JOINDRE LA RÉPONSE À L'ATTAQUE POUR DÉTERMINER L'IMPACT SUR LE PROTOCOLE J1939

COMBINING THE RESPONSE TO THE ATTACK TO DETERMINE THE IMPACT ON THE J1939 PROTOCOL

Un mémoire soumis à la Division des études supérieures
du Collège militaire royal du Canada
par

M.P. Fujioka, B. Ing.
Ltv

en vue de l'obtention du diplôme de
maîtrise ès sciences appliquées en génie électrique et génie informatique

Mai, 2026

© Ce mémoire peut être utilisé au ministère de la Défense nationale,
mais l'auteur conserve les droits de publication.

Dédicace - Dedication

Ce mémoire est un défi personnel. J'aurais pu choisir de faire un projet au lieu d'un mémoire, mais ça ne serait pas le même sens d'accomplissement. J'avais décidé de m'embarquer dans un domaine qui m'est inconnu et qui ne sera pas facile à accomplir. J'ai possiblement sous estimé le travail, mais je n'ai pas abandonné.

This dissertation was a personal challenge. I could have opted for the project instead of a thesis, but this would have not lead to the same sense of accomplishment. I decided to embark into the unknown knowing that it will not be easy. I may have underestimanted the work, but I never gave up.

Remerciements - Acknowledgements

Je prend cette opportunité pour remercier tous ceux qui n'ont, malgré les multiples années, jamais cessés de me demander quand j'aurai terminé mon mémoire. Je ne vais pas mentionner de noms, mais vous savez qui vous êtes. Une chose est certaine, vous étiez très persistent. Finalement, je veux remercier mon superviseur de mémoire Dr. Sylvain (Sly) Leblanc qui m'a supporté pendant toutes ces années. Votre dévouement profesionnel m'a permit de me rendre à une étape importante. Merci.

I am taking this opportunity to thank all that, despite the numerous years, never stopped asking when I will be done with the thesis. I will not name names, but you know who are are. One thing I will say is that you all were persistent. Finally, I would like to thank my supervisor Dr. Sylvain (Sly) Leblanc who supported me all these years. Your profesionnal devotion helped me reach this important step. Thank you.

Résumé

Les réseaux informatiques peuvent être protégés à l'aide de la combinaison d'un système de détection d'intrusion (IDS) et d'un système de prévention d'intrusion (IPS). L'IDS permet d'identifier des attaques ou des anomalies survenus sur le réseau; l'IPS peut ainsi appliquer une mesure de sécurité afin de bloquer ou de corriger les attaques identifiées. Lorsque l'IPS tente de bloquer ou de corriger l'attaque, il peut affecter le flux de l'information dans le réseau qui peut avoir un impact sur son opération. Dans le contexte des technologies de l'information, l'impact principal touche l'accès à l'information ou à l'interruption de services. Lorsqu'il est question de la protection d'un réseau véhiculaire, tel que le protocole « Society Automotive Engineers (SAE) » J1939, l'impact devient plus important. Les messages de ce réseau peuvent contenir des commandes de contrôles assujettis aux attaques qui peuvent affecter le comportement du véhicule et conséquemment son environnent.

Le but de cette recherche est de concevoir un modèle afin de considérer les impacts des attaques et des réponses à celles-ci sur un réseau SAE J1939. Nous avons développé un modèle, basé sur la simulation, pour déterminer l'impact d'une attaque survenue sur un réseau véhiculaire SAE J1939 ainsi que celui d'une réponse à cette attaque afin de déterminer l'impact résultant du réseau. Nous avons simulé deux cas d'utilisation. Le premier est la comparaison des états de la matrice de confusion qui représentent les différents impacts possibles du système en présence ou absence d'attaque, et le deuxième est l'implémentation de deux réponses similaires pour la même attaque. Lors de nos simulations, nous avons remarqué que l'impact résultant (tous impacts identifiés, y compris ceux qui sont temporaires) ne sont pas nécessairement représentatif de l'impact final subit par le système. La transition entre l'ajout de l'attaque ou celle de la réponse peut créer une instabilité momentanément. Nous avons conclu que notre modèle permet de déterminer l'impact résultant du système.

Abstract

Computer networks can be protected by combining an Intrusion Detection System (IDS) with an Intrusion Prevention System (IPS). The IDS can identify attacks or anomalies that occurred on the network. The IPS can then apply a security countermeasure in the hopes of blocking or correcting the identified attack. When the IPS attempts to block or correct the attack, it can also affect the flow of information within the network which can have an impact on its operations. In the realm of the Information Technologies, the impact is primarily on the access of the information or the interruption of the services. For the protection of vehicule networks, such as the Society Automotive Engineer (SAE) J1939, the impact have greater concerns. The messages exchanged in those networks may contain commands to control that can affect its behaviour and its environment.

The aim of this research is to design a framework that considers the impacts of attacks and their responses on a SAE J1939 network. We have developed a framework, based on simulation, to determine the impact of an attack on a vehicle network SAE J1939 and the response to that attack in order to determine the resulting impact. We have simulated two test cases. The first is the comparison between all the various states in the confusion matrix which represent all the possible impacts on the system in the presence or absence of an attack, and the second is the implementation of two similar responses for the same attack. Following the simulations, we have observed that the resulting impact (meaning all identified impacts including temporary impacts) are not necessarily the impact in the end state. The transition between the addition of the attack or the response can create a temporary instability. We have concluded that the framework allows to determine the resulting impact of the system.

Table des matières

Liste des tableaux

Liste des figures

Liste des acronymes

ABS . . . . . système de freinage antiblocage
AR . . . . . attaque et réponse
CAN . . . . . réseau de zone de contrôleur
CAN High . . . . valeur CAN élevée
CAN Low . . . . . valeur CAN basse
CIA . . . . . confidentialité, intégrité, et disponibilité
CRC . . . . . contrôle de redondance cyclique
DoS . . . . . déni de service
FN . . . . . faux négatif
FP . . . . . faux positif
IDPS . . . . . système de détection et de prévention d'intrusion
IDS . . . . . système de détection d'intrusion
IPS . . . . . système de prévention d'intrusion
IT . . . . . technologie de l'information
MCE . . . . . module de commande électronique
NIST . . . . . institut national des standards et technologies
OSI . . . . . interconnexion des systèmes ouverts
PGN . . . . . numéro de groupe de paramètres
PT . . . . . technologie des plateformes
SAE J1939 . . . . standard de la société de l'ingénierie de l'automobile J1939
SPN . . . . . numéro de paramètre suspect
VN . . . . . vrai négatif
VP . . . . . vrai positif

1 Introduction

Dans les dernières années, l'utilisation de la technologie dans la vie de tous les jours ne cesse de s'accroître. Cette observation s'applique autant pour l'électronique et le logiciel que pour l'interconnexion d'appareils. Les réseaux véhiculaires n'en font pas l'exception où l'interaction de leurs modules peut améliorer l'efficacité du véhicule ainsi que la qualité de vie des utilisateurs. Avec de plus en plus de modules installés, avec ou sans fil, ces types de réseaux véhiculaires sont devenus des champs d'intérêt. Historiquement, certains des protocoles pour de tels réseaux priorisaient la fonctionnalité au-dessus de la sécurité. Pour ce mémoire, le réseau véhiculaire choisi est le standard de la société de l'ingénierie de l'automobile J1939 (SAE J1939 de l'anglais *Society of Automotive Engineers J1939*) qui est principalement utilisé pour les véhicules lourds.

1.1 Motivation

Lorsqu'il est question de la protection d'un réseau, un système de prévention d'intrusion (IPS de l'anglais *Intrusion Prevention System*) peut être utilisé. Ce système permet la mise en place de mesures de sécurité afin de bloquer ou de corriger des attaques identifiées. Celles-ci ont été ciblées par un système de détection d'intrusion (IDS de l'anglais *Intrusion Detection System*) qui fournit l'information sur les attaques ou les événements reconnus comme étant malveillants. Donc, une fois que l'attaque est détectée par l'IDS, l'IPS peut appliquer une mesure de sécurité.

Lorsque l'IPS tente de bloquer ou de corriger l'attaque, il peut affecter le flux de l'information sur le réseau, ce qui peut avoir un impact sur l'opération du véhicule. L'impact va varier en fonction de la solution appliquée, par contre, pour certains types de réseaux, l'impact peut avoir des conséquences physiques. Dans le contexte de la technologie de l'information (IT de l'anglais

Information Technology), l'impact principal touche l'accès à l'information ou l'interruption de services. Pour les réseaux véhiculaires, où il pourrait y avoir des commandes de contrôles assujettis aux attaques. L'impact devient soudainement beaucoup plus resenti dans le domaine physique.

Lorsqu'une attaque est survenue sur un réseau véhiculaire, l'impact de celle-ci peut être déterminé, mais la priorité d'effort est souvent mise à contrer l'attaque. Ceci suppose que la réponse à l'attaque va rapporter le système à son état normal. L'impact de cette réponse à l'attaque n'est pas représenté dans les recherches, et de plus, celui-ci n'est pas comparé à l'impact de l'attaque elle-même. Cette comparaison pourrait apporter une perspective importante sur l'application de mesure de sécurité pour les réseaux véhiculaires.

Il existe une défaillance dans le domaine de recherche pour l'IPS où l'impact de la réponse est le seul qui est considéré, et ce, sans tenir compte de l'impact initial de l'attaque. De plus, une complexité est ajoutée par le fait qu'il peut y avoir des erreurs dans la détermination de l'impact d'une attaque, telles que les faux positifs qui suggèrent la présence d'une attaque quand il n'y en a pas.

1.2 But

Le but de cette recherche est de concevoir un modèle afin de considérer les impacts des attaques et des réponses à celles-ci sur un réseau SAE J1939.

Pour ce faire, nous avons développé un modèle (dans le sens du terme anglais *framework*), basé sur la simulation, pour déterminer l'impact d'une attaque survenue sur un réseau véhiculaire SAE J1939 ainsi que celui d'une réponse à cette attaque. Il est important de noter que notre travail présume la présence d'un IDS qui peut identifier les attaques et les assigner à des messages SAE J1939 particuliers, mais les détails de cet IDS sont hors de la portée de notre travail. L'architecture du réseau et du système véhiculaire a été établie pour inclure les interrelations entre les composantes et leurs messages échangés. La capacité à interagir avec le réseau est définie pour la source des attaques et des réponses. Les impacts ciblent les fonctionnalités physiques des composantes du réseau (e.g. la vitesse, le freinage, etc) et l'état de fonctionnalité de ces composantes. La simulation incorpore des scénarios que nous allons utiliser pour évaluer certains cas d'utilisation.

1.3 Structure du document

Le chapitre 2 présentera la revue de la littérature qui inclut les différentes technologies et l'état de l'art vis-à-vis les types d'attaques et les paramètres de décision permettant d'évaluer les réponses possibles. Le chapitre 3 décrira le modèle y compris la conception de la simulation et les cas d'utilisation permettant l'évaluation du modèle. Le chapitre 4 présente les résultats alors que le travail futur et la conclusion sont présentés dans le chapitre 5.

2 Revue de la littérature

Dans ce chapitre, nous présenterons les différentes technologies nécessaires à la compréhension de notre recherche, suivies de l'état de l'art en matière de réseaux véhiculaires. En premier lieu, nous présenterons les protocoles réseau de zone de contrôleur (CAN de l'anglais *Controller Area Network*) et SAE J1939, suivis de considérations de sécurité. En deuxième lieu, nous décrirons les IDS et les IPS. En troisième lieu, nous discuterons des recherches concernant les types d'attaques et la délibération sur la prise de décision.

2.1 Technologies

Dans cette section, nous allons décrire les protocoles CAN et SAE J1939. Pour chacun, nous allons fournir un aperçu des couches d'interconnexion des systèmes ouverts (OSI de l'anglais *Open Systems Interconnection*) [4] qu'ils implémentent ainsi que certaines de leurs fonctionnalités. Nous ferons ensuite un survol des considérations de sécurité de ces protocoles.

2.1.1 Bus CAN

Le bus CAN est un protocole de communication en série pour les véhicules [5]. Les réseaux véhiculaires utilisant ce protocole sont formés de modules de commande électronique (MCE) qui sont connectés à un bus commun. Selon le modèle d'OSI [6], le CAN est défini sur les couches physiques et de liaison de données alors que le SAE J1939 (discuté à la section 2.1.2) est défini sur la couche application, comme représentés à la figure 2.1.

