Conduite autonome : savoir concilier sécurité fonctionnelle et réduction des coûts

Dans les voitures totalement autonomes, le conducteur est totalement absent de l'équation. Les systèmes critiques pour la sécurité doivent donc agir comme des « systèmes opérationnels même en cas de défaillance ». Bien que cet objectif puisse être atteint grâce à une redondance totale des équipements, des architectures alternatives minimisant la duplication des fonctions et des systèmes sont nécessaires pour éviter les coûts et le poids liés à une redondance complète. Explication de NXP Semiconductors.

AUTEURS

Luc Van Dijk, IC Architect, Bart Vermeulen, Technical Director, et Alison Young, Functional Safety Architect, NXP Semiconductors.

L'objectif principal de la conduite autonome est d'éliminer les accidents causés par l'erreur humaine. L'éventuelle reprise en main par le conducteur en cas de panne du système n'est plus une option, car il n'y a pas de « conducteur » et aucune commande manuelle n'est prévue pour prendre le relais. Au lieu de s'appuyer sur un « système humain de secours », les systèmes critiques pour la sécurité doivent agir comme des « systèmes opérationnels même en cas de défaillance ». Bien que cet objectif puisse être atteint grâce à une redondance totale des équipements, des architectures alternatives minimisant la duplication des fonctions et des systèmes sont nécessaires pour éviter les coûts et le poids liés à une redondance complète.

Dans ce cadre, les architectures de réseau automobile adoptent une structure zonale afin de réduire le poids et le coût des véhicules pour une plus grande économie de carburant, des gains d'espace et un prix plus abordable. En raison du nombre croissant de fonctions critiques vis-à-vis de la sûreté de fonctionnement, la sécurité fonctionnelle est cruciale. Nous nous concentrerons principalement sur la contribution du réseau embarqué à la violation d'un « objectif de sécurité » dans les architectures zonales, par rapport aux architectures traditionnelles de réseaux de véhicules.

Architectures de domaines et de zones

La figure 1 compare les topologies typiques des architectures de véhicule par domaine et par zone. A gauche, dans l'architecture reposant sur les domaines, les capteurs et les actionneurs sont connectés en fonction du domaine fonctionnel auquel ils appartiennent. Chaque domaine dispose d'un processeur qui lui est propre en tant que contrôleur de domaine. A droite, dans l'architecture zonale, les capteurs et les actionneurs sont connectés en fonction de leur emplacement physique dans le véhicule. Les contrôleurs de zone, le module de calcul central ou une combinaison des deux gèrent les tâches de traitement traditionnellement exécutées par les contrôleurs de domaine et la passerelle centrale.

Le trafic de données hautement prioritaires, telles que les commandes de contrôle critiques pour la sécurité et certains types de données de capteur, doit atteindre sa destination et répondre dans un délai maximum spécifique. Pour le trafic de priorité moyenne, comme les données de divertissement embarquées, un temps de transmission et de réponse acceptable peut être maintenu en veillant à ce que, en moyenne, une bande passante de transmission suffisante soit disponible dans le sous-système de communication. Le trafic de données de type « best effort », quant à lui, n'est soumis à aucune exigence spécifique en matière de latence. Il suffit que les données arrivent finalement à leur destination et « aussi vite que possible », y compris la retransmission des informations au cas où les limites du sous-système de communication seraient atteintes pendant un certain temps.

