	Qualité de la diversification (notée sur 10)	Note de diversification
Canal de communication	n_{BUS}	technologie	0	N_{R_BUS}= 1/2
		éloignement physique	10	

FIG. 6.3 – Quantification des critères de diversification pour le canal de communication

Les canaux étant strictement identiques mais implantés de chaque coté du véhicule, cet éloignement est l'éloignement maximal possible au sein d'un même véhicule, c'est pourquoi nous donnons la note maximale au critère de diversification. On peut donc écrire $N_{R-BUS} = 10/20 = 1/2$.

Ainsi, suivant les formules proposées au chapitre 5, on obtient :

$$P_{err} = 1.10^{-2} - N_{R-BUS}(1.10^{-2} - 1.10^{-2*2}) \tag{6.2}$$

soit :

$$\boxed{P_{err} \simeq 5.10^{-3}}$$

6.6.2 Mesures collectées sur le trajet de référence

Il s'agit ici de récolter les mesures correspondant au champs électromagnétique enregistrées au cours d'un trajet de référence, puis d'utiliser ces mesures pour en faire un modèle d'erreur exploitable analytiquement. Le protocole à respecter pour la récolte des mesures nécessaires à la création de notre modèle d'erreur est présenté au paragraphe 5.5.4.

On appelle *r* le nombre de zones perturbantes rencontrée sur le trajet de référence, et la durée de chaque zone *i* est Z_i. Etant donné que l'on est dans le cas $\varepsilon_t \leq \varepsilon_n$, selon l'équation 5.3 on peut écrire le nombre maximal de cycles perturbés dans une zone Z_i :

$$\eta_{WC}(Z_i) = \left\lceil \frac{Z_i}{\varepsilon_n} \right\rceil + 2$$

6.6.3 Evaluation de la Fiabilité Comportementale

La Fiabilité Comportementale est mesurée par la probabilité d'occurrence de défaillance pour un trajet. On rappelle alors les formules, démontrées au paragraphe 5.5.5, qui nous permettent d'évaluer la probabilité d'occurrence de défaillance pour un trajet $T = \{Z_i\}$ composé d'une suite de zones Z_i.

$$Pd_{trajet}(T, P_{err}) = 1 - \prod_{i=1}^{r} \left[R(\eta_{max} + 1, \eta_{WC}(Z_i); P_{err})^{\eta_{WC}(Z_i)} \right] \tag{6.3}$$

Et la borne supérieure peut être calculée par :

$$Pd_{trajet}(T, P_{err}) \leq 1 - \prod_{i=1}^{r} \left[(1 - P_{err}^{(\eta_{max}+1)})^{\eta_{WC}(Z_i)} \right]$$

Par la suite, nous noterons $Pd^{sup}_{trajet}(T, P_{err})$ la borne supérieure de $Pd_{trajet}(T, P_{err})$.

Nous avons démontré au paragraphe 5.6.1 que seule la probabilité d'occurrence de défaillance pour un trajet donné nous permettait d'avoir une idée du respect - ou non - de la contrainte de sûreté. Nous utiliserons donc uniquement la formule 6.3 et l'algorithme de calcul donné dans la section 5.5.2 dans la suite de cette étude de cas.

Précision des calculs : les données manipulées étant particulièrement petites, la question de la précision des calculs peut se poser. Le programme développé en langage C est compilé et exécuté sur une plateforme de type Windows 32. Ainsi, tout calcul manipulant des données inférieures à 10^{-16} [22] peut être entaché d'erreurs conséquentes. Ainsi, pour éviter de manipuler des grandeurs inférieures à 10^{-16}, la valeur minimale de P_{err} avec laquelle nous pouvons obtenir des résultats corrects est 10^{-3}. Dans la suite du chapitre, les études de sensibilité reposeront sur des valeurs de P_{err} supérieures à 10^{-3}.

[22] D'après http ://msdn.microsoft.com/, section "représentation IEEE en virgule flottante", le plus petit entier positif manipulable est $2,2 \times 10^{-16}$.

6.7 Application de la méthode à un trajet de référence effectué en région très perturbée

Les mesures récoltées au cours du traject témoin sont représentées sur la figure 6.4[23].

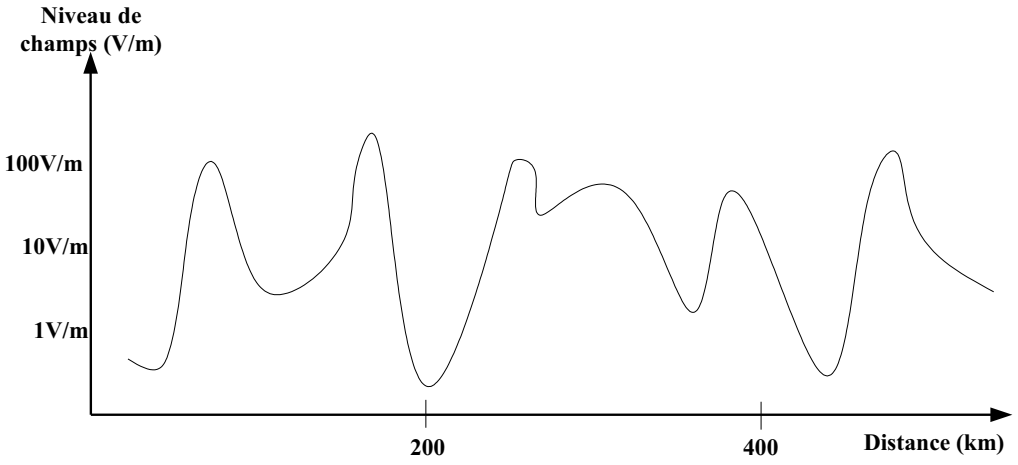

FIG. 6.4 – Mesures obtenues pour un trajet de référence effectué en région très perturbée

Le spectre de la figure 6.4 et le niveau de test imposée par les procédures interne au constructeur d'automobiles (ici 100V/m - cette mesure est un exemple de niveau de test qui peut varier en fonction des constructeurs-) nous permettent d'extraire la distribution des perturbations de la figure 6.5.

La figure 6.5 nous donne les valeurs suivantes :

$$\boxed{card(Z) = 4 \text{ et } Z = \{2, 50, 20, 2\}\text{(unités (s))}}$$

Soit :
- $r = 4$
- $Z_1 = 2s$
- $Z_2 = 50s$
- $Z_3 = 20s$
- $Z_3 = 2s$

6.7.1 Evaluation de la Fiabilité Comportementale pour un trajet de référence effectué en région très perturbée

L'architecture Steer-by-Wire de la figure 6.1 nous donne $\varepsilon_n = 5ms$. Selon l'analyse de la section 6.6.1, $P_{err} = 5 \times 10^{-3}$. En utilisant l'algorithme de calcul donné dans la section 5.5.2, on obtient le résultat suivant :

$$\boxed{Pd_{trajet}(T, P_{err}) = 0}$$

[23]Ce spectre est imaginaire, mais s'inspire des mesures observées dans le rapport du projet CEERF [94], notamment aux abords de radioémetteurs puissants. Cette remarque est valable pour tous les spectres apparaissant dans le document.

Interprétation du résultat : considérons que la propriété à respecter pour garantir la sûreté au niveau du véhicule, sur le trajet T considérée soit :

$$Pd_{trajet}(T, P_{err}) < 5 \times 10^{-10} \tag{6.4}$$

Cette propriété est donc respectée pour $P_{err} = 5 \times 10^{-3}$ et $\varepsilon_n = 5ms$. Comme expliqué au paragraphe 5.6.1, il n'est pas possible de tirer de conclusions quant au respect de la contrainte en terme de défaillance par heure, même si l'éventualité qu'elle ne soit pas respectée existe. Cependant, il montre que, si effectivement le pessimisme de l'approche est celui imposé par la gravité des défaillances associées, si le spectre est cohérent avec la réalité d'une quelconque région au sein de laquelle un véhicule pourrait être commercialisé, et si la quantification de P_{err} est effectivement celle mesurée, il est possible que la contrainte de sûreté soit respectée ; le système Steer-by-Wire pourrait être embarqué dans un véhicule dans l'état. Visiblement cette probabilité $P_{err} = 5 \times 10^{-3}$ n'est pas indispensable pour garantir la fiabilité et on peut encore relacher cette contrainte faisant ainsi diminuer le coût du système (par exemple diminuer la redondance, la qualité de conception ou la diversification des sous-systèmes). C'est pourquoi, l'objectif de notre méthode est aussi de prouver qu'il est possible de faire varier certains critères qui n'augmenteront pas forcément le coût de l'architecture. C'est ce que nous allons tenter de prouver dans les paragraphes suivants.

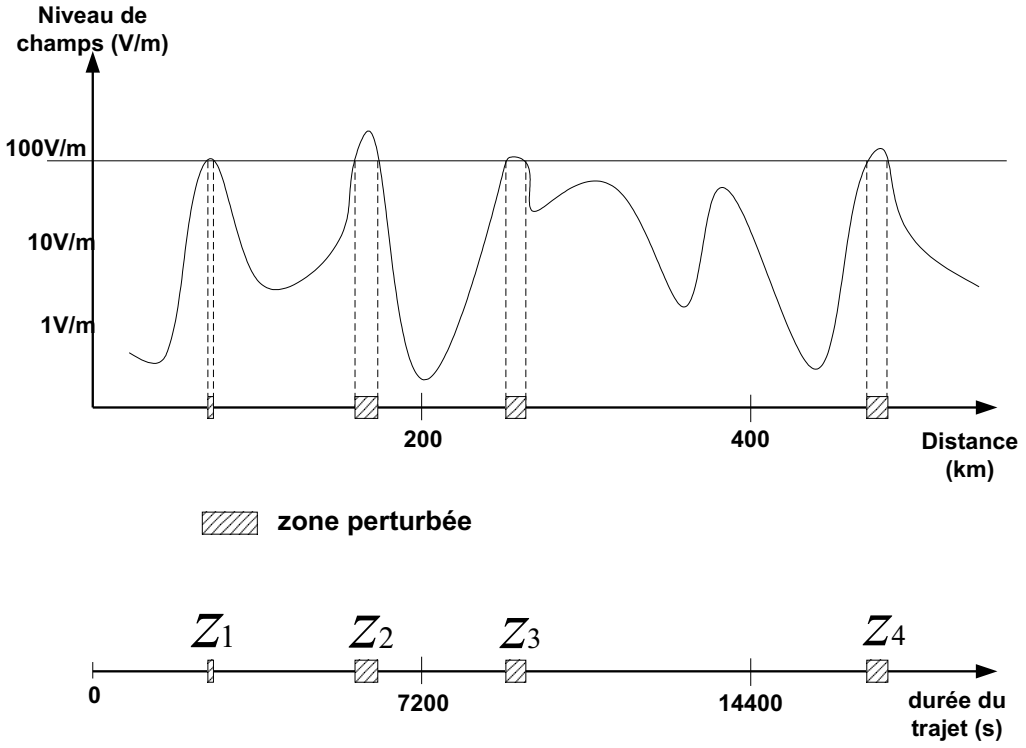

FIG. 6.5 – Distribution des perturbations pour un trajet de référence effectué en région très perturbée

6.7.2 Etude de sensibilité

L'intérêt de la méthode proposée dans ce document ne réside pas uniquement dans l'évaluation définitive de la Fiabilité Comportementale du système, mais aussi dans les études de sensibilités rendues possibles par la multiplicité des variables paramétrant la formule 6.3. On peut ainsi aisément évaluer l'influence du temps de cycle (ε_n) (et donc directement le pire retard pur tolérable T_{wcpd}) et de la robustesse du système en présence de perturbations dont le niveau dépasse celui spécifié en phase de test (P_{err}). S'il est évident que la robustesse du système est le principal "levier" pour augmenter la fiabilité comportementale du système, nous allons montrer que le choix de la durée du cycle de communication peut avoir une influence non-négligeable.