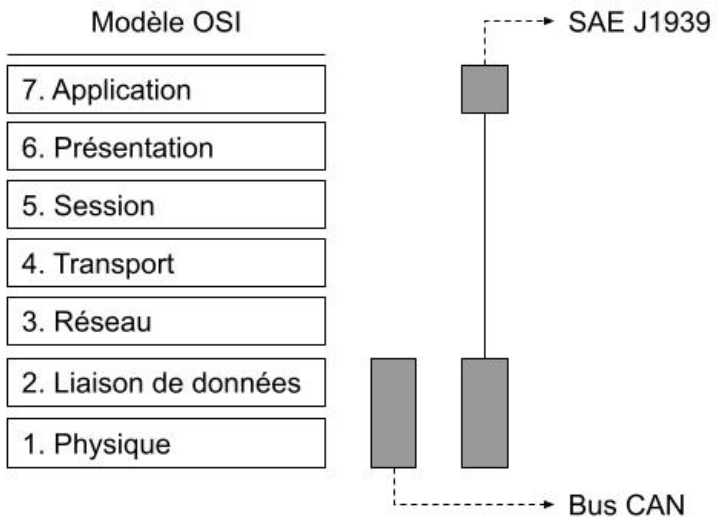

Figure 2.1: **Le modèle OSI**.

Couche physique

Le protocole CAN utilise le concept de bits dominants et récessifs qui est représenté à la figure 2.2. Pour l'implémentation de la couche physique, les connexions du bus CAN utilisent deux signaux distincts. Un signal pour une valeur élevée CAN High, et l'autre pour une valeur basse CAN Low. Un bit dominant est détecté lorsque la différence entre les deux signaux dépasse le seuil conçu. Si le seuil n'est pas atteint, un bit récessif est détecté. Par exemple, lors du premier créneau dans la figure 2.2, le CAN High et le CAN Low ont des valeurs respectives de 3.75 et 1.25. En présumant que le seuil est de 2.0, la différence de 2.5 dépasserait le seuil et deviendrait ainsi un bit dominant. Inversement, si la différence des deux valeurs est sous le seuil, un bit récessif serait détecté. Ceci est le cas pour la deuxième époque de la figure, où la différence entre le CAN High et le CAN Low est près du 0.

Les bits dominants représentent une valeur de zéro (0), et les bits récessifs représentent une valeur de un (1). Un mécanisme de bourrage de bits est utilisé lors de la transmission de cinq bits consécutifs de mêmes valeurs logiques. Suivant ces cinq bits, un bit d'une valeur opposée est transmis et celui-ci est ignoré par les MCE qui le reçoivent. Ce processus permet de différencier une transmission normale à une trame d'erreur qui est représentée par six bits consécutifs de mêmes valeurs logiques.

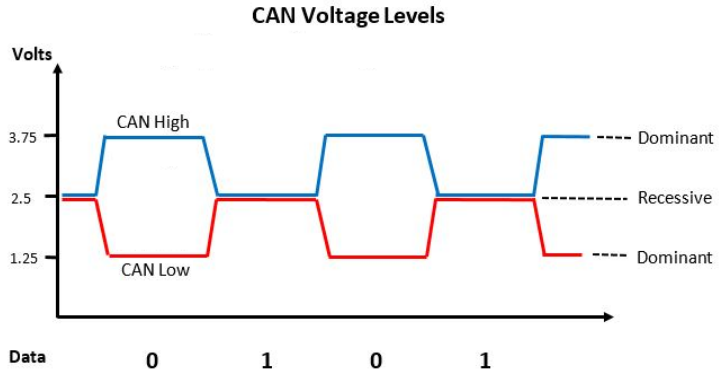

Figure 2.2: **La différence de potentiel du bus CAN [1].**

Couche de liaison de données

Un message CAN est une trame de données utilisée pour la couche de liaison de données. Celle-ci est constituée de plusieurs champs représentés à la figure 2.3. Dans la trame (*Data Frame*), entre l'espace intertrame (*Interframe Space*) et la trame de surcharge (*Overload Frame*), on trouve le début de la trame (*Start of Frame*), l'identifiant ou le champ d'arbitrage (*Arbitration Field*), le champ de contrôle (*Control Field*), le champ de données (*Data Field*), le contrôle de redondance cyclique (*CRC Field*), l'accusé de réception (*ACK Field*), et la fin de la trame (*End of Frame*). L'identifiant d'une trame par défaut contient 11 bits, et possède une option lui permettant d'étendre la longueur à 29 bits. Cette option est signalée dans le champ de contrôle où l'un de ces bits signifie le format de la longueur de l'identifiant. Sans tenir compte du champs de données, la trame possède une longeur de 62 bits incluant le format étendu de l'identifiant. Chaque message est transmis sur le bus par diffusion générale, donc tous les MCE connectés peuvent recevoir la totalité de l'information, bien qu'ils ignorent ce qui ne leur est pas destiné.

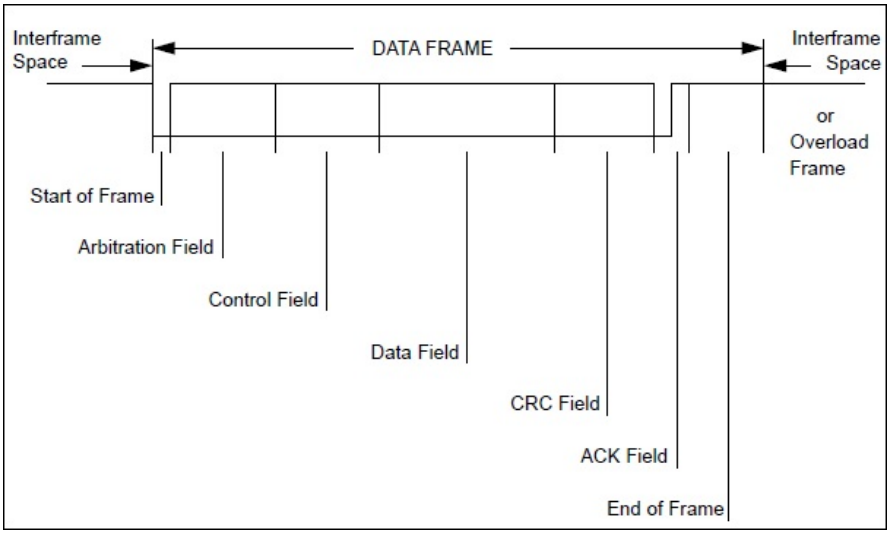

Figure 2.3: **Une trame du bus CAN [2]**.

Collision de transmission

Pour le bus CAN, les messages sont transmis par diffusion générale. Les collisions de transmission sont contrôlées par une fonctionnalité de la couche physique. Une collision survient lorsque plusieurs MCE transmettent sur le bus en même temps. Comme indiqué précédemment, la couche physique du protocole CAN utilise la différence des signaux pour déterminer le bit transmis. Si un bit récessif et un bit dominant sont transmis simultanément, le bus détectera seulement le bit dominant. Chaque MCE compare leur bit envoyé et celui détecté sur le bus. Si un bit récessif est envoyé et qu'un bit dominant est détecté, le MCE a deux réactions principales expliquées ci-dessous.

1. **L'arbitrage**. Lorsqu'un bit pour le début de trame est transmis, il n'est pas possible de savoir combien de MCE ont transmis le bit. Le champ d'arbitrage ou l'identifiant est utilisé à cette fin. Pour chaque bit de ce champ envoyé, les MCE comparent leur bit envoyé avec celui qui est détecté sur le bus. Si un bit dominant est détecté lors de l'envoi d'un bit récessif, le MCE en question cesse sa transmission. À la fin de la transmission de l'identifiant, il ne reste qu'un seul MCE qui continue l'envoi de son message. L'arbitrage agit donc aussi comme mécanisme pour prioriser les messages.
2. **Les erreurs**. Durant la transmission d'un message, tous les MCE, qu'ils transmettent ou non, continuent à évaluer le message transmis en cas d'erreur. Lorsqu'une erreur est détectée par un MCE, celui-ci envoie

une trame d'erreur qui est constituée de six bits dominants successifs. Lorsque cette trame est transmise, le MCE qui transmettait le message cesse sa transmission et le bus devient disponible à nouveau. Les erreurs possibles incluent les valeurs inattendues dans certains champs et le calcul erroné du CRC. Les MCE utilisent un mécanisme interne pour gérer les erreurs survenues sur le bus. Ce mécanisme évalue le nombre d'erreurs, soit transmis ou détecté, puis détermine un plan d'action. Les actions peuvent varier, mais la principale est de cesser la transmission de messages.

L'explication ci-dessus suppose le fonctionnement normal du bus CAN où il n'y a aucun abus de l'arbitrage ni de l'utilisation des trames d'erreur. Nous traiterons des implications de sécurité incluant les abus à la section 2.1.3.

2.1.2 SAE J1939

Couche d'application

Le SAE J1939 est un protocole véhiculaire utilisé principalement pour les véhicules lourds. Il utilise les couches physiques et de liaison de données de protocole du bus CAN, puis ajoute une implémentation de la couche d'application, comme représenté dans la figure 2.1. Les différences principales entre le SAE J1939 et le protocole CAN sont sur l'interprétation de l'information des messages [6], et l'identification (ou champ d'arbitrage) qui utilise le format étendu de 29 bits. Le mécanisme pour prioriser les messages, l'arbitrage, est le même que celui du bus CAN, comme l'est la gestion des erreurs. L'identifiant pour le SAE J1939, qui est représenté dans la figure 2.4, est séparé en trois parties; la priorité, le numéro de groupe de paramètres (PGN de l'anglais *Parameter Group Number*) et l'adresse de la source.

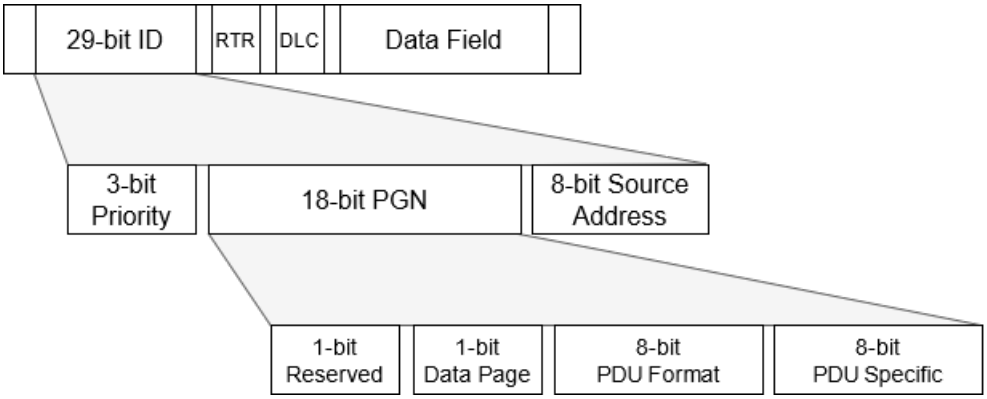

Figure 2.4: **Le message SAE J1939 [3].** 8

La priorité indique l'importance du message. Le PGN est la valeur principale utilisée pour définir le message et son contenu. Le PGN contient quatre parties. Les deux premières sont le bit réservé (pour implémentation future du protocole) et la page de données (une extension qui permet d'accroître le nombre de groupe de destinations). Les deux autres parties sont le format (*PDU Format*) et la spécification (*PDU Specific*) du groupe de destinations qui sont utilisés pour déterminer les MCE ciblés ainsi que le contenu du message. Le format et la spécification agissent aussi comme un identifiant et sont formés de huit bits chacun qui se traduisent à une valeur entre 0 et 255. Pour le format, il y a 240 identifiants pour désigner une destination unique, et 16 identifiants pour désigner un groupe de destinations. L'identifiant 255 est réservé pour désigner un groupe de destinations qui inclut tous les MCE. Pour la spécification, il y a 255 identifiants différents. Si le format désigne une seule destination, la spécification indiquera l'identifiant du MCE qui est unique. Si c'est un groupe de destinations, la spécification est utilisée en tant qu'extension pour désigner un groupe. La combinaison d'un format et d'une spécification, pour une certaine norme définit les données du message. L'adresse de la source est l'identifiant unique du MCE qui a transmis le message.