Évolution et sécurité fonctionnelle

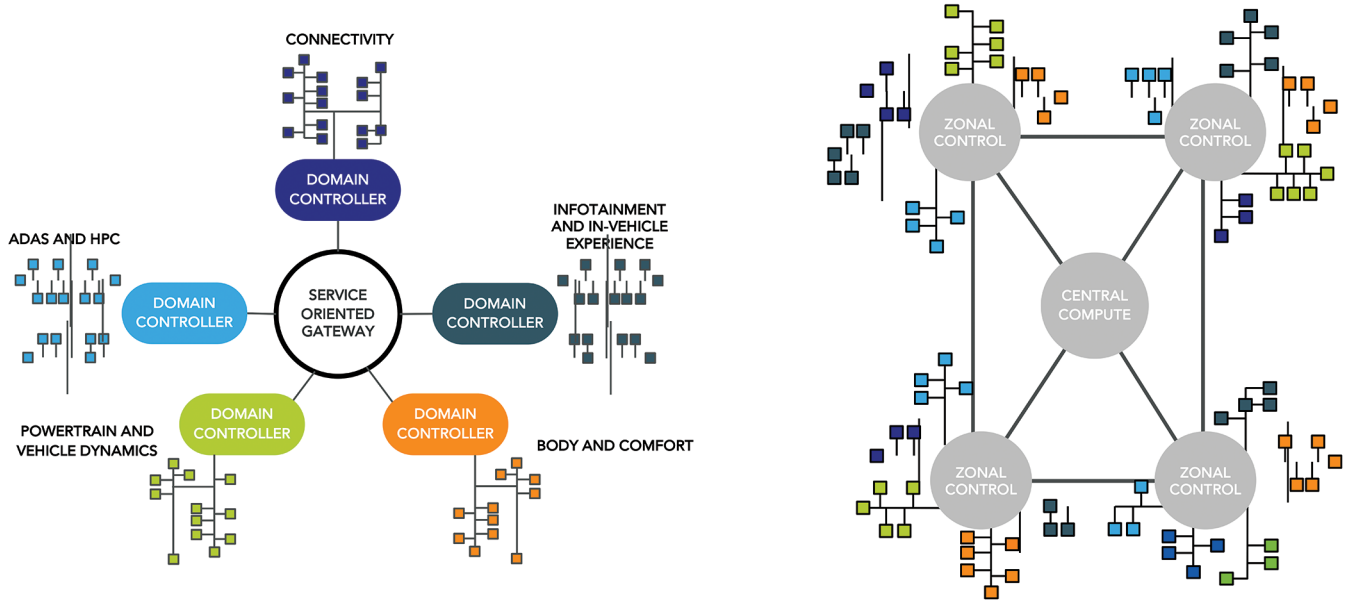
L'étude d'un système de freinage autonome permet d'expliquer les effets des architectures de domaine et de zone sur le niveau d'intégrité de sécurité automobile ASIL (Automotive Safety Integrity Level) souhaité, tel que défini par la norme ISO 26262. La figure 2 illustre un exemple de flux de données pour un système de freinage autonome.

Les cases marquées en noir sur la figure 2 sont des unités de commande électroniques ECU (Electro-

●Dans un véhicule totalement autonome, les systèmes critiques pour la sécurité doivent agir comme des « systèmes opérationnels même en cas de défaillance » car aucun humain ne peut venir à la rescousse.

1 TOPOLOGIES TYPIQUES DES ARCHITECTURES DE VÉHICULES PAR DOMAINE ET PAR ZONE.

A gauche, dans l'architecture reposant sur les domaines, les capteurs et les actionneurs sont connectés en fonction du domaine fonctionnel auquel ils appartiennent. Chaque domaine dispose d'un processeur qui lui est propre en tant que contrôleur de domaine. A droite, dans l'architecture zonale, les capteurs et les actionneurs sont connectés en fonction de leur emplacement physique dans le véhicule.



nic Control Units) et les cases marquées en gris représentent les informations échangées entre les ECU. L'unité radar envoie des données radar à la fonction de détection d'objet, qui extrait des données sur les objets détectés, lesquelles constituent une entrée pour la fonction de seuillage de distance. Le seuillage de distance calcule la décélération nécessaire pour maintenir la distance avec le véhicule qui précède et envoie la commande de freinage appropriée à l'ECU de freinage dans le cas où la distance passe en dessous d'une limite prédéfinie.

Les objectifs de sécurité de ce système sont définis pour éviter les freinages intempestifs et éviter l'indisponibilité du couple de freinage requis lorsqu'il est nécessaire. Comme il y a un risque de blessure grave, voire mortelle, en cas de dysfonctionnement, les deux objectifs doivent répondre à l'exigence ASIL D, qui est l'exigence d'intégrité la plus élevée selon la norme ISO 26262.