On rappelle les contraintes à respecter (voir paragraphe 1.7) :

– contrainte de sûreté : $\boxed{Pd_{trajet}(T, P_{err}) < 5 \times 10^{-10}}$

– contrainte sur le pire intervalle tolérable entre l'arrivée de 2 signaux valides : $\boxed{\tau_{max} = 38\,ms}$

La figure 6.6 montre quels sont les couples (P_{err}, ε_n) pour lesquels pour un trajet de référence effectué en région très perturbée, la contrainte de sûreté est respectée. Cette figure montre aussi la variation de la marge sur la durée de cycle en cas d'objectif de sûreté non tenu (jusqu'à 10^{-7}déf./trajet). En effet, il est plus facile de faire varier P_{err} que ε_n. A travers P_{err}, c'est toute l'architecture physique que l'on fait varier. En effet, les paramètres qui vont influer directement sur P_{err} sont la qualité de la conception des sous-systèmes, la redondance au sein du système même, et la diversification des éléments redondés.

Interprétation : La zone marquée par X nous permet de dimensionner l'architecture tout en respectant la contrainte de sûreté. Par exemple, pour un temps de cycle de 5ms, P_{err} peut être relachée jusqu'à 2×10^{-2} au lieu de 5×10^{-3}. Ou pour $P_{err} = 5 \times 10^{-3}$ on peut augmenter la durée de cycle jusqu'à 7ms. Par ailleurs, il est intéressant de constater que pour une probabilité d'erreur comprise entre 2×10^{-3} et 10^{-1} (ce qui parait être un intervalle raisonnable d'après le paragraphe 6.6.1), intervalle qui correspond à la partie marquée par X de la figure 6.6, il suffit de réduire le cycle d'1 ou 2 ms pour augmenter la Fiabilité Comportementale de l'architecture sans modifier sa robustesse. Or, généralement, l'ajustement de la durée d'une cycle n'est pas (ou peu) coûteux. Ainsi, si l'objectif de sûreté quantifé par la Fiabilité Comportementale n'est pas tenu, il est possible de l'atteindre sans forcément augmenter le coût du système. La figure 6.6 nous permet d'évaluer la marge sur la durée d'un cycle de communication pour une Fiabilité Comportementale donnée. Si la Fiabilité Comportementale évaluée est inférieure ou égale à 10^{-7}, la marge est représentée par la zone marquée par 0. L'étroitesse de la marge est un avantage considérable pour le concepteur qui, en réduisant de très peu le temps de cycle, peut ainsi aisément atteindre les objectifs de sûreté.

6.8 Application de la méthode en région moyennement perturbée

Les mesures récoltées au cours du trajet témoin sont représentées sur la figure 6.7. Comme précédemment, on peut extraire la distribution des perturbations représentées :

La figure 6.7 nous donne les valeurs suivantes :

$$\boxed{card(Z) = 2 \text{ et } Z = \{10, 5\}\text{(unités (s))}}$$

Soit :

– $r = 2$

– $Z_1 = 10s$

		longueur du cycle TDMA εn								
		2	3	4	5	6	7	8	9	10
	0.5									
	0.4									
	0.3									
	0.2	X								
	0.1	X	0							
	0.09	X	0							
	0.08	X	X							
	0.07	X	X	0						
	0.06	X	X	0						
	0.05	X	X	0						
	0.04	X	X	X	0					
Perr	0.03	X	X	X	0					
	0.02	X	X	X	V	0				
	0.01	X	X	X	X	X	0			
	0.0090	X	X	X	X	X	0			
	0.0080	X	X	X	X	X	0			
	0.0070	X	X	X	X	X	0			
	0.0060	X	X	X	X	X	X	0	0	
	0.0050	X	X	X	X	X	X	0	0	
	0.0040	X	X	X	X	X	X	0	0	
	0.0030	X	X	X	X	X	X	0	0	
	0.0020	X	X	X	X	X	X	X	X	
	0.0010	X	X	X	X	X	X	X	X	0

0 la probabilité d'occurrence de défaillance sur le trajet est inférieure à 5.10^{-7}

X la probabilité d'occurrence de défaillance sur le trajet est inférieure à 5.10^{-10}

FIG. 6.6 – Probabilité d'erreur maximale tolérable en fonction de la durée d'un cycle de communication pour un trajet de référence effectué en région très perturbée et marge sur la durée de cycle en cas d'objectif de sûreté non tenu (jusqu'à 10^{-7})

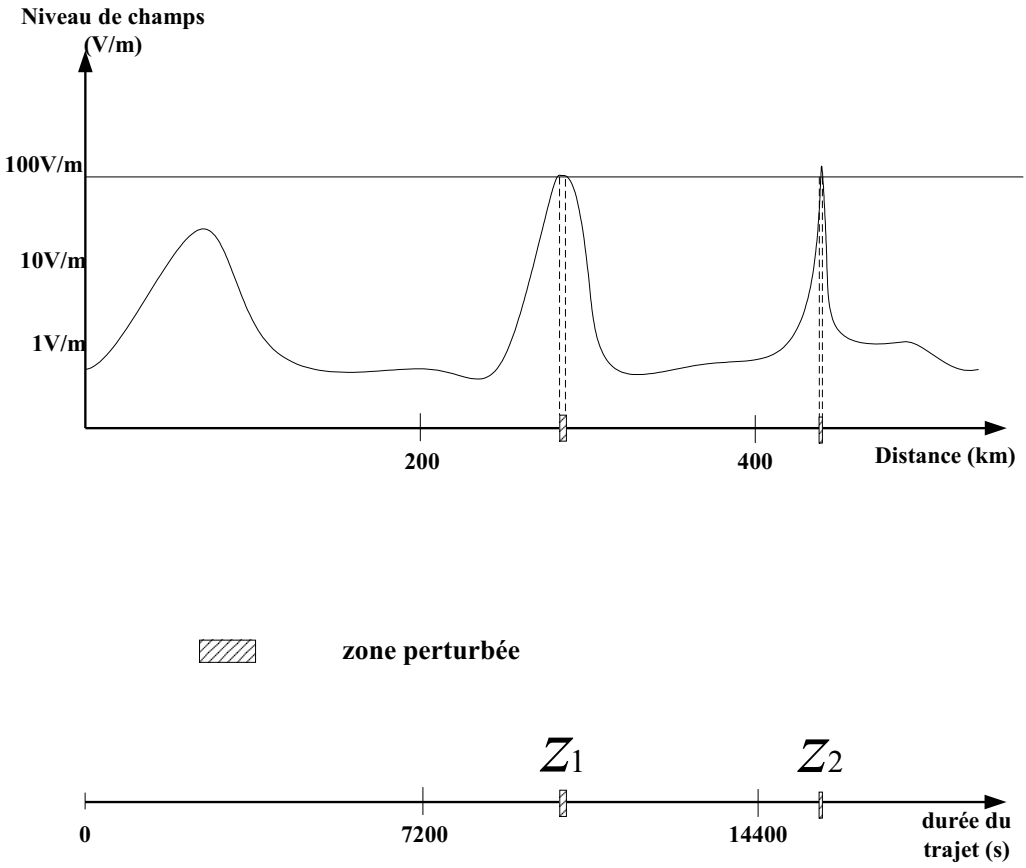

FIG. 6.7 – Distribution des perturbations pour un trajet de référence effectué en région moyennement perturbée

– $Z_2 = 5s$

6.8.1 Evaluation de la Fiabilité Comportementale pour un trajet témoin en région moyennement perturbée

Le calcul de la Fiabilité Comportementale donne :

$$\boxed{Pd_{trajet}(T, P_{err}) = 0}$$

Interprétation du résultat : Les conclusions sont par conséquent identiques à celles du trajet de référence effectué en région très perturbée.

6.8.2 Etude de sensibilité

La figure 6.8 montre la variation de la probabilité d'erreur P_{err} maximale tolérable en fonction de la durée d'un cycle de communication pour un trajet de référence effectué en région moyennement perturbée, ainsi que la variation de la marge sur la durée de cycle en cas d'objectif de sûreté non tenu (jusqu'à 10^{-7}).

Interprétation du résultat : en premier lieu, on remarque que la courbe est pratiquement identique à celle obtenue pour un trajet de référence en région très perturbée. Ainsi, dès que la probabilité d'erreur est supérieure à 5×10^{-3}, la durée d'un cycle de communication devient dimensionnante et elle doit toujours être inférieure à 7 ms.

6.9 Application de la méthode à un trajet de référence effectué en région peu perturbée

Les mesures récoltées au cours du traject témoin sont représentées sur la figure 6.9. On déduit de cette figure les quantifications suivantes :

$$\boxed{card(Z) = 1 \text{ et } Z = \{1\}\text{(unités (s))}}$$

Soit :
– $r = 1$
– $Z_1 = 1s$

6.9.1 Evaluation de la Fiabilité Comportementale

Le calcul de la Fiabilité Comportementale avec les paramètres énoncés ci-dessus nous donne :

$$\boxed{Pd_{trajet}(T, P_{err}) = 0}$$

Interprétation du résultat : l'exigence de sûreté est respectée. Par ailleurs, la criticité des systèmes et des défaillances associées sont telles que, si des systèmes X-by-Wire sont implantés dans des véhicules commercialisés en série dans quelques années, la majorité des trajets de référence devraient avoir une allure correspondant à celle de la figure 6.9. Si cette hypothèse était prouvée au moment de la mise à jour du rapport CEERF, l'architecture présentée à la figure 6.1 respecterait les contraintes de sûreté quantifié par la Fiabilité Comportementale pour une éventuelle commercialisation en série.

		longueur du cycle TDMA εn								
		2	3	4	5	6	7	8	9	10
Perr	0.5									
	0.4									
	0.3									
	0.2	X								
	0.1	X	X							
	0.09	X	X							
	0.08	X	X	0						
	0.07	X	X	0						
	0.06	X	X	0						
	0.05	X	X	X						
	0.04	X	X	X	0					
	0.03	X	X	X	0	0				
	0.02	X	X	X	X	0				
	0.01	X	X	X	X	X	0			
	0.0090	X	X	X	X	X	0	0		
	0.0080	X	X	X	X	X	0	0	0	
	0.0070	X	X	X	X	X	X	0	0	
	0.0060	X	X	X	X	X	X	0	0	
	0.0050	X	X	X	X	X	X	0	0	
	0.0040	X	X	X	X	X	X	0	0	
	0.0030	X	X	X	X	X	X	X	0	
	0.0020	X	X	X	X	X	X	X	0	0
	0.0010	X	X	X	X	X	X	X	X	0

0 la probabilité d'occurrence de défaillance sur le trajet est inférieure à 5.10^{-7}

X la probabilité d'occurrence de défaillance sur le trajet est inférieure à 5.10^{-10}

FIG. 6.8 – Probabilité d'erreur maximale tolérable en fonction de la durée d'un cycle de communication pour un trajet de référence effectué en région moyennement perturbée, et Marge sur la durée de cycle en cas d'objectif de sûreté non tenu (jusqu'à 10^{-7})