Un PGN est associé à un contenu (*Data Field*) prédéterminé d'une longueur maximale de 64 bits. Les données de ce contenu sont représentées par une énumération ordonnée de numéro de paramètre suspect (SPN de l'anglais *Suspect Parameter Number*). Chaque SPN a un identifiant unique, une longueur et une valeur. Les valeurs varient selon ce qu'elles signifient. Certaines sont des options ou des états, dont leur signification est détaillée dans la documentation, et d'autres sont des nombres entiers ou des pourcentages. Ces derniers ont souvent un multiplicateur permettant de les normaliser selon une échelle de données personnalisée. Dans la norme SAE J1939, le PGN représente un groupe de données, tandis que le SPN représente une de ces données. Donc, pour déterminer ce qu'un PGN contient comme information, il faut regarder ce que tous ses SPN signifient.

La longueur d'un message sans champ de données est de 62 bits tel que mentionné à la section 2.1.1. La longeur d'un message avec un champ de données maximal est de 126 bits. Dans ce mémoire, nous allons utiliser une longueur de messages de 135 bits qui contient la quantité maximale de bits pour les données ainsi que neuf bits pour le bourrage de bits.

2.1.3 Considérations de sécurité

Le bus CAN a été conçu pour être léger et pour maximiser l'échange libre entre les MCE [7]. Ce type de bus est efficace, robuste et simple à implémenter. Par contre, ces avantages ont un coût lorsqu'il est question de la sécurité du système. Les considérations de sécurités concernant le bus CAN sont applicables au protocole SAE J1939 puisqu'elles ne sont pas affectées par l'implémentation de la couche d'application. Les trois déficiences de sécurité principales du CAN sont les suivantes [7]:

1. **Les messages ne sont pas authentifiés**. Les MCE utilisent la diffusion générale pour transmettre leur message, et ils reçoivent tous les messages transmis sur le bus. Lors de la détection d'un message sur le bus, les MCE déterminent si celui-ci leur est destiné, puis utilisent son contenu si nécessaire. Sans authentification, n'importe quel MCE, légitime ou non, peut transmettre un message. Ceci permettrait à un appareil malveillant de facilement implémenter l'usurpation de message ou d'identité.
2. **Les MCE ne sont pas forcément segmentés**. L'architecture du bus CAN, sans appliquer les meilleures pratiques de sécurité, permet la communication entre tous les appareils connectés. Certains MCE sont nécessaires pour assurer le bon fonctionnement du système et la sécurité des passagers, tandis que d'autres le sont moins. Par exemple, les MCE qui contrôlent le moteur ou la transmission sont nécessaires pour le fonctionnement sécuritaire du véhicule, comparés au contrôle de la lumière d'ambiance du véhicule qui l'est beaucoup moins. La déficience existe car les MCE vitaux pourraient faire l'échange de messages avec des appareils qui le sont moins. Une segmentation peut être implémentée, mais les concepteurs doivent prendre en considération des limites véhiculaires telles la gestion de l'espace physique dans le châssis, et le poids additionnel relié à la segmentation du réseau.
3. **Le contenu des messages n'est pas encrypté**. Lors de la conception du bus CAN, le piratage des systèmes véhiculaires n'était pas un problème envisagé et la nécessité d'encrypter les messages n'était pas une priorité. Sans chiffrements, tous les messages sont visibles et la confidentialité de l'information n'est pas possible. Ceci permettrait à un appareil connecté d'effectuer des activités telles que l'attaque par usurpation, le reniflage réseau, et l'attaque par rejeu comme discuté à la section 2.3.1.

En plus des considérations mentionnées ci-haut, certaines fonctionnalités du CAN peuvent être abusées, ajoutant des implications de sécurité supplémen-

taires. Parmi celles-ci, les prédominantes sont l'arbitrage et la gestion des erreurs. Les MCE peuvent transmettre sur le bus à volonté. Ceci n'est pas un problème lorsque tous les MCE suivent les règlements du protocole CAN afin d'y assurer son bon fonctionnement. Par contre, ces règles ne fournissent pas des mécanismes qui bloquent les comportements malveillants. Un appareil pourrait donc transmettre des trames d'erreur et même usurper la priorité des messages sur le bus causant de sérieuses conséquences à la sécurité.

Dans cette section, les protocoles CAN et SAE J1939 ont été décrits. Nous avons présenté une description des différentes couches protocolaires du modèle d'OSI utilisées ainsi que les considérations de sécurité des protocoles.

2.2 IDS et IPS

Dans cette section, nous ferons un aperçu des IDS et des IPS. De plus, nous allons énumérer les différents types d'erreur existants concernant les attaques et leurs réponses.

Les IDS permettent d'identifier la présence d'activités suspectes sur un réseau ou sur un hôte, puis informent un administrateur [8]. Les IPS permettent de détecter des activités intrusives et peuvent tenter de les arrêter [8]. La figure 2.5 représente la matrice de confusion montrant les différents types d'erreurs entre la classe estimée et la classe réelle. La classe estimée est le résultat de la détection de l'IDS qui détermine si l'élément évalué est normal ou malveillant. La classe réelle représente le résultat qui aurait dû être détecté. L'interaction entre la classe estimée et la classe réelle représentent les quatre types de détections. Celles-ci sont le vrai positif (VP), le vrai négatif (VN), le faux positif (FP) et le faux négatif (FN).

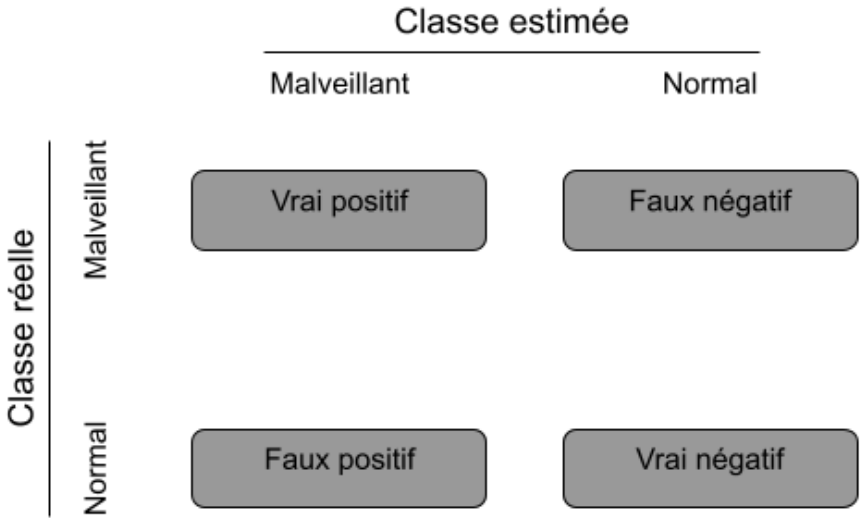

Figure 2.5: **La matrice de confusion**.

Les mécanismes principaux utilisés par l'IDS sont la détection basée sur une signature ou une anomalie [9].

1. **Signature**. Une signature est caractérisée par de l'information unique à la cyberattaque. Par exemple, cette information peut être représentée sous forme d'une chaîne de caractères uniques à l'attaque. Cette méthode est souvent utilisée par les pare-feu et les antivirus pour identifier le trafic réseautique et les logiciels malveillants. Ce type de détection a typiquement un taux élevé de vrais positifs. Un désavantage important de la détection par signature est l'inhabilité de détecter de nouvelles menaces qui exige la mise à jour constante des signatures.
2. **Anomalie**. Une anomalie est caractérisée par le comportement, du réseau ou de l'hôte, qui diverge de ce qui est considéré comme étant normal. Pour ce faire, il s'agit de déterminer le normal, puis le comparer au comportement d'intérêt afin d'identifier les anomalies. Cette méthode est très flexible, mais se distingue habituellement par un taux élevé de faux positifs. Nous suggérons que la méthode promet de meilleurs résultats pour les réseaux industriels et véhiculaires qui ont généralement un comportement prédéterminé ou périodique qui facilite la détermination du normale de ces réseaux. Pour la détection d'anomalies, le taux de faux positifs et de faux négatifs dépend grandement de la compréhension

du système (permettant de définir le normal) et de l'implémentation de l'IDS.

Dans ce mémoire, le concept de la détection basée sur une anomalie est la principale technique considérée. Une anomalie peut être représentée sous plusieurs formes. Par exemple, la fréquence d'un message peut être hors norme, ou la valeur d'un champ peut être différente de ce qui est attendu.

Peu importe la méthode de détection utilisée par l'IDS, chaque attaque possède une caractéristique qui a permis de l'identifier. Par exemple, la présence d'une valeur élevée pour le contenu d'un message, ou un message anticipé qui n'a pas été détecté. Ces caractéristiques seront détaillées dans la section 3.2.2 sous le terme « modificateur ».

Les IPS sont précaires envers les types d'erreurs pouvant être introduites lors de la détection. Nous discutons maintenant des implications de chacune de ces erreurs sur les IPS:

1. **Le VP**. Une attaque réelle a été détectée sur le système. Le système est impacté par l'attaque. Si l'IPS réagit, le système sera impacté par la réponse en plus de l'attaque.
2. **Le VN**. Aucune attaque n'a été détectée sur le système. L'IPS ne réagit pas parce qu'il n'y a pas d'attaques de détecté et aucune réponse n'est donc requise. Il n'y a aucun impact au système.
3. **Le FP**. Une attaque a été détectée sur le système tandis qu'il fonctionne normalement. L'attaque non existante ne cause aucun impact. Si l'IPS réagit, le système sera impacté par la réponse seulement.
4. **Le FN**. Aucune attaque n'a été détectée sur le système, mais une est présente. Le système est impacté par l'attaque. L'IPS ne réagit pas parce l'attaque n'a pas été détectée et celui-ci n'a donc aucun impact sur le système alors qu'il devrait y en avoir un.

Dans cette section, nous avons présenté une description des IDS et des IPS, ainsi qu'une courte discussion des quatre types d'erreurs. Ceux-ci représentaient la relation entre la présence d'une attaque et/ou d'une réponse et l'impact sur le système de celles-ci.

2.3 État de l'art

Cette section présentera un aperçu de l'état de l'art des protocoles CAN et SAE J1939. Les sujets d'intérêts seront les différents types d'attaques possi-

bles contre ces protocoles, ainsi que les différents paramètres pour la prise de décision en réponse à une attaque réelle ou perçue.

2.3.1 Types d'attaque

Les types d'attaques existants s'attardent à l'un ou plusieurs aspects reliés aux objectifs de sécurité du système. Ceux-ci sont la confidentialité, l'intégrité ou la disponibilité (triade CIA de l'anglais *Confidentiality, Integrity, Availability*). Bien qu'il existe plusieurs types d'attaques, ce mémoire se concentre sur les attaques de déni de service et de rejeu.

Déni de service

Mukherjee [10] décrit deux types d'attaques par déni de service (DoS de l'anglais *Denial of Service*) de densité élevée et de densité basse. Le DoS de densité élevée injecte beaucoup de messages afin d'épuiser la bande passante du réseau, alors que le DoS de densité basse tente d'épuiser les ressources du processeur d'un MCE. Dans les réseaux SAE J1939, l'arbitrage des PGN détermine la priorité des messages qui sont transmis sur le bus. Ceci peut être abusé et utilisé pour implémenter un DoS où des messages de haute priorité (i.e. PGN 0) sont transmis en succession rapide. Lorsque d'autres MCE tentent d'envoyer leur message, l'arbitrage sera majoritairement gagné par les messages du DoS. Dans une situation où plusieurs MCE envoient un PGN 0 en même temps, cette interaction sera gérée par la gestion des erreurs du protocole. Le DoS doit, par contre, envoyer ses messages à un débit assez élevé pour qu'ils fassent partie de tous les processus d'arbitrage suivants.

Il y a plusieurs mécanismes pour implémenter un DoS pour le SAE J1939, et l'effet de chacun peut varier. Le seul point en commun de ces implémentations est l'interaction entre les messages et le système. Surcharger un réseau SAE J1939 avec des messages PGN 0 va saturer la bande passante et aucun autre message ne sera envoyé. Les MCE qui utilisent le PGN 0 vont tenter de traiter les messages. Ceux-ci pourraient voir leurs ressources s'épuiser et perdre des messages qui ne sont pas traités. De plus, il est important à considérer que ces MCE tenteraient simultanément de traiter des messages supplémentaires qui contiennent de l'information. Cette information pourrait affecter l'intégrité du système même si l'objectif principal du DoS est d'affecter la disponibilité. Tout va dépendre de la spécification en matière de traitement de données. Évaluer l'implémentation de l'attaque et de la réponse est un aspect d'intérêt pour ce mémoire.