Les architectures de véhicule de domaine et de zone affectent différemment les objectifs de sécurité. La figure 3 montre un exemple de la partie relative au freinage autonome dans une architecture reposant sur les domaines. Ici, le radar, le système de freinage et le contrôleur de domaine sont connectés à un seul bus CAN (Controller Area Network). Le module radar reçoit des données du frontal radar, exécute la détection d'objets et effectue des tâches de seuillage de distance. Les commandes pour le contrôle du freinage sont envoyées via le bus CAN au module de freinage, qui exécute la tâche de freinage commandée.

La figure 4 montre comment cette même fonction peut être mise en œuvre dans une architecture zonale. Les unités de radar et de freinage sont connectées via deux bus CAN distincts à deux modules de zone distincts. Ces deux modules sont connectés à un cerveau central et éventuellement à d'autres modules de zone à l'intérieur du véhicule. Le module radar ne contient qu'un capteur et le module de freinage ne comprend qu'un actionneur. Contrairement aux modules radar et de freinage dans l'architecture reposant sur les domaines, aucun traitement majeur n'est effectué dans l'un ou l'autre des modules dans l'architecture zonale. Au lieu de cela, le module de traitement central effectue la détection d'objets et le seuillage de distance (les « calculs » en somme). Par conséquent, cette architecture est appelée architecture zonale avec traitement centralisé.

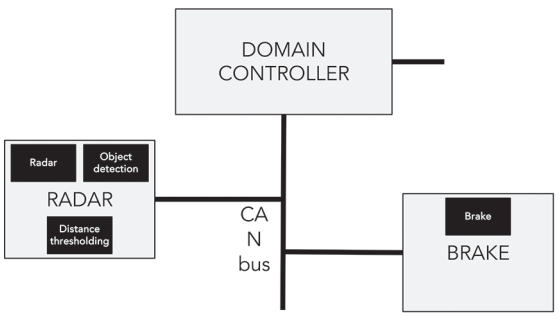
D'autres approches peuvent être adoptées, telles que l'exécution des tâches de détection d'objets et de seuillage de distance au sein du module de zone A et/ou B. De telles variantes sont appelées architectures zonales avec traitement local de zone.

2 FLOT DE DE DONNÉES TYPIQUE DANS UN SYSTÈME DE FREINAGE AUTONOME

Les cases marquées en noir sur la figure sont des unités de commande électroniques ECU (Electronic Control Units) et les cases marquées en gris représentent les informations échangées entre les ECU.

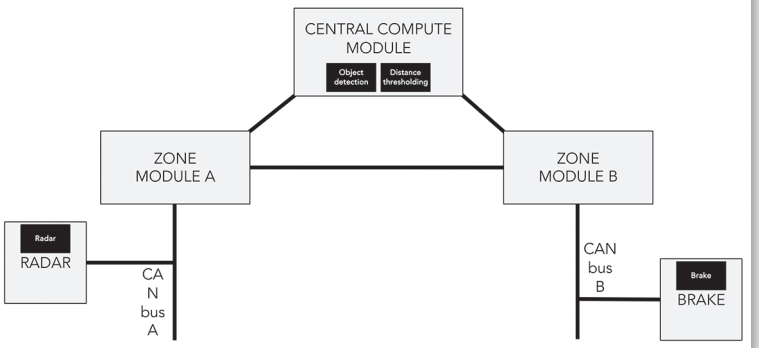
3 CONTRÔLE DE FREINAGE AUTONOME DANS UNE ARCHITECTURE DE DOMAINE

Cette figure montre un exemple de la partie relative au freinage autonome dans une architecture reposant sur les domaines. Le module radar reçoit des données du frontal radar, exécute la détection d'objets et effectue des tâches de seuillage de distance. Les commandes pour le contrôle du freinage sont envoyées via le bus CAN au module de freinage, qui exécute la tâche de freinage commandée.



4 FREINAGE AUTONOME DANS UNE ARCHITECTURE ZONALE AVEC TRAITEMENT CENTRALISÉ

Les unités de radar et de freinage sont connectées via deux bus CAN distincts à deux modules de zone distincts. Ces deux modules sont connectés à un cerveau central et éventuellement à d'autres modules de zone à l'intérieur du véhicule.