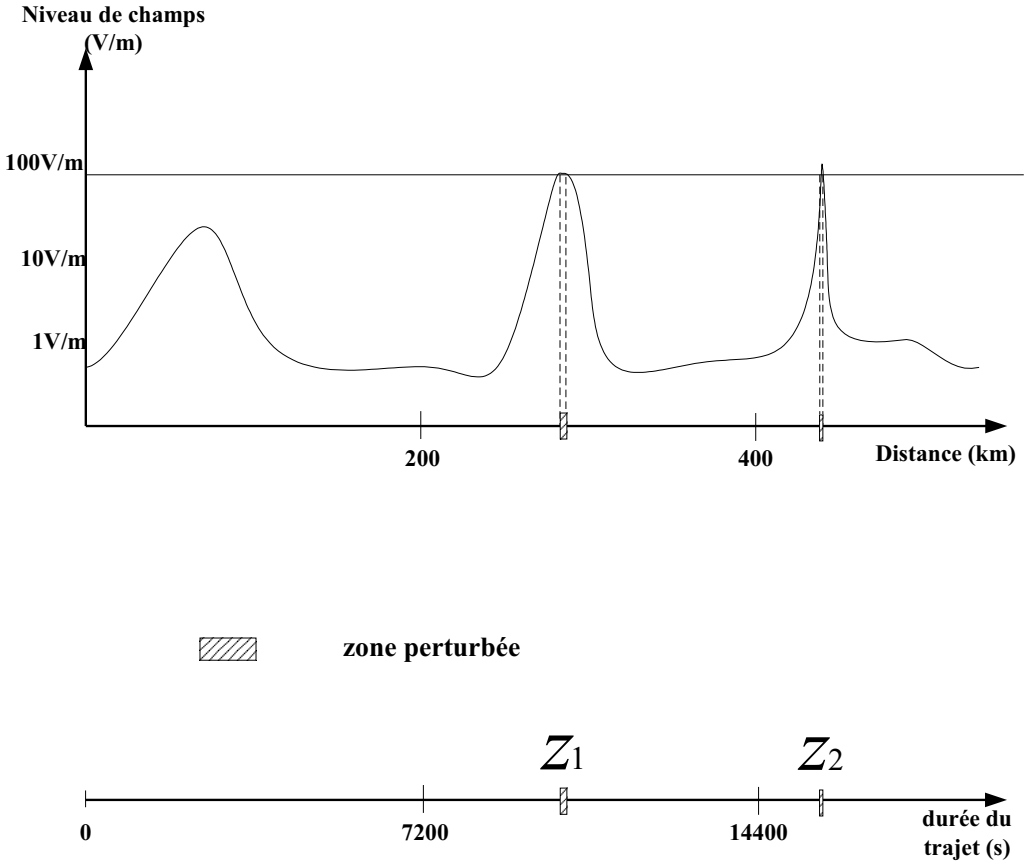

FIG. 6.9 – Mesures obtenues pour un trajet de référence effectué en région peu perturbée et distribution des perturbations

6.9.2 Etude de sensibilité

La figure 6.10 montre la variation de la probabilité d'erreur P_{err} maximale tolérable (pour respecter les contraintes énoncées ci-dessus) en fonction de la durée d'un cycle de communication pour un trajet de référence effectué en région moyennement perturbée, ainsi que la variation de la marge sur la durée de cycle en cas d'objectif de sûreté non tenu (jusqu'à 10^{-7}).

		longueur du cycle TDMA εn								
		2	3	4	5	6	7	8	9	10
Perr	0.5									
	0.4									
	0.3	**0**								
	0.2	**X**								
	0.1	**X**	**X**	**0**						
	0.09	**X**	**X**	**0**						
	0.08	**X**	**X**	**0**						
	0.07	**X**	**X**	**0**						
	0.06	**X**	**X**	**X**	**0**					
	0.05	**X**	**X**	**X**	**0**					
	0.04	**X**	**X**	**X**	**0**	**0**				
	0.03	**X**	**X**	**X**	**X**	**0**	**0**			
	0.02	**X**	**X**	**X**	**X**	**X**	**0**			
	0.01	**X**	**X**	**X**	**X**	**X**	**X**	**0**	**0**	
	0.0090	**X**	**X**	**X**	**X**	**X**	**X**	**0**	**0**	
	0.0080	**X**	**X**	**X**	**X**	**X**	**X**	**0**	**0**	
	0.0070	**X**	**X**	**X**	**X**	**X**	**X**	**0**	**0**	
	0.0060	**X**	**X**	**X**	**X**	**X**	**X**	**0**	**0**	
	0.0050	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**0**
	0.0040	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**0**
	0.0030	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**0**
	0.0020	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**0**
	0.0010	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

0 la probabilité d'occurrence de défaillance sur le trajet est inférieure à 5.10^{-7}

X la probabilité d'occurrence de défaillance sur le trajet est inférieure à 5.10^{-10}

FIG. 6.10 – Probabilité d'erreur maximale tolérable en fonction de la durée d'un cycle de communication pour un trajet de référence effectué en région peu perturbée

Si la courbe de la figure 6.10 a la même allure que celles obtenues pour des trajets de référence en région très et moyennement perturbées, sauf que la zone du respect de la sûeté est plus large. Ainsi pour une probabilité d'erreur de 5.10^{-10} le cycle de communication peut être étendu jusqu'à 9 ms.

En outre, si la contrainte de sûreté était de 10^{-9} déf./heure, la marge entre la Fiabilité Comportementale évaluée ici et la contrainte nous permettrait d'optimiser l'architecture. Cette optimisiation pourrait être réalisée selon 2 critères :

1. Le coût : dans ce cas, la qualité de la diversification ou de la redondance pourrait être revu à la baisse. Il est éventuellement possible de n'utiliser qu'un seul canal de communication (voir paragraphe 6.10) ou des rapprocher les canaux dans les cas d'une redondance double.
2. Le temps : on peut augmenter la durée d'un cycle de communication. Cette option peut être importante, notamment si le protocole de communication choisi est FlexRay. En effet, il sera tout à fait possible d'ajouter une partie dynamique au cycle de communication. Cette partir pourra être utilisée pour le transfert d'informations évenementielles dont certaines pourraient provenir de systèmes connexes au système Steer-by-Wire étudié. On peut aussi éventuellement se servir de la bande passante restante pour faire du diagnostic en ligne. Cependant, la durée du cycle de communication doit rester en adéquation avec les besoins en temps de réponse des différentes fonctions implémentées.

6.10 Influence du protocole de communication

Cette section s'attache particulièrement à montrer l'influence d'un mécanisme de détection d'erreur entraînant le passage en état "gelé" des noeuds sur la sûreté, mais aussi sur la disponibilité. En effet, le protocole de communication TTP/C propose un mécanisme de détection d'erreurs qui peut entraîner un "blackout" total du système si l'on applique notre modèle d'erreurs. Cependant, il faut garder à l'esprit que ce mécanisme peut être ajusté par le constructeur dans les couches supérieures et c'est dans ce sens qu'a été réalisée l'étude ci-dessous.

6.10.1 TTP/C

Les spécifications du protocole TTP/C [114] (page 28) nous indiquent que :

- TTP/C tolère toutes sortes de fautes qui n'affectent qu'une seule unité logique (par exemple un seul canal), sachant que chacune d'entre elles doit être répliquée.

- si un message répliqué est émis par 2 noeuds, la faute sera tolérée si la distance entre le début et la fin de la faute est inférieure à la distance entre les 2 fenêtre utilisées pour la transmission des 2 répliques.

- le flag "Communication system blackout" est mis à 1 si aucune activité n'est observée depuis au moins 1 TDMA Round. Le contrôleur entre alors en "freeze state" (état gelé) et arrête d'émettre et d'écouter ce qui se passe sur le réseau. Ce mécanisme peut amener le système dans un état critique, en effet, si chaque ECU adopte ce comportement, plus aucune information ne va circuler sur le réseau.

Ainsi, la perte d'un TDMA Round - ou d'un cycle de communication - complet ne fait pas partie des hypothèses de fautes sur lesquelles reposent les algorithmes de tolérance aux fautes du protocole de communication TTP/C, et cet événement entraîne le passage en état gelé de chacun des ECUs : on a alors $\eta_{max} = 1$. La stratégie proposée par PSA Peugeot Citroën dans le cas d'un passage en état gelé est de remonter immédiatement une alerte au conducteur pour qu'il stoppe le véhicule et le place en état sûr.

6.10.2 FlexRay

Les spécifications du protocole de communication FlexRay [37] ne donnent pas d'indication sur le passage en état gelé en cas d'erreurs détectées dans les trames reçues. L'erreur remontée dans le cas d'une erreur au moment du décodage de la trame est une "decoding error", mais qui n'entraînera aucun changement d'état au niveau du noeud. Par contre, le passage en état gelé pourra éventuellement se faire si le noeud détecte une erreur après un test interne de type BIST (Built In Self Test).

La politique du FlexRay-Group étant de laisser beaucoup de place au constructeur pour implanter ses propres mécanismes de tolérance aux fautes dans les couches supérieures du protocole de communication FlexRay, il est tout à fait possible de se servir des interruptions de type “decoding error” pour diagnostiquer des erreurs transitoires et ne forcer le passage du noeud en état gelé qu’en cas d’erreur transitoire de durée trop importante. Le paragraphe suivant propose une méthode pour le dimensionnement optimal de la durée avant le passage en état gelé.

6.10.3 Méthode de dimensionnement du temps avant la remontée d’une alerte au conducteur en cas d’erreur

Comme expliqué au chapitre 5, le système peut tolérer la perte de plusieurs cycles de communication consécutifs sans que la sécurité des occupants du véhicule ne soit entachée. Ainsi, il est possible d’attendre avant de remonter une alerte au conducteur. Cette attente peut permettre au système de réintégrer éventuellement un ou plusieurs sous-systèmes ayant subi une défaillance transitoire, mais aussi de tolérer les perturbations de très courte durée sans dégrader la sécurité. Si certaines perturbations sont tolérées et transparentes pour les passagers, les bénéfices en disponibilité peuvent être évidents.

Ainsi, si l’on considère qu’il faut approximativement 2 cycles de communication au système pour réintégrer proprement ses composants, le système peut attendre $\eta_{max} - 2$ (voir paragraphe 5.2.3) cycles de communication avant de remonter une alerte au conducteur. S’il l’on nomme N_{alerte} le nombre de cycles perdus tolérable avant la remontée d’alerte au conducteur, on peut écrire d’après la formule 5.1 :

$$\eta_{max} = \left\lfloor \frac{\delta_{max}}{\varepsilon_n} \right\rfloor \tag{6.5}$$

et $N_{alerte} = \eta_{max} - 2$
soit :

$$N_{alerte} = \left\lfloor \frac{\delta_{max}}{\varepsilon_n} \right\rfloor - 2 \tag{6.6}$$

Si on applique la formule 6.6 à l’architecture étudiée dans l’étude de cas précédente, on obtient :
$N_{alerte} = \left\lfloor \frac{38}{5} \right\rfloor - 2 = 3$

On peut alors quantifier la probabilité P_{stop} de s’arréter pendant le trajet de référence en région peu perturbée (on fait le choix de la région peu perturbée pour minimiser l’influence du trajet de référence sur le résultat) :

$$P_{stop} = Pd_{trajet}(T, P_{err})$$

$$Pd_{stop} = 1 - \prod_{i=1}^{r} \left[R(N_{alerte} + 1, \eta_{WC}(Z_i); P_{err})^{\eta_{WC}(Z_i)} \right]$$

La méthode proposée pour l’évaluation de N_{alerte} et de P_{stop} pourrait être utilisée pour le dimensionnement d’un algorithme de gestion de groupe, notamment dans le cadre d’une implémentation du protocole FlexRay qui laisse le soin au constructeur de développer cet algorithme en interne. On peut aussi imaginer une mise à jour de l’algorithme de membership de TTP/C qui laisse le soin au constructeur de paramétrer lui-même N_{alerte}

Conclusions générales sur la Partie 3

L'étude de cas présentée dans cette partie nous a permis de démontrer l'applicabilité de la méthode proposée. L'intégration de données pertinentes pour ce contexte (quantification des probabilités, architecture opérationnelle, multiplicité des trajets de référence, ...) et la cohérence des résultats obtenus montre l'intérêt direct de cette même méthode en vue d'une production en série de véhicules équipés de systèmes X-by-Wire.