Le DoS de densité basse n'affecte pas le débit de messages ni la bande passante. Plutôt, l'attaque utilise une fonctionnalité du système pour créer un DoS; la revendication d'adresse [11]. Ce processus permet à un MCE de faire une demande d'adresse. Ceci est normalement utilisé lors du démarrage d'un réseau SAE J1939 où tous les MCE réclament une adresse. Par contre, rien n'empêche que ce processus soit appliqué à n'importe quel moment par n'importe quel MCE. Une attaque peut abuser de cette fonctionnalité et permet à n'importe quel MCE de tenter de revendiquer une adresse qui est déjà en utilisation. Un appareil malveillant tente de réclamer une adresse utilisée jusqu'à ce qu'il réussit à l'avoir. Dans ce cas, le MCE qui avait l'adresse n'en a plus et tente d'en réclamer une autre. Ce MCE pourrait tenter de se réapproprier de son adresse originale, mais le DoS aura déjà affecté le système. Ce type d'attaque ne sera pas discuté en plus de détails dans ce mémoire, mais sera énuméré pour le travail futur.

Abbott-McCune et al. [12] mentionnent une autre implémentation d'une attaque par déni de service. Les MCE suivent les règlements du réseau pour assurer un bon fonctionnement. Ils effectuent l'arbitrage, envoient leurs messages et transmettent des trames d'erreurs lorsque nécessaire. Il n'y a aucunes restrictions sur la transmission de bit hors de ces règlements. Un MCE peut donc envoyer un bit en même temps que la transmission d'un autre MCE. Si un bit dominant est transmis en même temps qu'un bit récessif, le bit dominant est détecté sur le bus. Un DoS de densité élevée peut être implémenté en utilisant un concept similaire où les bits dominants sont forcés durant l'arbitrage. Ceci se traduit à envoyer un message PGN 0. La particularité de l'attaque en question est que les bits dominants sont transmis non seulement lors de l'arbitrage, mais durant le reste du message et peuvent générer des erreurs. L'attaque cible l'erreur de bit, de format et de contrôle de redondance cyclique. Une fois une erreur détectée, le mécanisme rejette le message. Cette méthode peut être utilisée pour créer un DoS qui cible un ou plusieurs messages spécifiques.

Ce type de DoS peut aussi être effectué en forçant un bit récessif sur le bus [13]. Lors de l'implémentation de la couche physique, les bits sont détectés en utilisant la différence de signal entre les fils CAN High et CAN Low. Si la différence dépasse un certain seuil, un bit dominant est détecté, sinon c'est un bit récessif. L'idée est de faire un court-circuit entre les deux fils d'où la différence de signal sera donc en dessous du seuil, et par ce fait, forcer un bit récessif sur le bus.

Attaque par rejeu

L'institut national des standards et technologies (NIST de l'anglais *National Institute of Standards and Technology*) [8] définit l'attaque par rejeu comme étant la retransmission d'un message, précédemment capturé, qui avait été authentifié correctement. Pour le bus CAN, l'authentification n'est pas implémentée, mais le reste de la définition demeure applicable. Par contre, une incertitude peut être déduite concernant l'intervalle de temps entre le message original et celui qui a été retransmis. Un message qui est retransmis directement après son message original peut facilement être remarqué. Sans authentification, si ce même message est retransmis à un intervalle indéterminé, l'associer à son message original n'est pas trivial. Dans le cadre de ce mémoire, l'attaque par rejeu est définie par un message retransmis identique au dernier message ayant le même identifiant. Ces deux messages peuvent être séparés par des messages ayant un identifiant différent.

Attaque par usurpation

NIST [8] définit l'attaque par usurpation (de l'anglais *spoofing*) comme induire délibérément un utilisateur ou une ressource à prendre une mauvaise action. Sans authentification, n'importe quelle composante connectée au réseau SAE J1939 peut facilement usurper une cible, par contre les messages légitime transmit par la cible peuvent être présents sur le réseau. Dans le cadre de ce mémoire, l'attaque par usurpation est définie par un message légitime qui est remplacé par un message malveillant.

2.3.2 Paramètre pour la prise de décision

Lorsqu'une cyberattaque est détectée sur un système, la réaction principale est de se protéger. Un IPS peut être utilisé pour appliquer une contre-mesure afin de diminuer ou de supprimer l'effet de l'attaque. Dans certains systèmes, notamment pour la technologie des plateformes (PT de l'anglais *Platform Technology*), une contre-mesure peut causer plus de dommage que la cyberattaque elle-même. Anwar et al. [14] quantifient les contre-mesures utilisées selon quelques paramètres. Bien que leur recherche s'applique à un système IT, la discussion concernant la prise de décision reste pertinente. Le concept principal est de comparer le coût des différentes contre-mesures avec le coût de l'attaque. Les paramètres permettant de déterminer le coût de la contre-mesure sont le pourcentage de succès et l'impact que cette contre-mesure a sur le système. Le taux de succès peut être déterminé au cours du temps en évaluant l'application de la contre-mesure. L'impact au système est représenté

par une valeur numérique, mais Anwar et al. ne mentionnent pas comment ils l'ont déterminée.

De plus, un autre défi est la présence de faux positifs lorsqu'un système IPS automatise l'implémentation d'une contre-mesure [14]. Comme discuté à la section 2.2, un vrai positif va affecter le système et la contre-mesure va tenter de corriger l'effet. Tandis que pour un faux positif, qui n'a pas d'effets sur le système, la contre-mesure appliquée peut ajouter un effet non désiré.

Dans le même ordre d'idée, Alsubhi et al. mentionnent deux facteurs utilisés pour déterminer l'impact des attaques et des réponses [15]. Le premier est le dommage potentiel qui tient compte de la sévérité de l'attaque et la probabilité que celle-ci soit présente (un vrai positif). Le deuxième est la perte opérationnelle qui représente le coût d'appliquer une réponse lorsqu'il n'y a pas d'attaque (un faux positif).

Dans cette section, nous avons présenté le déni de service, l'attaque par rejeu ainsi que des paramètres pour la prise de décision. La simulation dans ce mémoire va permettre d'implémenter ces types d'attaques. Nous voulons proposer une approche pour comparer les impacts des attaques et des réponses. Cette comparaison est la représentation des différences entre l'attaque, la réponse, et leur combinaison. La prise de décision est la délibération pour déterminer quel sera le plan d'action. La comparaison, faite dans ce mémoire, permettra de fournir des données pertinentes pouvant assister à la prise de décision d'un IPS.

3 Modèle

Le but de cette recherche est de concevoir un modèle afin de considérer les impacts des attaques et des réponses à celles-ci sur un réseau SAE J1939. Le chapitre 2 a fourni un survol des différentes technologies, des limitations de sécurités, des types d'attaques et des paramètres pour la prise de décision d'un IPS.

Dans le chapitre 3, ces concepts seront utilisés pour définir l'architecture de la solution. Pour ce faire, nous avons développé une approche, basée sur la simulation, pour déterminer l'impact d'une attaque survenue sur un réseau véhiculaire SAE J1939 et celui d'une réponse à cette attaque. Dans l'implémentation, nous avons créé des scénarios qui représentent différents cas d'utilisation; pour chacun, nous simulons le réseau initial avec une attaque, puis nous ajoutons une réponse. Normalement, un IDS analyse un réseau et détermine si une attaque est détectée. L'IPS applique ensuite une réponse pour contrer l'attaque. Dans la solution que nous présentons, l'IDS détecte les attaques, puis associe un modificateur aux messages SAE J1939 affectés. L'IPS évalue ainsi les différents impacts incluant l'attaque et la simulation de réponses à celle-ci en utilisant les modificateurs des messages. Un modificateur (discuté en plus de détails à la section 3.2.2) représente une caractéristique qui affecte un message ou une partie de celui-ci. Cette caractéristique constitue un aspect de la triade CIA qui est compromis. Par défaut, les messages contiennent le modificateur qui représente l'état normal. Par exemple, un des modificateurs est une valeur constante qui est associée à une attaque par rejeu, et un autre représente un message supprimé qui peut être associé à un DoS. Ces modificateurs seront détaillés à la section 3.2.2. La solution est représentée dans l'organigramme à la figure 3.1.

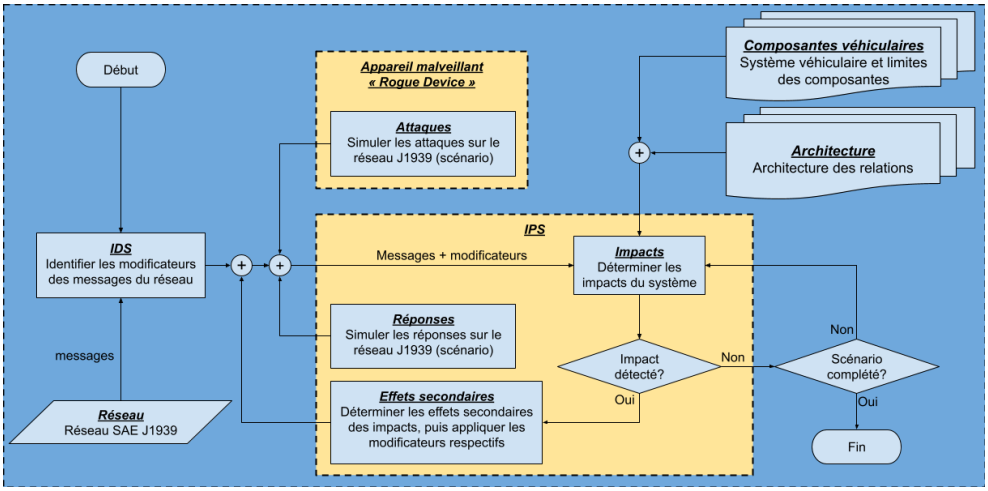

Figure 3.1: **La solution**.

L'organigramme à la figure 3.1 contient les composantes principales de la solution. Les composantes véhiculaires et l'architecture permettent d'établir la simulation des composantes du système (i.e. MCE), leurs limites et les messages échangés par ceux-ci. Cette information est utilisée par l'IPS pour déterminer l'impact potentiel d'une réponse sur le système. L'impact contient deux volets. Le premier concerne l'entrée des données des MCE ou les messages qu'ils reçoivent. Le deuxième concerne les réactions des MCE. Ces réactions incluent les limites des composantes qui peuvent affecter leur état physique ou envoyer des messages erronés sur le réseau. Ces messages peuvent ainsi affecter l'entrée des données, soit le premier volet en tant d'effets secondaires.

Le réseau SAE J1939 représente la séquence des messages qui est fournie à l'IDS, ainsi que l'appareil malveillant qui peut y injecter une attaque. L'IDS analyse le réseau et applique les modificateurs aux messages. Dans l'implémentation de la solution, nous avons simplifié cette étape où nous établissons directement les messages et leurs modificateurs qui tiennent déjà compte de l'attaque selon le scénario. Nous rapellons au lecteur que notre travail présume la présence d'un IDS mais les détails de celui-ci sont hors de la portée de notre travail. Les messages et leurs modificateurs représentent l'entrée de données du IPS et ainsi utilisé par celui-ci pour déterminer l'impact sur le véhicule. Des effets secondaires (discuté à la section 3.2.3) directement relié à l'impact peuvent ainsi être ajoutés au réseau en tant que modificateurs pour les messages affectés.

Pendant que les impacts de l'attaque sont évalués, l'IPS applique à son tour, les modificateurs de la réponse du scénario. L'IPS détermine ainsi l'impact du système résultant qui peut engendrer d'autres effets secondaires sur le réseau en appliquant leurs modificateurs. Ce processus est répété jusqu'à ce qu'un scénario soit complété. Plusieurs scénarios ont été créés afin de pouvoir représenter différents cas d'utilisation et de combinaisons d'attaques et de réponses que nous discuterons à la section 3.3.

Dans ce chapitre nous décrivons les détails de cette solution. En premier lieu, nous allons définir le système véhiculaire et ces composantes. Ceci va permettre d'identifier les spécifications du système pour déterminer l'environnement. En second lieu, nous allons décrire la méthode pour calculer les impacts. Ceci inclura l'intégration des attaques et des réponses ainsi que leurs effets sur le système. En troisième lieu, nous allons discuter des cas d'utilisation à évaluer qui incorporeront les choix de conception reliés à l'implémentation logicielle de la simulation. Finalement, nous allons définir les scénarios qui seront évalués.

3.1 Déterminer le système véhiculaire et ces composantes

Dans cette section, le système véhiculaire et ses composantes seront définis. Ceci va permettre d'identifier les limites et les capacités de l'environnement. Les sujets d'intérêts sont le protocole choisi, les fonctions du véhicule, les types d'information des messages et les messages sélectionnés. Une fois que ceux-ci sont établis, ils seront utilisés pour créer l'architecture d'interrelations des messages.