Calcul du taux de défaillance FIT pour la conformité ASIL D

La métrique de probabilité de défaillance matérielle PMHF (Probability Metric of Hardware Failure), qui est une valeur numérique de sécurité ISO 26262 reconnue, est la probabilité moyenne de violation d'un objectif de sécurité, exprimée en taux de défaillance FIT (Failure In Time). L'ISO 26262 exige un PMHF inférieur à 10 FIT (probabilité de défaillance de 10^{-8} par heure) pour le niveau ASIL D et inférieur à 100 FIT (probabilité de défaillance de 10^{-7} par heure) pour le niveau ASIL C.

Une valeur PMHF maximale est attribuée à chaque objectif de sécurité en fonction de sa note ASIL et de la norme ISO 26262. Cette valeur est répartie sur les trois groupes de composants différents distingués dans les exemples d'architecture : les composants de traitement et de fusion de capteurs, les composants de communication et les actionneurs.

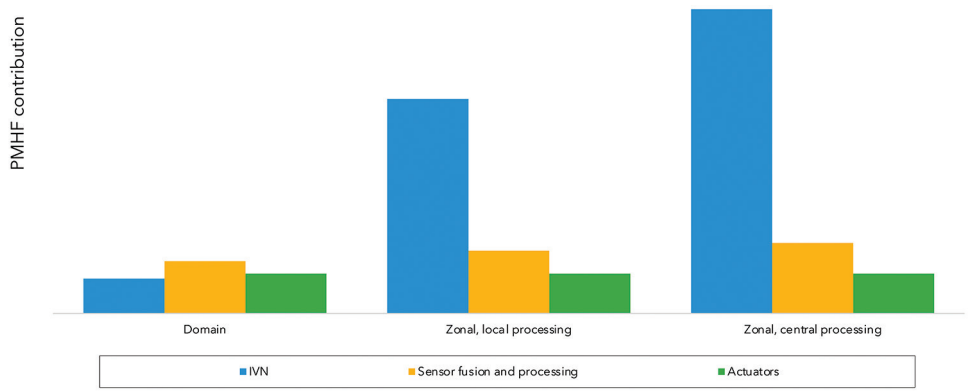
Chacun de ces groupes de composants individuels a sa propre probabilité de défaillance PMHFx, où x est le numéro d'ordre des composants. La valeur PMHF globale pour l'application est la somme des valeurs PMHFx des composants individuels. Pour satisfaire aux exigences globales de sécurité fonctionnelle de l'application, cette somme doit être inférieure ou égale à la valeur PMHF maximale liée à l'objectif de sécurité ASIL.

Lors du passage d'une architecture de domaine à une architecture zonale, les modifications architecturales et le remaniement des tâches qui en découle affectent la valeur PMHF d'une application. Dans les architectures zonales, un nombre beaucoup plus important de composants de communication et de traitement est nécessaire pour exécuter la même application par rapport à une architecture reposant sur les domaines.

Nous avons calculé le PMHF global des objectifs de sécurité dans notre exemple d'application, comparant ainsi l'architecture basée sur les domaines avec les deux variantes de l'architecture zonale que nous avons décrites précédemment. La contribution relative de chaque groupe de composants au PMHF global a ensuite été calculée, et les résultats sont présentés dans la figure 5. Le diagramme confirme que les architectures zonales plus distribuées entraînent une augmentation significative de la contribution des communications du réseau embarqué (In-Vehicle Network) au PMHF de l'application globale. On constate également qu'il n'y a pas de changement significatif dans la contribution liée aux traitements. Cela s'explique par le fait que la quantité globale de traitements ne change pas selon les différentes architectures.

5 CONTRIBUTION RELATIVE AU PMHF (PROBABILITY METRIC OF HARDWARE FAILURE) POUR CHAQUE GROUPE DE COMPOSANTS ET CHAQUE ARCHITECTURE

Le diagramme confirme que les architectures zonales plus distribuées entraînent une augmentation significative de la contribution des communications du réseau embarqué (In-Vehicle Network) au PMHF de l'application globale.