En mode nominal, on remarque qu'il y a une marge importante entre la contrainte sur le retard pur et son évaluation analytique. L'importance de la marge nous indique clairement que la performance (ou qualité de service) telle que perçue par le conducteur est relativement élevée. Si la contrainte n'était pas respectée, il faudrait revoir l'architecture opérationnelle avant même d'évaluer sa Fiabilité Comportementale.

En ce qui concerne le mode perturbé, il est clair que le premier "levier" de la Fiabilité Comportementale est la probabilité qu'un cycle soit erroné au sein d'une zone perturbée, et donc la robustesse de l'architecture. Cependant, c'est aussi la quantification la plus coûteuse. En effet, l'augmentation de la robustesse d'une architecture passe par la redondance diversifiée au maximum des systèmes et une amélioration de la qualité de conception. Les résultats obtenus lors de l'étude de cas montrent qu'il est particulièrement compliqué de concevoir une architecture pour une exigence donnée. En effet, il faudrait alors construire des cycles de communication dont la durée serait d'une taille inférieure aux besoins en terme de transmission.

Contrairement à ce que l'on aurait pu attendre, le trajet de référence n'a pas une incidence prépondérente. En effet, les différences ne sont pas réellement significatives, notamment quant à la robustesse et au temps de cycle nécessaires pour éviter la défaillance catastrophique. Cette conclusion peut être intéressante pour modérer le pessimisme de l'évaluation de la Fiabilité Comportementale si l'approche choisie pour l'évaluation de la Fiabilité Comportementale est une approche pire cas avec un trajet de référence en région très perturbée.

Enfin, cette méthode permet de montrer l'influence de certains mécanismes imposés dans les protocoles de communication. En effet, notre méthode montre clairement que le mécanisme de passage en "blackout" du réseau tel que proposé par le protcole TTP/C peut être particulièrement contraignant en terme de disponibilité. Cependant, nous avons montré qu'il est possible de calculer une valeur optimale de la durée avant la remontée d'alerte au conducteur - si celle-ci est paramétrable, comme c'est le cas pour le protocole de communication FlexRay - sans que la sécurité des occupants ne soit impactée.

Chapitre 7

Conclusion

7.1 Contributions

L'apport de ces travaux de thèse est d'ordre méthodologique. Ils s'adressent aux ingénieurs en sûreté des fonctionnement des constructeurs et équipementiers du secteur automobile. L'objectif visé est d'offrir une méthode pour évaluer quantitativement l'influence des fautes transitoires dues à l'environnement et des performances temps réel, sur la probabilité d'occurrence de défaillance catastrophique du système (ou sûreté). L'idée est de considérer le système X-by-Wire comme un sous-système d'un système de plus haut niveau : le véhicule. Il s'agit alors d'étudier la qualité de service du système telle que perçue par le conducteur, et d'en évaluer les limites en cas de retard et de pertes d'échantillons. Pour des raisons contextuelles exprimées précédemment, seuls les systèmes de direction Steer-by-Wire sont étudiés dans ce document. En effet, les critères de qualité de service et les modèles de simulation associés fournis par la société PSA Peugeot Citroën concernaient uniquement les systèmes de direction. Il est cependant tout à fait envisageable d'utiliser des critères de qualité de service propres aux systèmes de freinage pour appliquer la méthode proposée à ces derniers.

Par ailleurs, la cohérence des résultats obtenus dans l'étude de cas, et notamment la faible influence des trajets témoins, démontre l'intérêt des critères et des méthodes d'évaluation sélectionnés. En effet, le projet ambitieux d'une évaluation a priori - et donc statique - du comportement du système en mode nominal et en mode perturbé - et donc aussi dynamique - aurait pu aboutir à des résultats incohérents ou peu significatifs par rapport aux préconisations précisées au chapitre 1. Or, les ordres de grandeurs obtenus en terme de probabilité de défaillance correspondent à ceux des exigences de sûreté préconisées.

Nous rappelons ci-dessous les principaux apports, détaillés dans les chapitres précédents, de la méthodologie proposée :

1. En terme d'évaluation de la sûreté :
   (a) spécification et justification de la contrainte de sûreté,
   (b) évaluation par simulations du pire retard pur tolérable par le véhicule,
   (c) évaluation analytique du pire retard pur dû à l'architecture opérationnelle sous hypothèse d'absence de perturbations,
   (d) évaluation de la Fiabilité Comportementale (probabilité qu'une faute transitoire liée à l'environnement entraîne une défaillance catastrophique) en mode perturbé,

(e) mise à disposition d'un modèle d'erreur créé à partir de statistiques réelles.

2. En terme d'aide à la conception et à la configuration d'un système soumis à une contrainte de sûreté :

   (a) pour un taux de défaillance évalué du composant et exprimé sous la forme de la probabilité qu'un cycle de communication soit erroné dans une zone perturbé, calcul de la durée maximale possible pour un cycle TDMA ; ceci apporte une aide à l'évolutivité du système (adjonction de stations émettrices, par exemple),

   (b) pour un cycle TDMA de durée donnée, calcul de la pire probabilité qu'un cycle TDMA soit erroné dans une zone perturbée (choix d'un type de diversification ou d'un médium de communication).

De plus, nous avons montré comment optimiser la disponibilité du véhicule dans le cas où le protocole de communication propose des mécanismes de détection d'erreurs.

Enfin, cette méthode repose sur des calculs de complexité faible (complexité en o(N), si N est le nombre maximal de cycles potentiellement perturbés dans une zone).

Il est important de garder à l'esprit que l'exigence exprimée sur la Fiabilité Comportementale évaluée par la méthode est nécessaire pour montrer que l'on respecte les exigences en terme de quantification de la sûreté, mais elle n'est pas suffisante, car seules les fautes transitoires d'interaction dues à l'environnement sont traitées. Cependant, l'un des résultats majeurs de ces travaux de thèse est de proposer ce type d'exigence et la méthode d'évaluation associée comme un nouveau critère dimensionnant dans l'évaluation de la sûreté de fonctionnement d'un système X-by-Wire.

En outre, nous avons montré dans ces travaux que la quantification en probabilité d'occurrence de défaillance par heure est relativement complexe à manipuler pour l'évaluation de phénomènes transitoires. Ainsi, dans le cadre d'une éventuelle normalisation, il est primordial que la discussion de la quantification de l'influence des phénomènes transitoires soit discutée et traitée différemment que dans la norme CEI 61508.

7.2 Perspectives

La méthodologie, telle que proposée dans le présent document, est limitée à l'influence des perturbations électromagnétiques sur la sûreté des systèmes Steer-by-Wire. En conséquence, il serait en premier lieu intéressant d'élargir son applicabilité à :

1. l'ensemble des systèmes X-by-Wire,
2. toutes les fautes transitoires liées à l'environnement modélisables selon la technique de modélisation exposée au chapitre 5.

La réponse à la perspective 1 ne devrait pas poser de problèmes majeurs, puisqu'il suffit aux constructeurs d'automobile d'utiliser leurs propres critères de qualité de service pour le système étudié. La technique proposée ici pour l'injection de faute sous Matlab/Simulink (voir Annexe A) devra être appliquées aux modèles disponibles[24]Il est aussi imaginable d'élargir le champs d'applicabilité de la méthode à l'ensemble des systèmes électroniques embarqués dans l'automobile dont les défaillances ont une influence quantifiable sur la qualité de service telle que perçue par l'utilisateur.

La réponse à la perspective 2 peut sembler plus complexe, les causes phénoménologiques des fautes transitoires étant encore aujourd'hui mal maîtrisées. Cependant, comme expliqué au paragraphe 5.5.6, il est possible

[24]Matlab/Simulink étant devenu un standard de facto, ces modèles sont disponibles dans les services concernés.

d'utiliser un procédé de diagnostic en ligne qui enregistre chaque occurrence de trame détectée comme erronée ou absente sur un trajet de référence. Si, par exemple, le protocole de communication utilisé était TTP/C, ce diagnostic serait simplifié par le mécanisme de détection d'erreurs inclus dans le service de "membership". Il serait alors possible de construire un spectre similaire à celui relevé pour les perturbations CEM, mais pour l'ensemble des fautes entraînant la perte d'une trame ou d'un cycle de communication. Dans cette optique, il serait intéressant de réduire l'atomicité de l'erreur à la fenêtre temporelle et non plus au cycle de communication, mais ce changement demanderait la reconstruction d'une partie du modèle d'erreur (voir [41] pour des travaux sur l'optimisation du placement des répliques dans le cycle de communication).

La conclusion du chapitre 2 avait soulevé le problème des deux hypothèses fortes qui devront dans l'avenir être relachées :

– la plus petite durée d'une défaillance de niveau système est un cycle de communication,
– les critères de qualité de service sont les mêmes en mode nominal et en mode perturbé.

La problématique de la durée minimale de la défaillance a été traîtée au paragraphe précédent. En ce qui concerne les critères de qualité de service des systèmes en mode perturbé, ces travaux doivent être effectués directement chez le constructeur automobile. Lui seul a le savoir et les équipement nécessaire pour réaliser les tests qui vont servir à modéliser le plus finement possible le comportement du système en mode perturbé. Par exemple, pour les systèmes de direction, on peut aisément imaginer une batterie de tests type Inscription en Courbe ou Sinus Balayé (voir chapitre 3) réalisés avec un "perdeur de trames" paramétrable embarqué. On pourrait alors aussi évaluer l'impact de paramètres tels que l'angle de la trajectoire, l'adhérence de la route ou la vitesse du véhicule sur le pire retard tolérable et sur le pire intervalle tolérable (voir paragraphe 4.2) entre l'arrivée de deux instances valides de signal (voir paragraphe 5.2.2).

En ce qui concerne le champ d'application de la méthode, celle-ci pourrait aisément être utilisée pour comparer l'influence de certains protocoles de communication sur la Fiabilité Comportementale et sur la disponibilité. Si cette idée a déjà été appliquée au mécanisme de "passage en en état gelé" au paragraphe 6.10, il serait intéressant d'élargir la comparaison à des protocoles de communications event-triggered comme le CAN, aujourd'hui embarqué dans une majorité des véhicules disponibles sur le marché. Pour ce faire, il faudrait non plus considérer le cycle de communication comme durée minimale d'une erreur, mais le slot. Les résultats obtenus nous permettraient de comparer notre modèle d'erreur avec ceux proposés par Borster [17] et Navet [82].

Enfin, plus en amont, le fait de tolérer la perte de m échantillons sur k inclut les systèmes X-by-Wire dans une classe de systèmes communément appelés les systèmes $(m, k) - firm$ [74], et plus généralement dans les Weakly-hard-real-time-systems [10]. Plusieurs travaux émergent aujourd'hui sur l'adaptation en ligne du système à la qualité de service [106], et notamment à l'état des échantillons au niveau du consommateur. Les systèmes X-by-Wire, et plus généralement les systèmes utilisant la réplication temporelle d'informations pour des besoins de tolérance aux fautes, pourraient ainsi être des cas d'application intéressants pour la communauté travaillant aujourd'hui sur les systèmes $(m, k) - firm$.