3.1.1 Protocole choisi

Le protocole SAE J1939 a été sélectionné parce que sa conception inclut déjà plusieurs volets qui peuvent être utilisés pour créer l'environnement du système. Chaque message possède une source, un PGN et une liste de SPN. La source et le PGN, qui contient la destination, permettent d'identifier les liens entre les messages et les MCE. Le PGN et ses SPN associés possèdent déjà une description de leur contenu. Ces éléments du SAE J1939 vont permettre de créer une architecture suffisamment réaliste du véhicule.

3.1.2 Fonctions du véhicule

Les fonctions véhiculaires qui ont été identifiées sont la vitesse, le freinage et la direction. Celles-ci ont été choisies parce qu'elles sont les principales qui peuvent affecter la sécurité de la conduite. La vitesse est le mouvement rectiligne qui est positif (avancer) ou négatif (reculer). Celle-ci peut être constante ou inclure une accélération. Le freinage est la décélération relative du mouvement rectiligne. Que le mouvement soit positif ou négatif, la décélération diminue la vitesse vers une valeur de zéro. La direction est le mouvement rotationnel du véhicule vers la gauche ou vers la droite.

Les véhicules possèdent plusieurs autres fonctions telles que le contrôle des phares, des parebrises, des fenêtres et de la température. Bien quelles soient aussi importantes pour la sécurité de la conduite, elles sont situationnelles à l'environnement extérieur du véhicule. Pour ce mémoire, seules les fonctionnalités reliées au mouvement du véhicule seront considérées.

3.1.3 Types d'information des messages

Les SPN respectifs de chaque PGN représentent les données qui sont contenues dans le message. Les différentes valeurs possibles des SPN varient grandement et peuvent avoir diverses significations. Certaines sont des nombres entiers, d'autres emploient des coefficients pour rapporter la valeur selon une plage de donnée, et certains utilisent les différentes combinaisons des bits du SPN pour représenter un état spécifique.

Les fonctions du véhicule vont utiliser les PGN appropriés pour leurs calculs internes et leur implémentation. Si une fonction utilise une multitude de PGN, la quantité de SPN va s'accroître considérablement. Afin de limiter la quantité de combinaisons considérées, des types d'informations génériques ont été déterminés, soit le contrôle, les données et les options, tels que représentés dans la table 3.1. Ceux-ci permettront de regrouper des données similaires.

Type	**Description**
Contrôle	Ce type représente les commandes utilisées pour contrôler une des fonctions du véhicule (i.e. la vitesse, le freinage et la direction).
Option	Ce type représente une ou plusieurs options ou états utilisés dans les calculs de la fonction.
Données	Ce type représente des données numériques utilisées dans les calculs de la fonction.

Table 3.1: **Les types d'information**.

3.1.4 Messages sélectionnés

Le protocole véhiculaire SAE J1939 contient une grande variété de messages. Ceux-ci sont définis par leur fonctionnalité, leur(s) destinataire(s) et leur priorité. Nous avons reçu une banque de données d'environ un million de messages SAE J1939 du Centre de recherche et développement pour la défense Canada (RDDC) Valcartier, QC [16]. Ces données représentent l'utilisation normale du protocole SAE J1939 à partir de laquelle des statistiques ont été compilées et présentées dans la table 3.2. La table contient quatre colonnes. La première représente la quantité (Qté) de messages. La deuxième représente la proportion (%) de messages par rapport au nombre total de messages. La troisième représente le PGN, et la dernière est le titre ou la description du PGN. La première rangée contient des points de suspension qui indique la présence de messages dont leur quantité ou la proportion est inférieure aux valeurs affichées. Dans la documentation du SAE J1939, certains des PGN identifiés n'étaient pas standardisés, signifiant qu'aucune information sur leur contenu n'était disponible. Ceux-ci ne seront pas considérés dans ce mémoire.

Le titre de chacun des PGN a été ajouté afin d'indiquer leur interaction de haut niveau ainsi que l'utilisation du message. Pour la majorité des messages, le titre du PGN indique une catégorie d'information ou un groupe d'information. Par exemple, les PGN 61443, 65247 et 61444 (en caractères gras dans la table 3.2) ont le même titre à l'exception d'une valeur numérique différente pour chacun d'eux. Afin de les différencier davantage, leur contenu respectif (i.e. SPN) doit être utilisé.

Qté	%	**PGN**	**Titre**
...	...	...	...
013087	1.3	065215	Information concernant la vitesse des roues
013172	1.3	065170	Non standardisé
013172	1.3	065266	Non standardisé
013176	1.3	061445	Non standardisé
013176	1.3	061452	Non standardisé
013176	1.3	065098	Contrôleur électronique de la transmission 7
021720	2.2	000000	Contrôle de la vitesse de couple 1
026324	2.6	065264	Information sur la puissance de décollage
026342	2.6	061455	Post-traitement 1 pour la sortie de gaz 1
026343	2.6	061450	Débit du gaz du moteur
026343	2.6	061491	Non standardisé
026344	2.6	061454	Post-traitement 1 pour le gaz d'admission 1
026505	2.7	000259	Non standardisé
039411	3.9	061441	Contrôleur électronique du freinage 1
039430	3.9	065265	Régulateur de vitesse pour le véhicule
065856	6.6	**061443**	**Contrôleur électronique du moteur 2**
065856	6.6	**065247**	**Contrôleur électronique du moteur 3**
065857	6.6	**061444**	**Contrôleur électronique du moteur 1**
078528	7.9	061449	Contrôle de la stabilité dynamique du véhicule 2
131756	13.2	061442	Contrôleur électronique de la transmission 1

Table 3.2: **Statistiques sur les PGN**.

La sélection des PGN considérés dans ce mémoire a été effectuée en examinant le contenu des messages, les compostantes physiques du système et leur fonctions véhiculaires avec lesquelles l'opérateur peut interagir. Les composantes cyber physiques seront discutées à la section 3.1.5 et les fonctions choisies sont le contrôle de la vitesse, du freinage et de la direction. Pour chacune de ces fonctions, l'information ciblée est l'entrée des données et les échanges entre les MCE.

Peu d'information est disponible à propos des sources et destinations qui sont représentées par des valeurs numériques. La majorité des destinations sont des groupes dont leur format (*PDU Format*) et leur spécification (*PDU Specific*) sont uniques. Les sources et destinations ont été déterminées en utilisant les SPN des messages et la relation logique de ceux-ci. Ces sources ou destinations (i.e. MCE) sont le moteur, la transmission, le châssis et le système de freinage antiblocage (ABS de l'anglais *Anti-lock Braking System*). Les messages sélectionnés sont dans la table 3.3 et représentent 35.1% du trafic normal.

PGN	Titre	Contenu
0	Contrôle de la vitesse de couple 1	Données pour calculer la vitesse
61441	Contrôleur électronique du freinage 1	Contrôle de la pédale de freinage
61442	Contrôleur électronique de la transmission 1	Données pour calculer la vitesse
61443	Contrôleur électronique du moteur 2	Contrôle de la pédale de vitesse
61449	Contrôle de la stabilité dynamique du véhicule 2	Contrôle du volant
65215	Information concernant la vitesse des roues	Données pour calculer la stabilité

PGN	Source	Destination
0	Transmission	Moteur
61441	Moteur, Châssis	ABS, Transmission
61442	Transmission	Moteur
61443	Moteur	Transmission
61449	ABS	Transmission
65215	ABS	Transmission

Table 3.3: **Les PGN sélectionnés**.

Dans la figure 2.4, le PGN et l'adresse de la source sont deux champs différents. Ceci signifie qu'un PGN peut avoir plusieurs sources différentes qui transmettent de l'information similaire. Comme de fait, dans la table ci-haut, le PGN 61441 possède plusieurs sources et destinations. Afin de différencier les types d'information des PGN envoyés par des sources différentes, une description additionnelle et optionnelle va être ajoutée, celle-ci est discutée dans la prochaine section.

3.1.5 Architecture d'interrelations des messages

L'architecture d'interrelations des messages sera établie en combinant les sous-sections précédentes. Cette architecture sera utilisée pour déterminer les impacts et les effets secondaires du système.

En utilisant les messages sélectionnés et l'information disponible sur ceux-ci, les MCE choisis sont le moteur, la transmission, l'ABS et le châssis. Les MCE interagissent directement avec le bus SAE J1939 et permettent à d'autres appareils de s'y interfacer comme représenté à la figure 3.2. Les MCE principaux sont connectés à leurs composantes véhiculaires respectifs qui agissent soit comme senseur ou actionneur. Les pédales d'accélération et de freinage

sont connectées au MCE moteur et sont des senseurs. Le châssis est un senseur connecté au MCE châssis. Les freins et ABS sont connectés au MCE ABS et ils sont des actionneurs tout comme la transmission et le moteur.

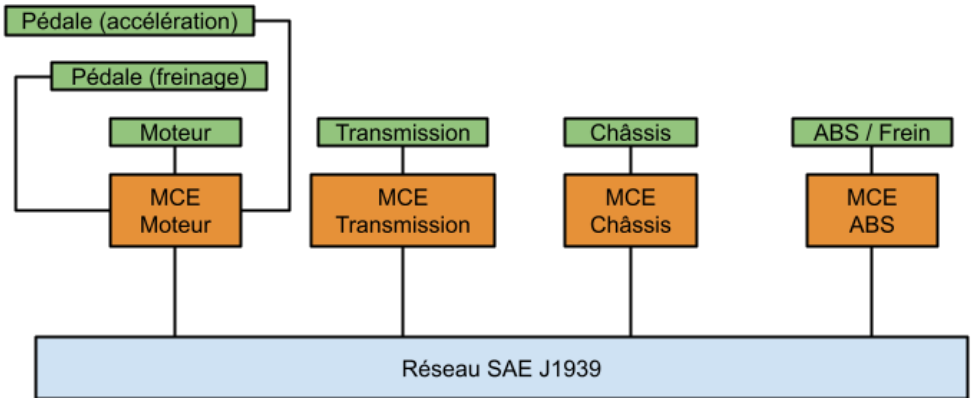

Figure 3.2: **Le système véhiculaire**.

L'architecture d'interrelations est représentée dans la figure 3.3. Ce diagramme détermine les connexions entre les MCE, les PGN, les types, et les fonctions. Les boîtes bleues sont les MCE et elles sont associées à une fonction et à un type. La majorité des MCE sont associés à une fonction unique, par contre, ce n'est pas toujours le cas. Par exemple, la fonction du MCE moteur est associée à la vitesse, mais le MCE est aussi physiquement connecté à la pédale du frein qui est associé au freinage.

La description optionnelle est utilisée pour amplifier l'utilisation de la fonction; nous discutons de chacune des valeurs possibles de cette description optionnelle. La valeur d'entrée indique que le MCE reçoit de l'information d'un senseur et une valeur de sortie indique que le MCE contrôle un actionneur. L'outrepasser signifie un contournement de la normale de la fonction. Par exemple, le freinage possède une priorité pour affecter la vitesse et doit outrepasser la fonction normale de la vitesse.

Les boîtes grises sont les PGN et elles sont associées à un type. La description optionnelle est utilisée pour amplifier l'utilisation du PGN. Aucune fonction n'y est associée, car les messages ne sont pas directement connectés à un senseur ou à un actionneur. Les flèches de couleurs représentent la direction des lignes qui relient les boîtes. Le vert indique le début de la connexion et le rouge indique la fin. L'utilisation des flèches de couleurs sert uniquement

à simplifier la représentation visuelle du diagramme dans lequel certaines des connexions vont dans le sens inverse.