« L'opérationnel après panne » pour la conduite autonome

La conduite entièrement autonome, pour laquelle les passagers ne peuvent pas prendre le relais en cas de défaillance, nécessite des systèmes « opérationnels après panne », ou Fail Operational, qui garantissent une fonctionnalité complète ou dégradée en cas de panne. Diverses architectures permettent d'atteindre cet objectif, mais chacune présente des avantages et des inconvénients.

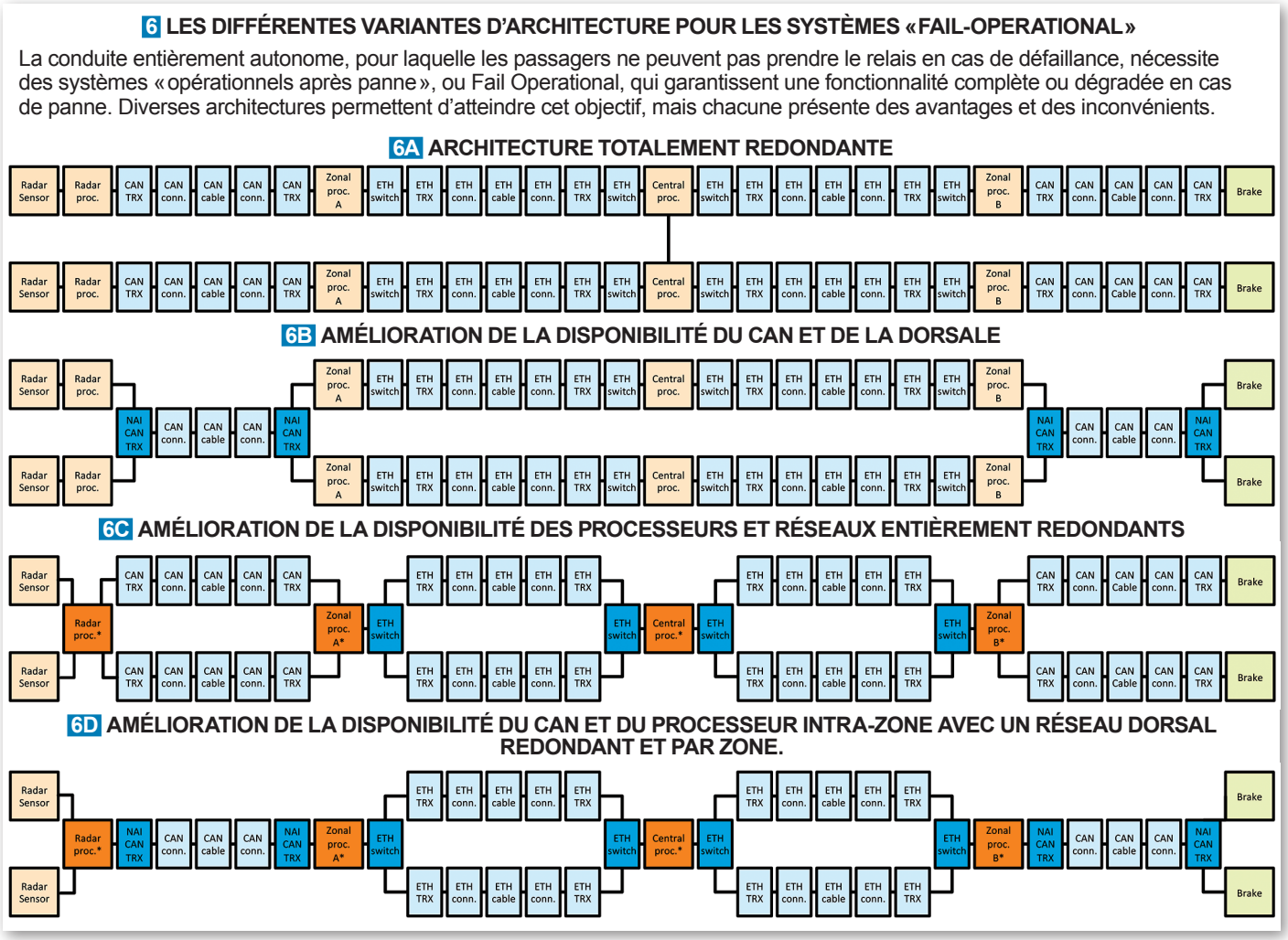
Variante d'architecture 1

Un exemple est la redondance homogène, qui duplique le système en deux implémentations parallèles indépendantes (figure 6A). Cette variante permet un comportement « fail-operational » en cas de défaillance aléatoire au sein de l'une des deux implémentations. Une et une seule seulement de ces implémentations parallèles est active à la fois, bien que le chemin « de secours » (ou redondant) puisse être périodiquement auto-testé pour détecter les défauts latents. En cas de défaillance du chemin principal, le second chemin peut être sélectionné pour garantir sa disponibilité.