Notations

Notation	Grandeur
τ_{max}	Pire retard tolérable
$\tau_{max,Calage}$	Retard (intervalle entre l'acquisition d'une consigne conducteur et sa mise à disposition au niveau de l'actionneur) correspondant au seuil maximal tolérable de la note de Calage
$\tau_{max,Reponse\_Precision}$	Retard correspondant au seuil maximal tolérable de la note de Réponse Précision
$\tau_{max,Ecart\_Trajectoire}$	Retard correspondant à l'écart de trajectoire maximal tolérable
ε_c	Période d'échantillonnage de l'information
d_t	Durée d'exécution du traitement de l'information sur un calculateur "volant"
ε_t	Période d'activation des traitements sur un calculateur volant
ε_n	Durée d'un cycle de transmission sur le réseau
d	Intervalle de temps entre le dernier réplica du signal étudié et la fin du cycle
T_{WCPD}	Retard Pur Pire Cas
Z	Durée de traversée d'une zone perturbée
τ_{err}	Durée d'erreur sur les réplicas
$\delta_{max,Calage}$	Intervalle entre deux consommations valides d'instance correspondant au seuil maximal de la note de Calage
$\delta_{max,Ecart\_Trajectoire}$	Intervalle entre deux consommations valides d'instance correspondant au seuil maximal de la note de Réponse Précision
$\delta_{max,Ecart\_Trajectoire}$	Intervalle entre deux consommations valides d'instance correspondant à l'écart de trajectoire maximal tolérable
δ_{max}	Intervalle maximal tolérable entre deux consommations valides
η_{max}	Nombre de cycles de communication perdus maximal tolérable tels que $\eta_{max} = \delta_{max}/\delta_n$
$\eta_{WC}(Z)$	Nombre maximal de cycles de communication potentiellement affectés par une perturbation de durée Z
P_{err}	Probabilité de perdre toutes les répliques d'un message au sein d'un cycle en cas de perturbation
λ	Probabilité de défaillance d'un composant (et un seul) en cas de perturbation
N_{R_X}	Note de diversification du système X
r	Nombre de zones perturbées par trajet de référence

Table des figures

Annexes

Annexe A : simulateur

A.1/ Présentation de l'outil SimulinkCar

Matlab[25] est une plateforme de calcul, d'analyse et de visualisation numérique basée sur un langage de calcul scientifique de haut niveau utilisable pour une grande variété d'applications telles que le traîtement du signal, le traîtement d'images, la conception, le prototypage et le test des système de contrôle-commande, etc..., et Simulink est l'environnement graphique associé qui permet de modéliser et simuler des schémas blocs faciles à éditer. Des produits supplémentaires étendent l'environnement Simulink au moyen d'outils conçus pour des tâches spécifiques de modélisation et de conception, la génération de code, la mise en oeuvre d'algorithmes, les tests et les vérifications.

L'outil SimulinkCar est un modèle Simulink conçu par la société PSA Peugeot Citroën. Il permet au concepteur de disposer d'un modèle dynamique du véhicule et de son environnement dédié à l'automatique. Il s'agit d'un modèle assez proche de la réalité qui permet de simuler et dimensionner les lois de commande et des paramètres allant des caractéristiques propres au véhicule (type, vitesse...) aux caractéristiques du trajet (adhérence de la route, trajectoire...). Cet outil est interne à la société PSA Peugeot Citroën, et est donc entièrement dédié à la modélisation de véhicules Peugeot et Citroën. Nous avons donc utilisé l'environnement Matlab/Simulink pour simuler le comportement du système Steer-by-Wire (modèle Matlab/Simulink du système) dans un environnement véhicule spécifique (modèle SimulinkCar du véhicule et de l'environnement de test).

La figure 1 illustre cette approche. Le point d'entrée de notre modèle est donc un modèle de conducteur au sein duquel l'utilisateur paramètre le profil de la trajectoire selon le test à réaliser (ici : inscription en courbe). Ce profil est traduit en une consigne d'angle à la roue qui est le point d'entrée de notre modèle Steer-by-Wire. La position de la crémaillère telle que calculée par le système est alors transmise au modèle SimulinkCar qui peut alors alimenter tous les paramètres nécessaires à la simulation du parcours de la trajectoire par le conducteur.

A.2/ Modèle Simulink du système Steer-by-Wire

Le modèle présenté à la figure 2 est un modèle "gros grain" d'une architecture Steer-by-Wire. Pour des raisons de confidentialité, le modèle d'actionnement ne sera pas présenté dans cette annexe. Les blocs grisés sur la figures correspondent aux blocs ajoutés par nos soins au modèle existant et disponible chez PSA Peugeot Citroën au moment des travaux. En effet, le modèle disponible était continu, nous avons donc ajouté un bloqueur pour simuler l'échantillonnage des signaux (bloc échantillonnage). Nous avons aussi ajouté un générateur d'erreur et un bloc correspondant aux mécanisme de tolérance aux fautes inclus dans les lois de commande. Ces derniers nous ont permi de simuler un mode perturbé.

[25] http ://www.mathworks.com

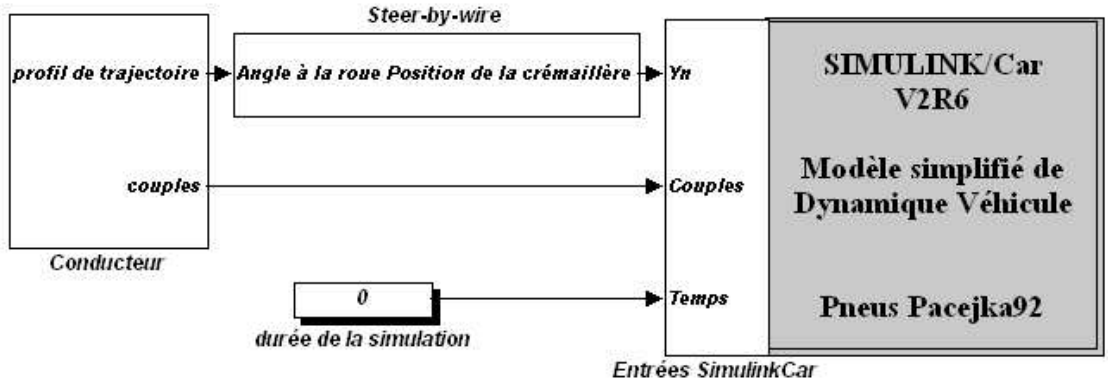

FIG. 1 – Intégration d'un modèle Simulink de système Steer-by-Wire dans SimulinkCar

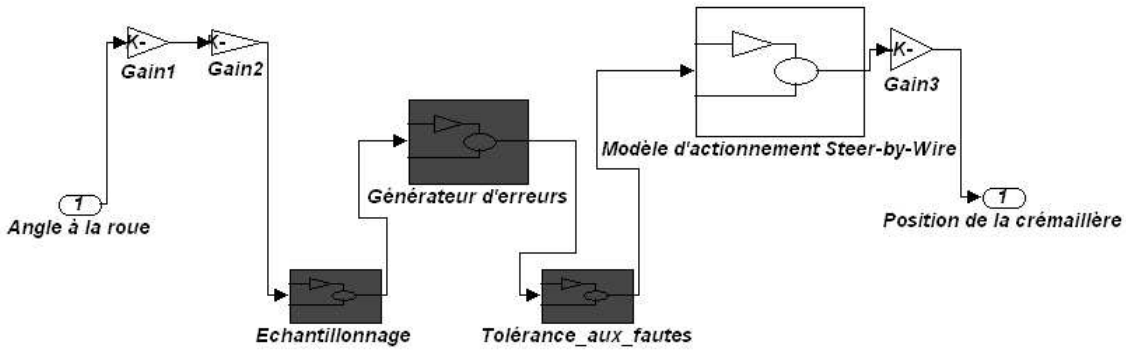

FIG. 2 – Modèle Simulink du système Steer-by-Wire (ERREUR !

A.2.1/ Echantillonnage du signal d'angle à la roue

Ce bloc permet de fournir un angle à la roue au modèle du système avec une périodicité équivalente à la durée d'un cycle de communication ε_n de l'architecture opérationnelle Steer-by-Wire étudiée. Pour ce faire, nous utilisons un bloqueur dont la période d'échantillonnage correspond à la durée du cycle de communication ε_n.

A.2.2/ Générateur d'erreur

Nous avons fait l'hypothèse au paragraphe 5.2.1 que la probabilité de recevoir et de ne pas détecter des valeurs erronnées est nulle. Ainsi, chaque échantillon erroné sera rejeté au profit du dernier échantillon valide. Nous avons donc modélisé le générateur d'erreurs de la figure 3.

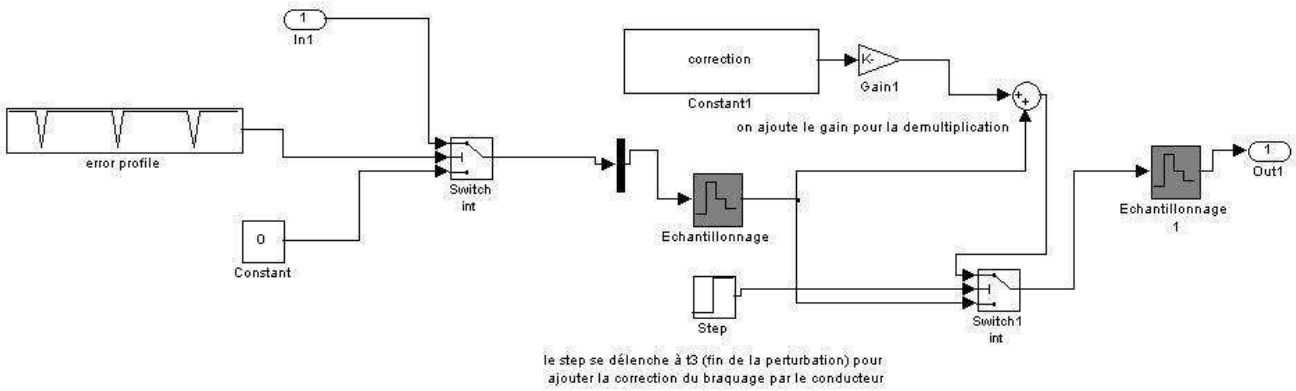

FIG. 3 – Générateur d'erreurs

Le profil d'erreur ajustable nous permet de répartir les erreurs sur toute la durée de la simulation. Il est possible d'agir sur l'instant d'arrivée de la perturbation comme sur sa durée. On fait donc varier ces paramètres au cours de simulations successives pour obtenir le pattern d'erreur correspondant au pire cas (voir paragraphe A.3.3).

A.2.3/ Tolérance aux fautes

Comme expliqué précédemment, les échantillons erronés sont rejetés au profit du dernier échantillon valide. Le bloc nous permettant de modéliser ce mécanisme de tolérance aux fautes est présenté à la figure 4.

En sortie de ce bloc, le signal est transmis à l'actionneur dont le bloc est représenté à la figure 2.

A.3/ Simulations

Un modèle continu Simulink simplifié d'une architecture fonctionnelle Steer-by-Wire a été développé au sein du projet Axones [30]. Ce modèle permet d'observer l'influence d'un retard constant de la consigne sur la qualité de service du système de direction simulé (voir chapitre 3) sur les critères de qualité de service étant le Calage et l'Ecart de trajectoire (les résultats donnés par le modèle d'environnement véhicule SimulinkCar pour le critère de réponse-précision ne sont pas satisfaisants).

A.3.1/ Simulation d'un test d'inscription en courbe

Le modèle simulé est un modèle continu simplifié permettant essentiellement de modéliser la limitation en vitesse et en accélaration qui inclus le retard propre aux actionneurs. Le bloc permettant de paramétrer le retard pur est un point d'entrée de ce modèle. Un angle à la roue par rapport à la position initiale est calculé à partir d'un profil de trajectoire. Un retard ou une perte de cette consigne a le même effet qu'un retard ou une perte de l'information angle volant. Un bloqueur d'entrée nous permet d'échantillonner la période de livraison des informations selon la durée du cycle de communication imposé par l'architecture opérationnelle. La consigne d'angle à la roue a donc l'allure de la figure 5.