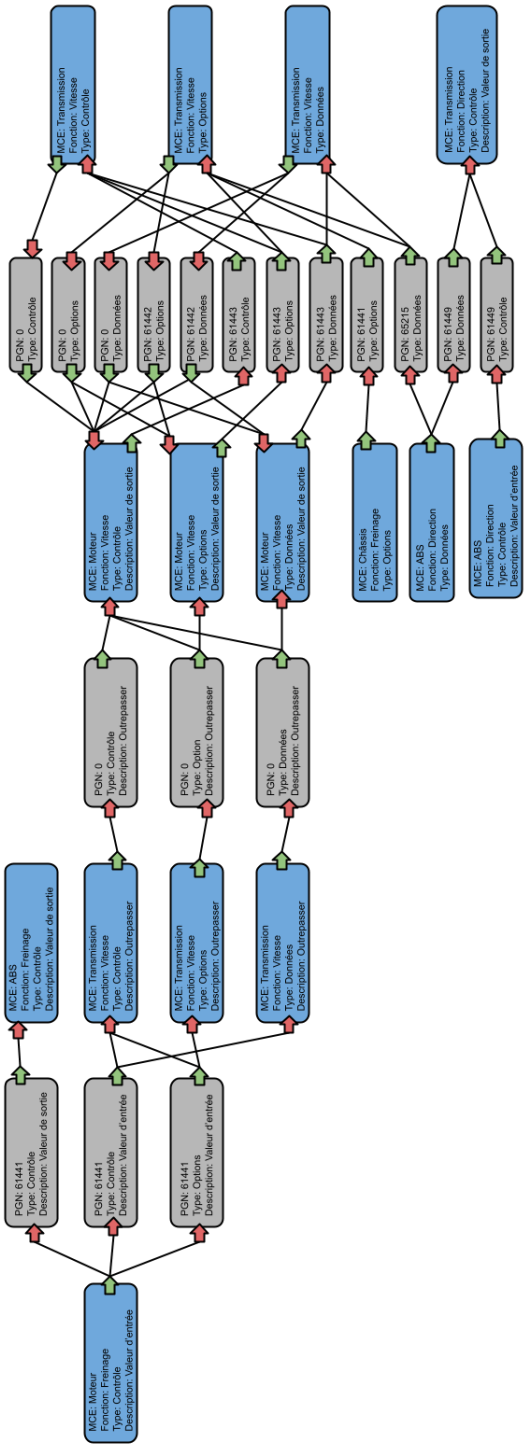

Figure 3.3: **L'architecture d'interrelations.**

3.2 Méthode permettant de calculer les impacts

Dans cette section nous identifions la méthode pour calculer les impacts. Ceci va permettre de représenter les liens entre les composantes, les messages et les impacts. Les sujets d'intérêts sont les capacités des composantes, les modificateurs, les impacts et effets secondaires, et le mécanisme pour déterminer l'impact.

3.2.1 Capacités des composantes

Les composantes du réseau et leurs capacités à l'influencer sont représentées à la figure 3.4. Les MCE peuvent écouter, transmettre et recevoir des messages. L'écoute de messages indique que l'appareil peut déterminer ce qui est transmis sur le bus sans intervenir. Tous les appareils peuvent écouter sur le bus, car le SAE J1939 est un bus « tous informés », une fonctionnalité héritée du bus CAN. La transmission de messages signifie que les MCE peuvent envoyer des messages sur le bus. La réception de messages signifie que les MCE peuvent déterminer quand ils sont destinataires du contenu des messages et qu'ils réagissent lorsque ceux-ci sont reçus. L'IPS peut écouter, collecter, transmettre et interrompre le bus. Tandis que l'IDS peut seulement écouter sur le bus et collecter des messages de celui-ci. La collection d'information est la capacité à analyser les messages échangés sur le bus. L'interruption du bus est la capacité de transmettre, hors du fonctionnement normal du réseau, qui inclut cesser la transmission d'un message. L'appareil malveillant ou « Rogue Device » peut aussi écouter, collecter, transmettre et interrompre le bus. La différence principale entre ceux-ci est que l'IPS et l'appareil malveillant ne reçoivent pas de messages, et donc ne peuvent pas être affectés par le réseau ou le contenu des messages.

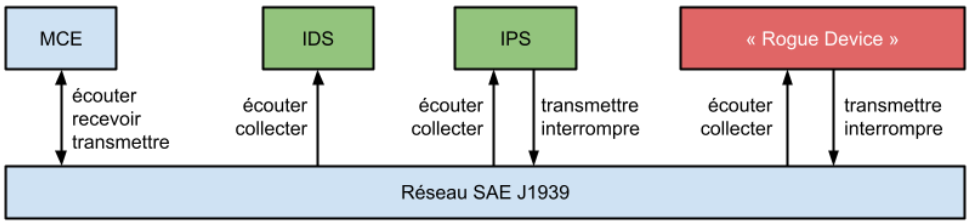

Figure 3.4: **La portée du système**.

3.2.2 Modificateurs

Un modificateur représente une caractéristique qui affecte un message ou une partie de celui-ci. Les modificateurs sont séparés en trois types selon les composantes de la triade CIA, soit la confidentialité, l'intégrité et la disponibilité. Dans ce mémoire, la confidentialité sera exclue du travail, car elle représente l'accès non autorisé à l'information qui n'a pas d'impact sur le système.

Les modificateurs sont présentés à la table 3.4. Le premier groupe de la table contient les modificateurs principaux qui sont obligatoires. Le terme obligatoire est utilisé pour indiquer qu'un message ne peut pas exister sans un de ces modificateurs. Le deuxième groupe est des modificateurs secondaires qui doivent être combinés à un modificateur du groupe précédent du même type.

Groupe 1 (Obligatoire)

Modificateur	**Description**	**Type**
N	Contiens une valeur normale.	Intégrité
C	Contiens une valeur constante.	Intégrité
U	Contiens une valeur inconnue.	Intégrité
X	Contiens une valeur supprimée.	Disponibilité

Groupe 2 (Secondaire)

Modificateur	**Description**	**Type**
L	Contiens une valeur anormalement moindre.	Intégrité
H	Contiens une valeur anormalement supérieure.	Intégrité

Table 3.4: **La liste des modificateurs**.

L'intégrité découle de l'évaluation du contenu qui détermine si celui-ci suit ou diverge de la normale. Les modificateurs utilisés dans ce contexte sont le « L », « H », « C », « U » et « N ». Le « L » signifie que la valeur du contenu est moindre que celle anticipée. Le « H » signifie que la valeur du contenu est supérieure que celle anticipée. Ces deux modificateurs sont utilisés pour les types du contrôle et des données. Le « C » indique que le contenu du message est constant ou identique au message précédent du même PGN. Par exemple, les messages ajoutés par une attaque par rejeu auraient ce modificateur. Le « U » indique que le contenu du message est inconnu, mais n'est pas considéré moindre ou supérieur que la valeur anticipée. Ce modificateur peut être utilisé dans les situations où il y a une incertitude sur l'interaction entre l'attaque et la réponse. Le « N » indique que le contenu est normal, anticipé ou sans erreurs. Il est principalement utilisé pour les messages qui suivent le

fonctionnement attendu du système et c'est le modificateur par défaut qui est utilisé dans le trafic simulé.

La disponibilité découle de l'évaluation de la présence ou de l'absence d'un message. Le seul modificateur utilisé dans ce contexte est le « X ». Celui-ci indique que le message a été supprimé, c'est-à-dire qu'il n'a pas été envoyé sur le bus. De plus, la disponibilité évalue la bande passante du bus et la fréquence de transmission ou de réception des messages. Celles-ci ne sont pas représentées sous forme de modificateurs, mais peuvent tout de même créer un impact sur le système.

3.2.3 Impacts et effets secondaires

Comme mentionné précédemment, l'impact au système contient deux volets. Le premier concerne l'entrée des données des MCE. Lorsqu'ils reçoivent des messages, le contenu de ceux-ci peut les affecter directement. Ceci inclut les fonctionnalités du MCE et les limites de ces composantes internes qui peuvent bouleverser leur état physique. Le deuxième concerne la sortie des données suivant le premier impact. Les changements induits par l'entrée des données peuvent influencer les messages que le MCE transmet. Ces messages peuvent, à leur tour, influencer l'entrée des données des autres MCE. Les impacts qui sont ainsi induits représentent les effets secondaires du système.

Quatre éléments peuvent affecter un message ou ses modificateurs dans le système. Le premier est le réseau de base qui contient les messages échangés et leur modificateur par défaut. Dans ce mémoire, le réseau de base ne contient pas d'erreurs. Les deuxième et troisième sont l'appareil malveillant « Rogue Device » et l'IPS qui peuvent interrompre le réseau. Le dernier est la sortie des données d'un MCE qui a été affecté par leur entrée des données.

La source qui introduit chacun de ces quatre éléments détermine l'ampleur des effets qu'elle peut avoir sur le réseau. L'intégrité des messages du réseau peut seulement être affectée par les MCE. L'IPS et l'appareil malveillant peuvent affecter l'intégrité d'un message, par contre, ce sera seulement pour un message qu'ils ont eux-mêmes transmis sur le réseau. La disponibilité des messages peut être affectée par les quatre éléments. La disponibilité indique soit l'ajout, la suppression ou un délai de la transmission d'un message.

La figure 3.5 représente l'interaction entre les quatre éléments. Un scénario sera utilisé pour expliquer la séquence de messages transmis dans le dia-

gramme. Dans celui-ci, un appareil malveillant usurpe un message qui supprime le message original en le remplaçant par un message erroné ayant une valeur constante anormalement élevée. L'IPS contre ce comportement par la suppression du message erroné pour le remplacer par un message ayant une valeur constante. Ici, nous utilisons un IPS qui transmet un message avec une valeur constante uniquement pour aider à la compréhension des quatre éléments. Les numéros signifient les quatre éléments qui peuvent affecter l'entrée des données. Dans l'ordre, le Nº1 signifie un message normal transmis par un MCE. Le premier Nº2 est une attaque de disponibilité qui supprime un message original. Le deuxième Nº2 est l'ajout d'un nouveau message avec une valeur constante et élevée par l'appareil malveillant. À ce point-ci, tous les messages normaux ont été supprimés et remplacés. Le premier Nº3 est l'ajout d'un message avec une valeur constante par l'IPS. Le deuxième Nº3 indique la suppression d'un message malveillant. À ce point-ci, tous les messages normaux et malveillants ont été supprimés, et il ne reste que les messages de l'IPS. Le message à valeur constante est reçu par un MCE et peut ainsi introduire un impact et affecter son comportement et ses messages de sortie. Dans ce scénario, l'entrée de données influence le MCE à transmettre un message ayant une valeur constante. Le Nº4 représente la sortie des données d'un MCE où son message normal contient maintenant une valeur constante. Des effets secondaires peuvent ainsi suivre ce changement où des impacts subséquents ont été subis par d'autres MCE du réseau.

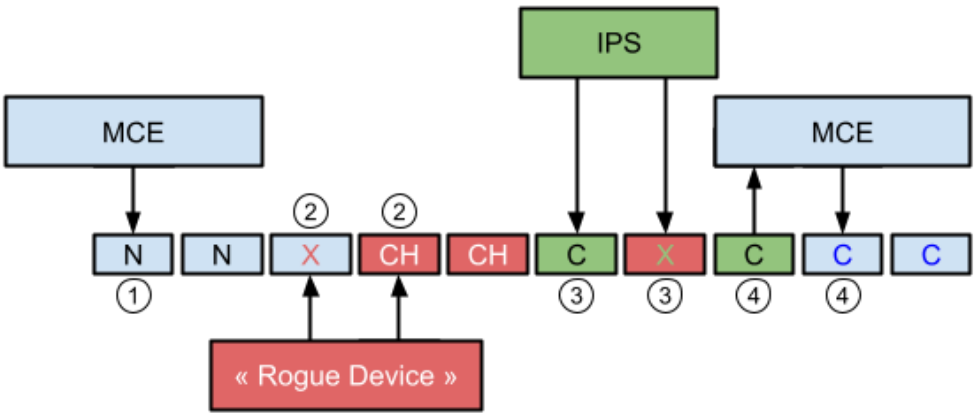

Figure 3.5: **Un exemple des messages et de leurs modificateurs**.

3.2.4 Mécanisme pour déterminer l'impact

La figure 3.3 montre les liens entre les PGN et les MCE. L'entrée de données de ces connexions existantes peut provoquer des impacts sur le MCE qui reçoit les messages.

Nous établissons des profils d'entrée de données pour déterminer les impacts. Ces profils agissent similairement à un IDS par anomalie discutée à la section 2.2, mais au lieu d'être utilisés pour détecter un événement malveillant, ils sont utilisés pour identifier les impacts. Le mécanisme doit pouvoir reconnaître des messages normaux ainsi que quelques variations telles que le déni de service, l'attaque par rejeu, et l'attaque par usurpation. La solution implémentée utilise les dix derniers messages ayant les mêmes PGN, type et description, puis les compare à des profils prédéterminés. L'impact est présent si la comparaison avec les profils excède un seuil de similarité établi. Nous discutons de la sélection du seuil à la section 3.4. Pour chaque MCE, les impacts sont influencé par l'entrée de données, le type d'information, leurs fonctions au véhicule et leur relation avec les autres MCE. Lorsqu'un impact est présent, les données de sortie du MCE peuvent être affectées créant ainsi un effet secondaire. Les impacts sont représentés dans la table 3.6.