Cette approche repose sur l'hypothèse qu'il est peu probable qu'un défaut systématique affecte les deux implémentations en même temps, et l'impact d'un défaut systématique peut être minimisé en utilisant des composants différents dans les deux chemins. C'est ce qu'on appelle la diversification. Les inconvénients sont le doublement du nombre de composants silicium et, par conséquent, l'augmentation du coût global du système.

6 LES DIFFÉRENTES VARIANTES D'ARCHITECTURE POUR LES SYSTÈMES «FAIL-OPERATIONAL»

La conduite entièrement autonome, pour laquelle les passagers ne peuvent pas prendre le relais en cas de défaillance, nécessite des systèmes «opérationnels après panne», ou Fail Operational, qui garantissent une fonctionnalité complète ou dégradée en cas de panne. Diverses architectures permettent d'atteindre cet objectif, mais chacune présente des avantages et des inconvénients.



Variante d'architecture 2

Une deuxième variante (figure 6B) utilise des bus CAN uniques pour connecter les composants de fusion de capteurs, de traitement et d'actionneur. Cela évite de dupliquer la structure du bus CAN (c'est-à-dire le câblage) et utilise à la place un nouveau type d'émetteur-récepteur CAN qui permet un fonctionnement en cas de panne unique au sein de la structure du réseau. La disponibilité du CAN intra-zone est améliorée tandis que la dorsale du réseau reste entièrement redondante. Cela permet d'économiser les dépenses associées aux émetteurs-récepteurs redondants et de réduire le poids du câblage tout en offrant la même disponibilité qu'une architecture entièrement redondante.

Variante d'architecture 3

Une troisième variante, caractérisée par la non-duplication des modules de traitement et des commutateurs Ethernet, est illustrée dans la figure 6C. Un deuxième processeur fonctionnant en parallèle augmente la disponibilité des modules de traitement. Ce processeur peut avoir une spécification de performance inférieure, obligeant ainsi à un mode de fonctionnement dégradé en cas d'échec. Cela peut être acceptable pour certains cas d'utilisation, par exemple lorsqu'il faut que le véhicule s'écarte de la route en toute sécurité.

Variante d'architecture 4

La quatrième variante (figure 6D) combine les améliorations de la disponibilité du CAN et du traitement intra-zone avec un réseau dorsal entièrement redondant. Cette disposition améliore la disponibilité du CAN et du traitement, ce qui permet de réaliser les économies de câblage observées dans la variante 2, avec la réduction du nombre de modules de contrôle observée dans la variante 3.

Conclusion

Des niveaux plus élevés d'autonomie des véhicules évitent l'implication humaine dans le processus de conduite. A ces niveaux supérieurs, les systèmes de conduite autonome peuvent supporter des pannes tout en restant dans un état opérationnel. Bien que la redondance complète soit une solution irréalisable pour répondre à cette exigence, l'adoption réfléchie de fonctionnalités de communication et de traitement améliorant la disponibilité peut permettre d'obtenir la même disponibilité pour un coût global du système moins élevé.

Les architectures de réseau de véhicules évoluent vers des architectures zonales, visant à prendre en charge une plus grande fonctionnalité tout en minimisant le poids et le coût des véhicules. D'autre part, la zonalisation nécessite une conception minutieuse pour garantir que les systèmes critiques liés à la sécurité, tels que le freinage autonome, peuvent atteindre le niveau ASIL requis. Nous avons montré que la probabilité moyenne de violation d'un objectif de sécurité en raison de la contribution du réseau embarqué augmente considérablement dans les réseaux zonaux par rapport aux topologies traditionnelles de réseau de véhicules. ■