La trajectoire imposée par le profil paramétré dans SimulinkCar doit quant à elle avoir l'allure de la figure 6. On voit bien sur les deux figures que la variation angulaire a lieu juste après 1s de simulation, ce qui correspond à un abscisse située entre 30 et 40m sur la trajectoire. C'est à cette période que la dérivée du signal d'entrée est maximale et que l'angle volant varie. La fin de la simulation correspond à l'émission d'une valeur constante.

A.3.2/ La recherche du retard pur maximal tolérable par simulation

Les informations obtenues en fin de simulation nous permettent d'évaluer la qualité de service du système en fonction du retard pur constant. On réalise alors une succession de simulations aux cours desquelles on va faire varier le retard pur, puis on utilise la formule suivante pour obtenir le retard pur maximal tolérable :

$$\tau_{max} = min(\tau_{max,Calage}, \tau_{max,Ecart\_Trajectoire}) \quad (1)$$

L'hypothèse de départ est que la note de Calage - au même titre que l'écart de trajectoire et la réponse/précision - est représentative de la qualité de service telle que perçue par le conducteur quel que soit son l'état du système

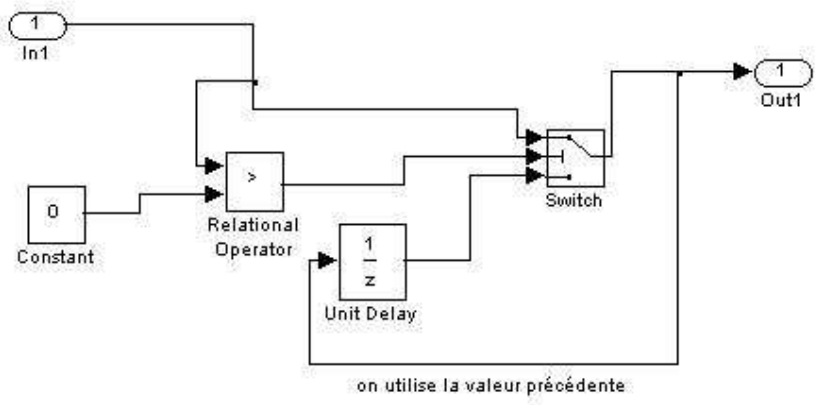

FIG. 4 – Remplacement des échantillons érronés par les derniers échantillons valides

X-by-Wire embarqué dans le véhicule. On utilise ainsi la méthode de recherche par simulation du retard pur maximal tolérable (voir paragraphe précédent) dans un contexte où le système est perturbé. L'idée étant d'évaluer l'influence des perturbations sur la note de Calage. Cependant, pour pouvoir générer des erreurs et modéliser plusieurs mécanismes déterminants en cas d'erreurs, ce modèle a été discrétisé et étoffé.

A.3.3/ La recherche du plus grand intervalle tolérable entre deux consommations valides d'instances d'un signal

Nous étudions ici le système en mode perturbé. Pour simuler ce mode, nous injectons des "0" dans la consigne d'angle à la roue représentée à la figure 5, sachant qu'un mécanisme détecte ces "0" (le bloc tolérance aux fautes), et délivre alors à l'actionneur la dernière instance de signal valide reçue (voir figure 7).

Les informations obtenues en fin de simulation nous permettent d'évaluer la qualité du système. On réalise alors une succession de simulations aux cours desquelles on va faire varier le début de la période d'erreur et sa durée jusqu'à obtenir le plus grand intervalle tolérable entre deux consommations valides d'instances d'un signal . Pour ce faire, on utilise la formule suivante, démontrée au paragraphe 5.2.2 :

$$\delta_{max} = min(\delta_{max,Calage}, \delta_{max,Ecart\_Trajectoire})$$

et correspond à un nombre maximal tolérable de cycles perdus $\eta_{max} = \frac{\delta_{max}}{\varepsilon_n}$.

La figure 8 nous donne la réponse du système correspondant pour un nombre maximal tolérable de cycles de communication $\eta_{max} = \frac{\delta_{max}}{\varepsilon_n}$.

L'hypothèse de départ est que la note de Calage - au même titre que l'écart de trajectoire et la réponse/précision - est représentative de la qualité de service telle que perçue par le conducteur quelque soit l'état du système X-by-Wire embarqué dans le véhicule. Onutilise ainsi la méthode de recherche par simulation du retard pur maximal tolérable (voir paragraphe précédent) dans un contexte où le système est perturbé. L'idée étant d'évaluer l'influence des perturbations sur la note de Calage.

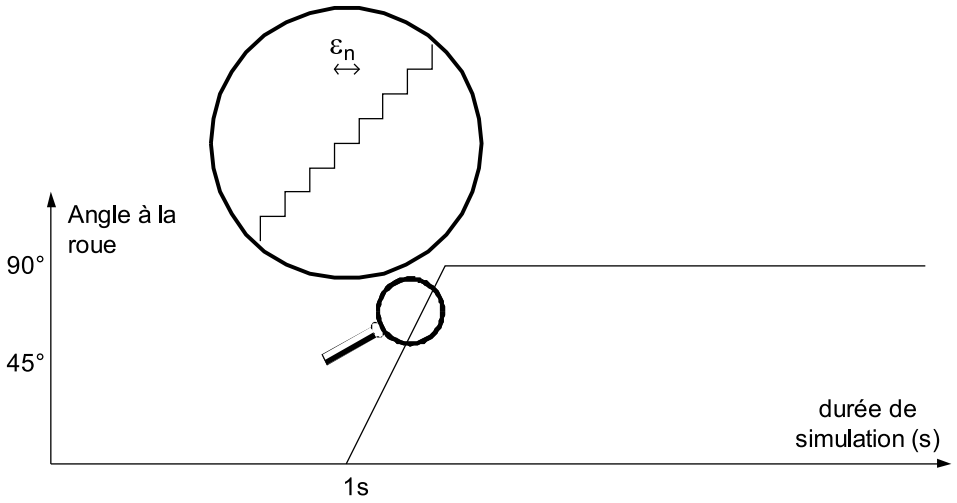

FIG. 5 – Consigne d'angle volant en degrés

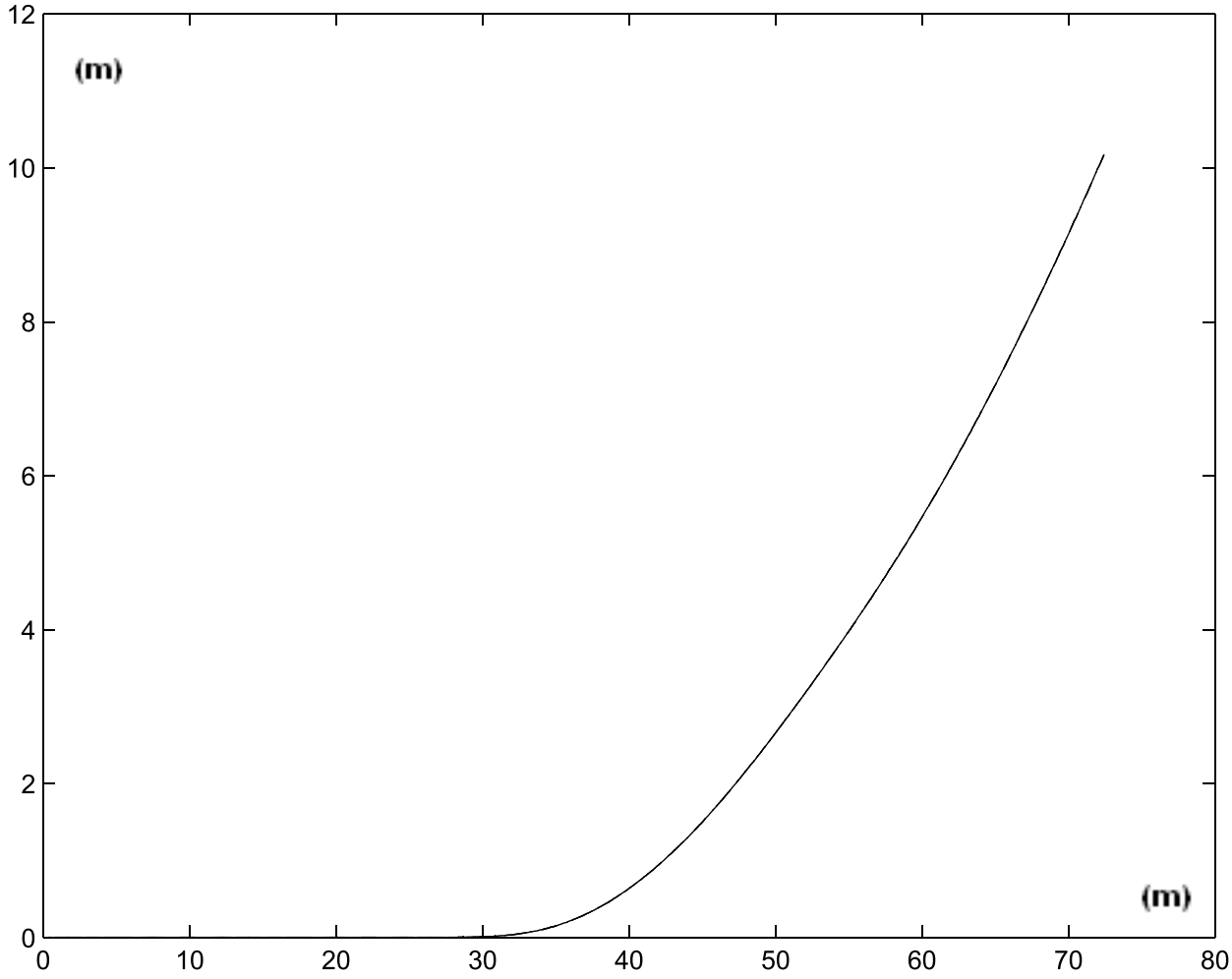

FIG. 6 – Trajectoire du test d'Inscription en Courbe

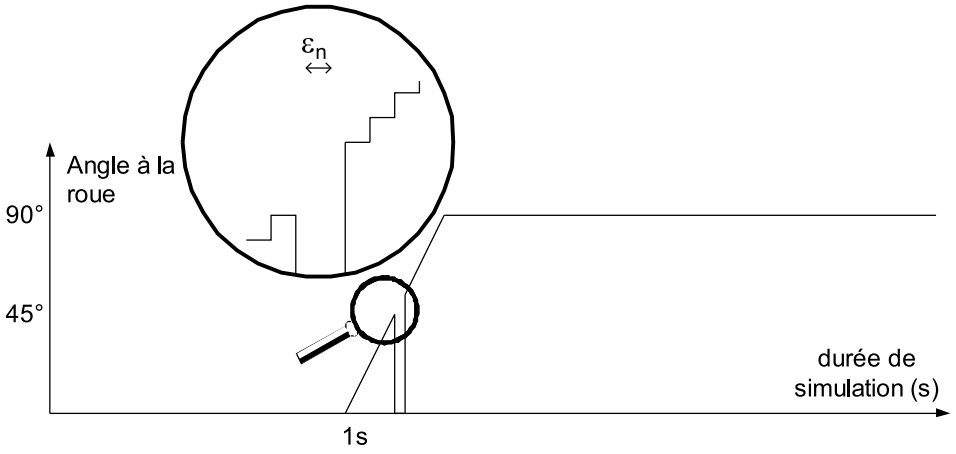

FIG. 7 – Injection d'erreurs dans la consigne angle volant

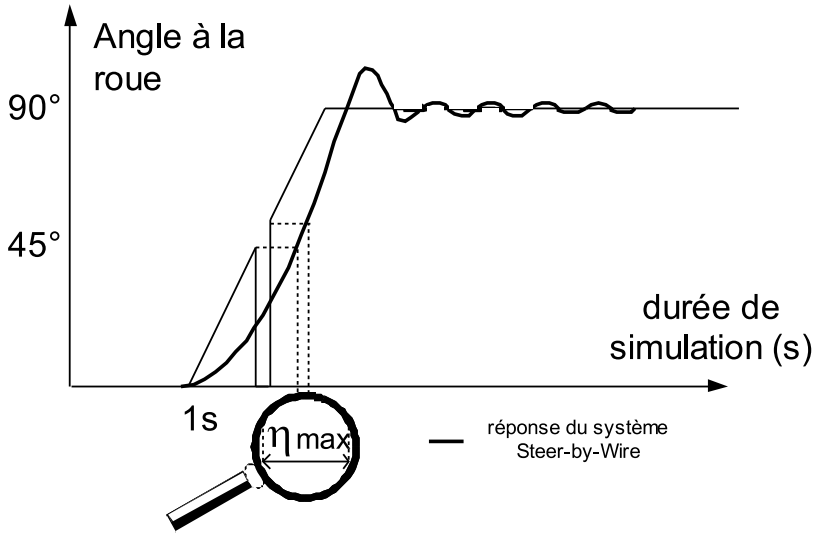

FIG. 8 – Réponse du système Steer-by-Wire pour un nombre maximal de cycle de communication perdus

Bibliographie

[1] Federal Aviation Administration. System safety handbook - chapter 3 : Principles of system safety. Technical report, Federal Aviation Administration, 2000.