Ce mécanisme est expliqué à l'aide de l'exemple à la figure 3.6 et à la table 3.5. Cette figure représente une portion de l'architecture d'interrelations de la figure 3.3. Dans la figure 3.6, le MCE ciblé est celui de la transmission qui outrepasse le contrôle de la vitesse et celui-ci est identifié à l'aide d'un losange vert. L'entrée de données est le PGN 61441 qui contient de l'information de contrôle et la sortie de données est le PGN 0 qui contient aussi de l'information de contrôle. Dans la table table 3.5, les profils sélectionnés contiennent l'entrée de données, un impact associé et la sortie de donnée attendue pour trois exemples. Le premier exemple indique que les dix derniers messages sont normaux, qu'aucun impact n'est identifié et que la sortie des données anticipée est un message normal. L'information pour le contrôle du PGN 61441 contient une valeur normale que la transmission reçoit. Une fois reçu, le MCE transmet un PGN 0 où son information de contrôle est normale.

Le deuxième exemple représente une attaque par rejeu où une valeur constante est identifiée à chaque deux messages. Dans cet exemple, la valeur de contrôle est mise à jour à chaque deux messages, ce qui a pour impact de ralentir le temps de mise à jour de la vitesse de la transmission. La sortie des données, la valeur de contrôle du PGN 0, est la même que l'entrée et alterne

entre un message normal et constant. Le moteur reçoit ainsi le PGN 0 où la valeur pour le contrôle pour outrepasser la vitesse alterne entre une valeur normale et constante. Cet MCE applique, à son tour, les impacts de ces profils. Cet effet se propage au travers du reste du système.

Le troisième exemple représente une attaque par usurpation où l'appareil malveillant transmet des valeurs aléatoires. Pour le contrôle de la vitesse, ceci signifie qu'il est imprévisible et que sa sortie de données est aussi inconnue. Le PGN 0 transmis entre la transmission et le moteur contient donc aussi de l'information inconnu pour le contrôle de vitesse.

Dans la figure 3.6, nous avons ajouté une deuxième rangée où le MCE et le PGN s'attardent au type de données pour outrepasser la vitesse. Le PGN 61441 (le contrôle de la vitesse) influence aussi les données de la vitesse de la transmission. Ceci peut affecter, à son tour, les données du PGN 0. Le moteur qui reçoit le PGN 0 doit considérer la partie du message qui contient la valeur pour le contrôle et celle des données.

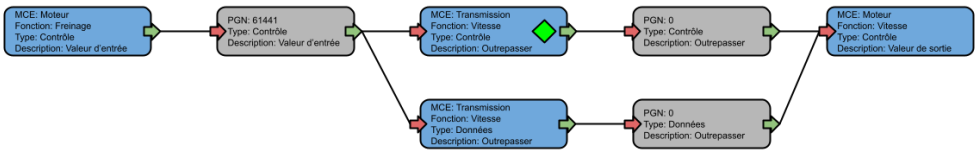

Figure 3.6: **Portion de l'architecture d'interrelations**.

Entrée des données (Profil)	**Impacts**	**Sortie des données**
N N N N .. →	-	→ N...
N C N C .. →	réduction du temps de mise à jour pour la vitesse	→ N C...
U U U U .. →	valeur de vitesse imprévisible	→ U...

Table 3.5: **Exemple de profils**.

Si plusieurs modificateurs sont appliqués à un même PGN, une comparaison est calculée pour déterminer le modificateur résultant. Ce calcul se résume à $N < C < U < X$ et $L < H$ où le modificateur le plus élevé est la résultante. Ceci est utilisé pour la sortie de données lorsque l'appareil malveillant ou l'IPS affecte les messages. Le modificateur X, relié à la disponibilité ou à

la suppression d'un message, possède la plus grande valeur.

La table 3.6 contient la liste complète des profils selon les valeurs d'entrée, les impacts et les valeurs de sortie. Le contrôle, les options et les données ne vont pas affecter les impacts avec la même envergure. Les fonctions du MCE sont affectés directement pour le contrôle, ainsi que le stress physique qu'il pourrait subir. Dans la solution présentée à la figure 3.1, les limites du stress physique seraient déterminées par les composantes véhiculaires. Dans ce mémoire, le cas principal qui peut causer un stress physique est l'alternance de l'entrée des données entre une valeur basse et une valeur élevée représentée à l'aide des modificateurs L et H .

Contrôle

Entrée	**Impacts**	**Sortie**
N..	-	N..
CL..	La fonction est forcée à une valeur constante faible.	CL..
C..	La fonction est forcée à une valeur constante.	C..
CH..	La fonction est forcée à une valeur constante élevée.	CH..
N C..	Il y a une réduction du temps de mise à jour de la fonction.	N C..
U..	Le contrôle de la fonction est imprévisible.	U..
X..	Le contrôle de la fonction n'est pas disponible.	X..
N CH..	L'appareil véhiculaire associé subit une augmentation de stress physique.	N CH..
NL NH..	L'appareil véhiculaire associé subit une dangereuse augmentation de stress physique.	NL NH..
N NH..	L'appareil véhiculaire associé subit une augmentation de stress physique.	N NH..

Options

Entrée	**Impacts**	**Sortie**
N..	-	N..
C..	Les options sont constantes.	C..
U..	Les options sont instables.	U..
X..	Les options ne sont pas disponibles.	X..

Données

Entrée	**Impacts**	**Sortie**
N..	-	N..
C..	Les données ont une valeur constante.	C..
N C..	Il y a une réduction du temps de mise à jour des données.	N C..
U..	Les données sont imprévisibles.	U..
X..	Les données ne sont pas disponibles.	X..

Table 3.6: **Survol des profils**.

3.3 Cas d'utilisation

Dans cette section, nous allons présenter deux cas d'utilisation qui seront utilisés pour supporter l'aspect exploratoire du but. Nous rappelons que le but de cette recherche est de concevoir un modèle afin de considérer les impacts des attaques et des réponses à celles-ci sur un réseau SAE J1939.

Le premier cas d'utilisation est utilisé pour explorer l'implémentation du modèle. L'objectif est de confirmer que le modèle peut considérer les attaques et les réponses pour déterminer l'impact résultant. Pour ce faire, nous allons déterminer l'impact pour chaque état de la matrice de confusion, puis les comparer aux impacts anticipés. Pour le VP, l'attaque et la réponse affectent le système. Pour le VN, le système n'est pas affecté. Pour le FP, uniquement la réponse affecte le système. Pour le FN, uniquement l'attaque affecte le système. Le deuxième cas d'utilisation sert à explorer la sensibilité de l'implémentation du modèle. Son objectif est d'évaluer si le modèle peut déterminer des impacts résultants différents pour des situations similaires. Pour ce faire, nous allons simuler deux réponses similaires pour la même attaque, puis comparer les impacts résultants.

Les cas d'utilisation contiennent des scénarios qui représentent la simulation d'un système où une attaque ou réponse peuvent survenir. Pour le premier cas d'utilisation, le premier scénarios est l'implémentation d'une attaque et réponse, puis le deuxième scénario est l'implémentation de cette même réponse uniquement. Pour le deuxième cas d'utilisation, les scénarios sont l'implémentation de deux réponses similaires pour une même attaque. Les séquences de messages des cas d'utilisation sont représentés dans les tables 3.7 et 3.8. Les groupes représentent un message ajouté ainsi que tous les changements de modificateurs qui l'affectent. Dans la colonne du groupe, le (A) représente un aspect de l'attaque et le (R) celui de la réponse. Les valeurs de ($d1$, $d2$, ...) dans la colonne du temps de début sont un décalage de temps pour ordonner les messages. Ce décalage, de l'ordre de 1 milliseconde, est utilisé pour forcer une séquence lorsqu'un message est ajouté. Cette limitation est causée par l'arbitration où deux messages ayant le même PGN vont causer des collisions lorsqu'ils sont transmis en même temps.

3.3.1 Cas d'utilisation 1 - Impact d'une attaque et d'une réponse

L'objectif du premier cas d'utilisation est de confirmer que le modèle peut considérer les attaques et les réponses pour déterminer l'impact résultant. Pour ce faire, nous allons déterminer l'impact pour chaque état de la matrice de confusion, puis les comparer aux impacts anticipés. Le premier scénario, où l'attaque et la réponse sont présents, démontre le VN, FN et le VP. Le deuxième scénario, où seulement la réponse est présente, démontre le VN et le FP. Les résultats pour ces scénarios seront décrits en détail à la section 4.1.

La situation qui pourrait causer ces scénarios serait un appareil malveillant qui usurpe le PGN 61441 pour lui donner une valeur élevée constante afin d'affecter la valeur de sortie du contrôle du freinage. Pour ce faire, l'appareil malveillant ferait l'interruption du message original du PGN 61441, et retransmettrait un message du même PGN où le contrôle (valeur de sortie) possède le modificateur CH. Pour la réponse, l'IPS interrompe le message usurpé que l'appareil malveillant a transmis.

Groupe	PGN	Type et description	Intervalle (ms)	Début (s)	Mod
1	0	-	10	0	N
2	61441	-	100	0	N
2.1 (A)	61441	-	100	2	X
3 (A)	61441	-	100	2 ($d1$)	N
3.1 (A)	61441	Contrôle, Valeur de sortie	100	2 ($d1$)	CH
3.2 (R)	61441	-	100	4 ($d1$)	X
4	61442	-	10	0	N
5	61443	-	50	0	N
6	61449	-	10	0	N
7	65215	-	100	0	N

(a) Scénario 1 - Attaque présente

Groupe	PGN	Type et description	Intervalle (ms)	Début (s)	Mod
1	0	-	10	0	N
2	61441	-	100	0	N
2.1 (R)	61441	-	100	4	X
3	61442	-	10	0	N
4	61443	-	50	0	N
5	61449	-	10	0	N
6	65215	-	100	0	N

(b) Scénario 2 - Pas d'attaque

Table 3.7: **Séquence de messages du Cas d'utilisation 1 - Impact d'une attaque et d'une réponse**.

La table 3.7(a) représente le premier scénario. Dans ce scénario, les PGN 0, 61442, 61443, 61449 et 65215 (ou les groupes 1, 4, 5, 6 et 7) sont inchangé par l'attaque ou la réponse. Leur modificateur est celui par défaut de N, leur intervalle est celui associé à leur PGN respectif, et leur temps de début est de 0 seconde. Ces PGN peuvent être affectés lorsque la simulation effectuera les calculs des impacts et des effets secondaires. Le groupe 2 représente le PGN 61441 original dont son intervalle, temps de début et modificateur sont ceux du réseau de base. Dans le groupe 2.1(A), au temps de 2 secondes, l'attaque interrompe le PGN 61441 et le modificateur associé est le X. Ceci indique que l'appareil malveillant a supprimé ce message. Dans le groupe 3(A), l'appareil malveillant ajoute, à son tour, un PGN 61441 dont il change le modificateur de contrôle (valeur de sortie) à CH. Ce changement est effectué dans le groupe 3.1(A). Les groupes 3(A) et 3.1(A) sont effectué au temps de début de 2 secondes lors de la période pour l'attaque. L'IPS interrompt le PGN 61441 malveillant au temps de 4 secondes durant la période de la réponse. Ceci est

effectué dans le groupe 3.2(R) et le modificateur associé est le X. Ce scénario représente un appareil malveillant qui attaque un réseau en usurpant un message et un IPS qui supprime ce message en réponse à l'attaque.

La table 3.7(b) représente le deuxième scénario. Dans ce scénario, les PGN 0, 61442, 61443, 61449 et 65215 (ou les groupes 1, 4, 5, 6 et 7) sont inchangé par l'attaque ou la réponse. Leur modificateur est celui par défaut de N, leur intervalle est celui associé à leur PGN respectif, et leur temps de début est de 0 seconde. Ces PGN peuvent être affectés lorsque la simulation effectuera les calculs des impacts et des effets secondaires. Le groupe 2 représente le PGN 61441 original dont son intervalle, temps de début et modificateur sont ceux du réseau de base. Dans le groupe 2.1(R), au temps de 4 secondes, l'IPS interrompe le PGN 61441 et le modificateur associé est le X. Ceci est une adaptation où l'IPS supprime le PGN 61441, car ce PGN a été identifié par l'IDS comme étant malveillant. Ce scénario représente un IPS qui supprime un message faussement identifié comme étant malveillant.