[2] K. Akita and H. Nakamura. Safety and fault tolerance in computer-contyrolled railway signalling systems. *Dependable Computing for Critical Application*, pages 107–131, 1991.

[3] S. Allmaier and S. Dalibor. Panda - Petri net analysis and design assistant. In *Performance TOOLS'97*, Saint Malo, France, 1997.

[4] N. Andreff. Robustness to jitter in real-time systems. Technical Report ISRN LUTFD2/TFRT-5507-SE, Dept of Automatic Control, Lund Institute of Technology, Sweden, 1994.

[5] J. Arlat. Fault injection for the experimental validation of fault-tolerant systems. In *Workshop Fault-Tolerant systems*, pages 33–40, Kyoto, Japon, 1992.

[6] J. Arlat, Y. Crouzet, J. Karlsson, P. Folkesson, E. Fuchs, and G. Leber. Dependability assessment of the Mars Architecture by means of physical and software-implemented fault fnjection. Technical Report 99513, LAAS, 1999.

[7] P. Armengaud. Le X-by-Wire pour tous en stand-by. *Le journal de l'automobile*, page 22, october 2003.

[8] Y. Atamna. Réseaux de petri temporisés stochastiques classiques et bien formés : définition, analyse et application aux systèmes distribués temps réel. Master's thesis, Thèse de l'Université Paul Sabatier, Toulouse III, France, 1994.

[9] A. Avizienis, J-C. Laprie, B. Randell, and C. Landwher. Basic concept and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1) :11–33, janvier 2004.

[10] G. Bernat, A. Burns, and A. Llamosi. Weakly-hard real-time systems. *IEEE Transactions on Computers*, 50(4) :308–321, avril 2001.

[11] S. Blanc, J. Gracia, and P. J. Gil. A fault hypothesis study on the TTP/C using VHDL-based and pin-level fault injection techniques. In *17th IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT'02)*, Vancouver, Canada, 2002.

[12] A. Bondavalli, D. Latella, M. Dal Cin, and A. Pataricza. High-level Integrated Design Environment for Dependability (HIDE). In *Proceedings of the Fifth International Workshop on Object-Oriented Real-Time Dependable Systems*, page 87. IEEE Computer Society, 1999.

[13] J-C. Boudenat. Environnement radiatif naturel, dans : Influence de l'environnement radiatif naturel sur la fiabilité des systemes électroniques. *Veille Technologique*, 28, 2003.

[14] C. Bourroux. Qualité fiabilité le grand test. RTL Info : http ://www.rtl.fr/rtlinfo, 2003.

[15] Brite-Euram. X-by-wire - safety related fault tolerant systems in vehicles. Technical report, Brite-EuRam III Program, october 1998.

[16] I. Broster, A. Burns, and G. Rodriguez-Navas. Probabilistic analysis of CAN with faults. In *Proceedings of the 23rd Real-time Systems Symposium*, Austin,USA, Dec 2002. IEEE.

[17] I. Broster, A. Burns, and G. Rodríguez-Navas. Comparing real-time communication under electromagnetic interference. In *Proceedings of the 16th Euromicro Conference on Real-Time Systems*, pages 45–52, Catania, Italy, July 2004. IEEE Computer Society.

[18] K. Buchacker. Modeling with Extended Fault Trees. In *Fifth IEEE International Symposim on High Assurance Systems Engineering (HASE'00)*, Albuquerque, New Mexico, 2000.

[19] A. Burns, S. Punnekkat, L. Stringini, and D.R. Wright. Probabilistic scheduling guarantees for fault-tolerant real-time systems. In *7th International Working Conference on Dependable Computing for Critical Applications*, San Jose, California, U.S.A., 1999.

[20] E-J. Burr and G. Cane. End-To-End Arguments in system design. *Biometrika*, 48 :461–465, 1961.

[21] E. Bonhoure C. Wilwert and T. Clément. Application of the concept of behavioral and static reliability to the evaluation of steer-by-wire system dependability. In *Proceedings of Convergence 2004*, Detroit, USA, 2004.

[22] CEI. Compatibilité électromagnetique, techniques d'essais et de mesures, essais d'immunité aux décharges électrostatiques. CONFIDENTIEL service normes véhicules PSA Peugeot Citroen.

[23] CEI. Liste des termes de base, definitions et mathématiques applicables a la fiabilité. Publications 271 (1974), 271A (1978), 271B (1983), 271C (1985), 1985.

[24] CEI. Securite fonctionnelle des systemes électriques/électroniques/electroniques programmables relatifs a la sécurite- Partie 1 : Prescriptions généralités. CEI/IEC 61508-1 :1998, 1998.

[25] CEI. Securite fonctionnelle des systemes electriques/electroniques/electroniques programmables relatifs a la securite- Partie 4 : Définitions et abréviations. CEI/IEC 61508-4 :1998, 1998.

[26] CENELEC. Railway applications-safety related electronic systems for signalling, 2001.

[27] M-T. Chao, J-C. Fu, and M-V. Koutras. Survey of reliability studies of consecutive-k-out-of-n :F and related systems. *IEEE Transactions on reliability*, 44(1) :120–127, march 1995.

[28] D. Chayet. La mésaventure d'Hicham Dequiedt étonne les spécialistes mais un autre témoignage renforce les soupcons. *Le Figaro*, octobre 2004. édition du 4/10/04.

[29] P. Chevochot and I. Puau. Conception de systemes distribués temps réel strict tolerants aux fautes avec du matériel sur étagère. In *Real-Time Systems (RTS'01)*, Paris, France, 2001.

[30] T. Clément. Dossier de justification de la sous-specification technique globale steer by wire pour le vehicule pré-industriel. Technical report, PSA Peugeot Citroën, 2003. CONFIDENTIEL.

[31] J. Couvillion, R. Freire, R. Johnson, W. Douglas Obal, M. Akber Qureshi, M. Rai, W.H. Sanders, and J. E. Tvedt. Performability modeling with UltraSAN. *IEEE Software*, 8(5) :69–80, 1991.

[32] D.D. Deavours, G. Clark, T. Courtney, D. Daly, S. Derisavi, J. M. Doyle, W. H. Sanders, and P.G. Webster. The Moebius framework and its implementation. *IEEE Transaction on Software Engineering*, 28(10) :956–969, 2002.

[33] M. Debia and J. Zayed. Les enjeux relatifs a la perception et a la communication dans le cadre de la gestion des risques sur la santé publique. *VertigO :la revue en sciences de l'environnement sur le WEB*, 4(1), May 2003.

[34] E. Dilger, T. Fuhrer, B. Miller, and S. Poledna. The X-by-Wire Concept : Time-Triggered information exchange and fail silence support by new system services. Technical Report 7/1998, Technishe Universitat Wien, Austria, 2003. also available as SAE Technical Paper 98055.

[35] EN954. Standards EN954-1 Safety of Machinery - Safety-related Parts of Control Systems - Part 1 : General Principles for Design provides such a set of categories. EN954, 1997.

[36] J. Ferreira, P. Pedreiras, L. Almeida, and J-A. Fonseca. The FTT-CAN protocol for flexibility in safety-critical systems. *IEEE Micro*, 22(4) :46–55, July 2002.

[37] FlexRay-Consortium. Specification du protocole FlexRay, version 2.0. http ://www.flexray-group.com, 2003.

[38] G. Florin and S. Natkin. Les réseaux de Petri stochastiques. *Techniques et Sciences Informatiques*, 4(1) :143–160, 1985.

[39] J-C. Fu. Reliability of a large consecutive-k-out-of-n system. *IEEE Transactions on Reliability*, 34 :127–130, 1985.

[40] T. Führer, B. Muller, W. Dieterle, F. Hartwich, R. Hugel, and M. Walther. Time Triggered communication on CAN. Technical report, Robert Bosch GmbH, 2000.

[41] B. Gaujal and N. Navet. Optimal replica allocation for TTP/C based systems. In *5th FeT IFAC Conference (FeT'2003)*, Aveiro, USA, 2003.

[42] A. Goyal, P. Shahabuddin, P. Heddelberger, V.F. Nicola, and P.W. Glynn. A unified framework for simulating markovian models of highly dependable systems. *IEEE Transactions on Computers*, 41(1) :36–51, 1992.

[43] P. Grillinger and S. Racek. Simulation-based evaluation of TTP/C controller reintegration time. In *Applied Electronic 2002*, pages 71–74, Pilsen, Czech Republic, Sept 2002.

[44] P. Grillinger and S. Racek. Transient fault robustess evaluation of safety critical system using simulation. In *Baltic Electronic Conference*, pages 257–260, Talin, Estonia, 2002.

[45] R. Hammett and P. Babcock. Achieving 10-9 dependability with drive-by-wire systems. In *SAE - Society of Automotive Engineers*, Detroit, USA, 2003.

[46] B. Hedenetz and R. Belschner. Brake-by-wire without mechanical backup by using a TTP-Communication Network. In *SAE - Society of Automotive Engineers*, Detroit, USA, 1998.

[47] H-D. Heitzer and A. Seewald. Development of fault-tolerant steer-by-wire steering system. In *Proceedings of Convergence 2004*, Detroit, USA, 2004.

[48] C. Hennebert and G. Guiho. Sacem : A fault tolerant system for train speed control. In *23rd Int. Symp. on Fault-Tolerant Computing (FTCS-23)*, pages 624–628, Toulouse (France), 1993.

[49] P. Herout, S. Racek, and J. Hlavicka. Model-based dependability evaluation method for TTP/C applications. In *EDCC-4 - Fourth European Dependable Computing Conference*, pages 271–282, Toulouse, France, octobre 2002.

[50] J. Hu and K. Salisbury. Temperature spectrum of an automotive environnment for fatigue reliability analysis. Technical report, november 1994.

[51] F-K Hwang. Simplified reliabilities for consecutive-k-out-of-n :F systems. *Algebric Discrete Methods*, 7 :258–264, 1986.

[52] Ing.-Automobile. Vers une approche globale de la dynamique vehicule. *Ingenieurs de l'automobile*, pages 24–33, août 2000. traduction francaise de l'article original.

[53] ISO. Vehicules routiers : perturbations électriques par rayonnement d'énergie electromagnetique en bande etroite, méthode d'éssai d'un équipement - genéralites et definitions. CONFIDENTIEL service normes véhicules PSA Peugeot Citroen.

[54] IST-10748. Fault injection for TTA-FIT/report deliverable 3. Technical Report deliverable 3, TU Wien, Chalmers, Motorola, Volvo, UP Valencia, Carinthia TI, Czech TU, TTTECH, 2001.

[55] IST-10748. Fault injection for TTA-FIT/combined report. Technical Report deliverable 5.1-5.5, TU Wien, Chalmers, Motorola, Volvo, UP Valencia, Carinthia TI, Czech TU, TTTECH, 2002.

[56] D-P. Reed J-H. Saltze and D-D. Clark. End-to-end arguments in system design. *ACM Transactions on Computer Systems*, 2(4) :277–288, nov 1984.

[57] D. Jampi. Détermination d'une méthodologie d'aide a la conception d'un systeme de contrôle-commande numérique sur de fonctionnement. Master's thesis, CRAN-INPL, 2001.

[58] G. Juanole and I. Blum. Influence des fonctions de base (communication-ordonnancement) des systèmes distribués temps-reel sur les performances d'application de contrôle-commande. In *7ème Colloque Francophone sur l'Ingénierie des Protocoles (CFIP)*, 1999.

[59] F. Jumel. Définition et gestion d'une qualité de service pour les applications temps-réel. Master's thesis, LORIA - INPL, november 2003.

[60] K. Kanoun and L. Blain. SURF-2 - A tool for modeling and evaluation of dependability measures. In *IPDS'96 : Proceedings of the 2nd International Computer Performance and Dependability Symposium*, page 61. IEEE Computer Society, 1996.

[61] T.A. Kelm. 42 volts - the view from today. In *Proceedings of CONVERGENCE 2004*, Detroit, USA, october 2004. SAE.

[62] R. Klein. Normes de compatibilité électromagnétiques. *Hygiène et sécurité du travail*, 181, 2000.

[63] A. Kleyner and P. Pavan. Reliability prediction of substitute parts based on component temperature rating and limited accelerated test data. In *Reliability and Maintainability Symposium*, Tampa, USA, 2003.

[64] H. Kopetz. A comparison of CAN and TTP. Technical report, Technishe Universitat Wien, Austria, 1998.

[65] H. Kopetz. A comparison of TTP/C and FlexRay. Technical Report 10/2001, Technische Universität Wien, Institut für Technische Informatik, 2001.

[66] H. Kopetz, H. Kantz, G. Grünsteidl, P. Puschner, and J. Reisinger. Tolerating transient faults in MARS. In *Proc. 20th IEEE Symposium on Fault Tolerant Computing*, pages 466–473, June 1990.

[67] P-B. Ladkin and W. Schepper. Emi twa 800 and swissair 111. Technical Report RVS-Occ-00-01, University of Bielefeld - Faculty of technology, 2001.

[68] M. Lambris and S.G. Papastavridis. Exact reliability formulas for linear and circular consecutive-k-out-of-n :F systems. *IEEE Transactions on Reliability*, 34 :124–126, 1985.

[69] L. Lamport. The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, 4(3) :382–401, 1982.

[70] J-P. Landragin. Avec le 42v, l'automobile aborde la révolution du tout-électrique. *Electronique Magazine*, 2003.

[71] J-C. Laprie. *Guide de la Sûreté de Fonctionnement*. Cépaduès, 1995.

[72] J-C. Laprie. Presentation : state of art on dependability, october 2003.

[73] C. Liu and J. Layland. Scheduling algorithm for multiprogramming in a hard real-time environment. *Journal of ACM*, 29(1), 1973.

[74] M. Hamdaoui M. and P. Ramanathan. A dynamic priority assignment technique for streams with (m, k)-firm deadlines. *IEEE Transactions on Computers*, 44(4) :1443–1451, décembre 1995.

[75] D-A. Mackall. Development and flight test experiences with a flight-crucial digital control system. Technical Report NASA Technical Paper 2857, NASA Ames Research Center, 1988.

[76] J.A. McDermid. Trends in system safety : a european view. In *Proceedings of the 7th Workshop on Safety Critical Systems and Software*, Adelaide, Australie, 2002.

[77] J-F Meyer. Closed form solutions of performability. *IEEE Transactions on Computers*, 31(37) :648–657, 1982.

[78] MISRA. Development guidelines for vehicle based software, 2001.

[79] G. Mousty. Processus et méthode de sûreté de fonctionnement applicable au by-wire. In *Real-Time Systems (RTS'03)*, Paris, France, 2003.

[80] M. Muselli. New improved nounds for reliability of consecutive-k-out-of-n systems. *J. Appl. Prob.*, 37 :1164–1170, 2000.

[81] N. Navet. Evaluation de performances temporelles et pptimisation de l'ordonnancement de tâches et de messages. Master's thesis, LORIA - INPL, november 1999.

[82] N. Navet, Y-Q. Song, and F. Simonot. Worst-case deadline failure probability in real-time applications distributed over CAN. *Journal of Systems Architecture*, 46(7), 2000.

[83] NFR. Véhicules routiers : qualite de l'immunité aux perturbations électromagnetiques en chambre semi-anéchoidique. CONFIDENTIEL service normes vehicules PSA Peugeot Citroen.

[84] M. Nicholaidis. Problème des erreurs transitoires en technologie sous-micronique : l'approche d'iroc dans : Influence de l'environnement radiatif naturel sur la fiabilité des systèmes electroniques. *Veille Technologique*, 28, 2003.

[85] J. Nilsson. Real time control systems with delays. Master's thesis, Lunch Institute of technology, Sweden, 1998.

[86] K. Ogata. *Discrete-time control systems*. Prentice-Hall, Inc., 1987.

[87] H.J Otway and J.J. Erdmann. Reactor safety and design from a risk view point. *Nuclear Engineering and Design*, 13, 1970.

[88] Y. Papadopoulos and J.A. McDermid. The potential for a generic approach to certification of safety-critical systems in the transportation service. *Journal of Reliability Engigeering and System Safety*, 63 :47–66, 1999.

[89] A. Pedrono. Caractérisation de l'environnement électromagnetique routier. Technical report, INRETS, 2000.

[90] H. Pfeifer. Formal analysis of fault-tolerant algorithms in the time-triggered architecture. Master's thesis, Université d'Ulm, 2003.

[91] M. Plankenstein. Presentation : a comparison of TTP, TTCAN, FlexRay, 2003.

[92] S. Poledna, P. Barrett, A. Burns, and A. Wellings. Replica determinism and flexible scheduling in hard real-time dependable systems. *IEEE Transactions on Computers*, 49(2) :100–111, 2000.

[93] P. Ponticel. Industry taking active stance on safety. *Automotive Engineering International*, 112(4) :42, april 2004.

[94] PREDIT-CEERF. Caractérisation de l'environnement electromagnétique routier en france. Technical report, ATDI, INRETS, LRPC, PSA Peugeot Citroën, Renault, UTAC, 2003. CONFIDENTIEL.

[95] PSA. Specification technique globale d'environnement des équipements électriques et électroniques caractéristiques électriques. CONFIDENTIEL service normes vehicules PSA Peugeot Citroen, 2001.

[96] QS9000. Quality system requirement : QS 9000, 1988.

[97] R. Roy. Dossier compatibilité électromagnetique : maîtriser la CEM. Technical report, CETIM-Informations, 2001.

[98] RTCA-Inc. DO-178B : Software Considerations in Airborne Systems and Equipment Certification, 1992.

[99] J. Rushby. A comparison of bus architectures for safety-critical embedded systems. Technical report, Computer Science Laboratory SRI International, 2003.

[100] SAE. I.r. Class C Multiplexing, Part 1, Applications Requirements. Standard SAE, 1993.

[101] SAE. Public discussion : 42 volts electrical systems and fuel cells : harmonious marriage or incompatible partners ?, 2003. Technical discussion between : General Motors (Ch.Borroni-Bird, Director of Design and Technology Fusion), Delphi (J.Botti, Innovation Center), Daimler Chrysler (T.Moore, Vice President, Liberty and Technical Affairs), UTC Fuels Cells (F.R.Preli, Vice President, Engineering).

[102] E. Scarry. TWA 800 and electromagnetic interference : work already completed and work that still needs to be done. *The New York Review of Books*, 47(14) :47–66, 2000.

[103] R. Schoenig. Exemple de calcul de la fiabilité d'un système hybride. In *4ème Conférence Internationale sur l'Automatisation Industrielle*, Montreal, Canada, june 2003. SEE.

[104] Sécurite-Routière. Bilan de l'accidentologie de l'annee 2003. Technical report, La Securite Routiere, 2003.

[105] Sextant. La problematique des neutrons atmospheriques dans les nouvelles technologies, dans : Influence de l'environnement radiatif naturel sur la fiabilité des systèmes électroniques. *Veille Technologique*, 28, 2003.

[106] Y-Q. Song and A. Koubâa. Gestion dynamique de la QdS temps rél selon (m,k)-firm. In *Ecole d'été Temps Réel 2003 ETR 2003*, pages 327–342, Toulouse (France), 2003.

[107] C. Starr. Social benefit versus technological risk. *Science*, 165, 1969.

[108] C. Temple. Avoiding the babbling-idiot failure in a Time-Triggered communication system. In *International Symposium on Fault-Tolerant Computing (FTCS)*, Munich, Germany, 1998.

[109] P. Thambidurai and Y-K. Park. Interactive consistency with multiple failure modes. In *7th Symposium on Reliable Distributed Systems*, pages 93–00, Columbus, USA, 1988. IEEE Computer Society.

[110] K. Tindell and A. Burns. Guaranteed message latencies for distributed safety critical hard real-time networks. Technical Report YCS 229, Dept. Computer Science Univ. of York, 1994.

[111] K. Tindell, H. Hansson, and A. Welling. Analysing Real-Time Communication : Controller Area Network (CAN). In *IEEE RTSS'94*, S. Juan, Dec 2003. IEEE.

[112] M. Torngren. Modelling and design of distributed real-time control application. Master's thesis, Royal Institute of Technology, KTH, Sweden, 1995.

[113] M. Törngren. Fundamentals of implementing real-time control applications in distributed computer systems. *Real-Time Systems*, 14 :219–250, 2003.

[114] TTTECH. Specification du protocole TTP/C, version 1.1. http ://www.tttech.com, 2002.

[115] R. Velazco. Méthodes et outils pour la prédiction des taux d'erreurs provoques par des SEUs (Single Event Upsets) dans des architectures digitales dans : Influence de l'environnement radiatif naturel sur la fiabilité des systemes électroniques. *Veille Technologique*, 28, 2003.

[116] A. Verdevoye. Les voitures francaises sont perdantes sur la qualité. *La Tribune*, août 2002. édition du 1/08.

[117] A. Villemeur. *Sûrete de Fonctionnement des Systèmes Industriels*. Eyrolles, 1988.

[118] J. H. Wensley, L. Lamport, J. Goldberg, M. W. Green, K. N. Levitt, P. M. Melliar-Smith, R. E. Shostack, and C. B. Weinstock. Sift : The design and analysis of a fault-tolerant computer for aircraft control. *IEEE Proc*, 66(10) :1240–1255, october 1978.

[119] C. Wilwert, A. Charlois, and F. Gailliègue. Les services réseaux pour les systemes x-by-wire. In *Real Time Systems Conference (RTS03)*, Paris, France, 2003.

[120] C. Wilwert, N. Navet, Y-Q. Song, and F. Simonot-Lion. *Design of Automotive X-by-Wire Systems dans The Industrial Communication Technology Handbook*. CRC Pres, december 2004.

[121] E. Zanoni and P. Pavan. Improving the reliability and safety of automotive electronics. *IEEE Micro*, 13 :30–48, 1993.

[122] C. Ziegler. Sûrete de fonctionnement d'architectures informatiques embarquées sur automobile. Master's thesis, INPT-LAAS, Juillet 1996.

[123] G. Zwingelstein. Sûrete de fonctionnement des systèmes industriels complexes. *Techniques de L'Ingénieur*, S(4), 1999.