3.3.2 Cas d'utilisation 2 - Impact de réponses différentes à une attaque

L'objectif du deuxième cas d'utilisation est d'évaluer si le modèle peut déterminer des impacts résultants différents pour des situations similaires. Pour ce faire, nous allons simuler deux réponses similaires pour la même attaque, puis comparer les impacts résultants. Les résultats seront décrits en détail à la section 4.2.

La situation illustrant ceci est un appareil malveillant qui essaie de contrôler ou de noyer le PGN 0 en envoyant trois messages additionnels à la suite du message original. Ces messages CH veulent forcer une augmentation de vitesse. L'IPS réagit en envoyant trois autres messages pour tenter de contrer les effets des messages malveillants. Ces messages CL veulent contrer cette augmentation de vitesse en forçant une vitesse basse. Les deux implémentations vont transmettre leurs trois messages. La première réponse va les entrelacer avec ceux qui sont malveillants et la deuxième va les transmettre après les messages malveillants. Les scénarios sont représentés dans la table 3.8.

Groupe	PGN	Type et description	Intervalle (ms)	Début (s)	Mod
1	0		10	0	N
2 (A)	0		10	2 ($d1$)	N
2.1 (A)	0	Contrôle	10	2 ($d1$)	CH
3 (R)	0		10	4 ($d2$)	N
3.1 (R)	0	Contrôle	10	4 ($d2$)	CL
4 (A)	0		10	2 ($d3$)	N
4.1 (A)	0	Contrôle	10	2 ($d3$)	CH
5 (R)	0		10	4 ($d4$)	N
5.1 (R)	0	Contrôle	10	4 ($d4$)	CL
6 (A)	0		10	2 ($d5$)	N
6.1 (A)	0	Contrôle	10	2 ($d5$)	CH
7 (R)	0		10	4 ($d6$)	N
7.1 (R)	0	Contrôle	10	4 ($d6$)	CL
8	61441		100	0	N
9	61442		10	0	N
10	61443		50	0	N
11	61449		10	0	N
12	65215		100	0	N

(a) Réponse 1 - Entrelacé

Groupe	PGN	Type et description	Intervalle (ms)	Début (s)	Mod
1	0		10	0	N
2 (A)	0		10	2 ($d1$)	N
2.1 (A)	0	Contrôle	10	2 ($d1$)	CH
3 (A)	0		10	2 ($d3$)	N
3.1 (A)	0	Contrôle	10	2 ($d3$)	CH
4 (A)	0		10	2 ($d5$)	N
4.1 (A)	0	Contrôle	10	2 ($d5$)	CH
5 (R)	0		10	4 ($d6$)	N
5.1 (R)	0	Contrôle	10	4 ($d6$)	CL
6 (R)	0		10	4 ($d7$)	N
6.1 (R)	0	Contrôle	10	4 ($d7$)	CL
7 (R)	0		10	4 ($d8$)	N
7.1 (R)	0	Contrôle	10	4 ($d8$)	CL
8	61441		100	0	N
9	61442		10	0	N
10	61443		50	0	N
11	61449		10	0	N
12	65215		100	0	N

(b) Réponse 2 - Subséquent

Table 3.8: **Séquence de messages du Cas d'utilisation 2 - Impact de réponses différentes à une attaque**.

Les deux scénarios indiqués à la table 3.8 portent sur le même réseau de base et subissent la même attaque, mais l'IPS effectue deux réponses différentes. Dans ces scénarios, les PGN 61441, 61442, 61443, 61449 et 65215 (ou les groupes 8, 9, 10, 11 et 12) sont inchangé par l'attaque ou la réponse. Leur modificateur est celui par défaut de N, leur intervalle est celui associé à leur PGN respectif, et leur temps de début est de 0 seconde. Ces PGN peuvent être affectés lorsque la simulation effectuera les calculs des impacts et des effets secondaires. Le groupe 1 représente le PGN 0 original dont son intervalle, temps de début et modificateur sont ceux du réseau de base. Dans ces scénarios, l'appareil malveillant ajoute trois messages fautifs. Dans la table 3.8(a), pour les groupes $2(A)$, $4(A)$ et $6(A)$, l'appareil malveillant ajout un PGN 0 dont il change le modificateur du contrôle (valeur de sortie) à CH. Ce changement est effectué dans les groupes $2.1(A)$, $4.1(A)$ et $6.1(A)$ respectivement. Dans la table 3.8(b), cette même séquence d'attaque est effectuée pour les groupes $2(A)$, $2.1(A)$, $3(A)$, $3.1(A)$, $4(A)$ et $4.1(A)$. Les temps de début des attaques de ces deux scénarios sont décalés par les mêmes valeurs de $d1$, $d3$ et $d5$ respectivement. Cette séquence de décalage a été choisie parce qu'elle est inchangée pour les deux réponses dont l'une entrelace ces messages avec ceux de l'attaque.

La première réponse de la table 3.8(a) entrelace des messages entre ceux de l'attaque. Dans les groupes $3(R)$, $5(R)$ et $7(R)$, l'IPS ajout un PGN 0 dont il change le modificateur du contrôle (valeur de sortie) à CL. Ce changement est effectué dans les groupes $3.1(R)$, $5.1(R)$ et $7.1(R)$ respectivement. Les temps de début des réponses sont décalés par les valeurs de $d2$, $d4$ et $d6$ respectivement.

La deuxième réponse de la table 3.8(b) ajoute des messages après ceux de l'attaque. Dans les groupes $5(R)$, $6(R)$ et $7(R)$, l'IPS ajout un PGN 0 dont il change le modificateur du contrôle (valeur de sortie) à CL. Ce changement est effectué dans les groupes $5.1(R)$, $6.1(R)$ et $7.1(R)$ respectivement. Les temps de début des réponses sont décalés par les valeurs de $d6$, $d7$ et $d8$ respectivement.

3.4 Choix de conceptions

Dans cette section, nous allons présenter certains choix de conception qui ont été faits afin d'adapter ou de faciliter l'implémentation logicielle de la simulation. Ces choix incluent la simulation du système et une représentation chronologique.

3.4.1 Simulation du système

La simulation du système a été conçue pour permettre une flexibilité sur l'implémentation des réponses. Les choix de conception principaux, discutés ici-bas, comprennent la création de scénarios, la linéarité des messages, la séquence des attaques et des réponses, la sélection du seuil et la représentation des messages supprimés.

L'implémentation de la simulation utilise des scénarios pour définir le réseau, les attaques et les réponses. Dans le chapitre 3, nous avons présenté les différents éléments du diagramme de la figure 3.1. Parmi ceux-ci, nous avons le réseau, les attaques et les réponses. Ces trois éléments sont définis pour chaque scénario, puis la simulation calcule les impacts et effets secondaires du système.

Chaque scénario contient sa propre représentation chronologique qui peut ainsi être comparée à d'autres scénarios. Pour le premier cas d'utilisation, deux scénarios sont créés où le premier contient l'attaque et la réponse, et le deuxième seulement la réponse. Pour le deuxième cas d'utilisation, un scénario est créé pour chaque réponse.

Tous les messages du système sont générés avant de simuler leur transmission sur le réseau. Dans un réseau normal du SAE J1939, les MCE vont tenter de transmettre leurs messages à leur fréquence prédéterminée indépendamment des autres MCE. Lorsqu'il y a une collision lors de la transmission, le processus d'arbitration permet au réseau de gérer la priorité des messages. Un seul message est transmis, et le reste des messages vont tenter plus tard. Ce processus transforme l'entrée de donnée parallèle tentée par les MCE en flux linéaire de messages sur le bus. La simulation enlève cet aspect parallèle afin de simplifier l'implémentation. Les messages sont générés à leur fréquence respective, puis l'arbitration est faite au niveau du logiciel de simulation pour déterminer l'ordre de messages à transmettre.

Les scénarios définissent la séquence des attaques et des réponses en utilisant les messages et leurs modificateurs. Dans un réseau normal, un IDS serait utilisé pour identifier quels messages sont affectés par une attaque, puis un IPS implémenterait une réponse. L'IDS et l'IPS sont ainsi des tierces parties indépendantes du réseau. Afin de simplifier cette interaction, les attaques et les réponses sont introduites par la simulation lors de la génération des messages. Elles sont représentées par l'utilisation de modificateurs. Pour un scénario, chaque message contient une liste de changement de modificateurs en fonction du temps. Les modificateurs associés à l'attaque commencent à 2 secondes, et ceux qui sont associés à la réponse commencent à 4 secondes. Donc, une fois que les messages sont générés, les seuls changements additionnels aux messages sont les effets secondaires.

La simulation associe de l'information additionnelle à chaque message pour contrôler sa transmission dans la séquence de messages. Chaque message va avoir un temps de début et de fin, une fréquence, et une longueur. La longueur par défaut est de 135 bits, discutée à la section 2.1.2. Nous avons choisi une longueur de 0 bit lorsque le message est supprimé. Cette valeur peut varier en fonction de l'implémentation des attaques ou des réponses. Par exemple, un appareil malveillant qui veut usurper un message, mais qui désire utiliser la majorité de l'information réelle, devra supprimer le message une fois que les données sont transmises sur le bus. Le PGN, les temps de début et de fin, la fréquence et la longueur sont utilisés pour déterminer l'ordre des messages selon l'arbitration. Les messages du réseau de base ont un temps de 0 à 6 secondes, les attaques de 2 à 6 secondes, et les réponses de 4 à 6 secondes.

Les modificateurs peuvent affecter les messages en entier ou seulement certaines composantes telles que les combinaisons de types d'information et description. Nous expliquons cette relation à la figure 3.7. Dans la figure, le PGN 0 contient trois types d'information qui sont le contrôle, l'option et les données. Le PGN 0 a un modificateur N de 0 à 4 secondes, puis X de 4 à 6 secondes. Ce modificateur affecte le message en entier, donc à la seconde 4 tout le contenu du PGN 0 va contenir un modificateur X. Si le contrôle possède un modificateur C de 2 à 6 secondes, le X du message sera tout de même appliqué. Les lignes pointillées signifient qu'aucun modificateur n'existe, donc par défaut ça sera celui du message qui possède un modificateur N. Pour chaque scénario déterminé dans la section 3.3, les modificateurs des messages et leurs combinaisons de types d'information et description seront spécifiés.

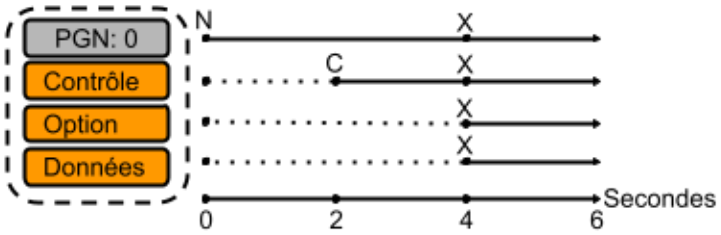

Figure 3.7: **Exemple d'un modificateur d'un message**.

Les messages supprimés n'existent pas dans un réseau réel, mais la simulation doit traiter de tels messages. Nous avons identifié trois situations pour lesquelles des choix de conception ont été implémentés afin de s'adapter aux messages supprimés. La première situation est lors de la génération des messages. L'arbitration compare les messages qui attendent d'être transmis et les sélectionne en ordre de priorité. Il existe une possibilité où un PGN en attente n'est pas transmis et que son prochain message arrive dans la liste d'attente. Pour ce cas, un message supprimé est transmis dans la simulation et le premier des deux messages est enlevé de la liste d'attente. Le message qui est transmis a une longueur de 0 bit et un modificateur de X.

La deuxième situation est lors de la sélection des messages pour les calculs des impacts. Nous utilisons les dix derniers messages d'un PGN pour calculer les impacts, par contre, des délais de transmission pourraient exister. Il existe une possibilité que ces dix messages soient reçus sur une grande période de temps; par exemple, un PGN envoyé à un intervalle anticipé de 100 ms qui reçoit son dixième message 2 secondes plus tard. Dans ces cas, ce dernier message peut engendrer des résultats aberrants. Pour corriger cette situation, une plage de temps maximal est calculée entre le premier et dernier message d'une suite. Cette plage de temps vaut 20 fois l'intervalle du message, qui équivaut au double du temps dans lequel les messages sont attendus pour deux itérations.

La troisième situation est lors du calcul des impacts. Les messages supprimés sont inclus dans les dix derniers messages reçus. Il se peut que beaucoup de messages supprimés existent et qu'il y ait trop de modificateurs X lors des calculs d'impacts. Le calcul des impacts, qui utilise la séquence des modificateurs, peut devenir aberrant. Pour corriger cette situation, chaque impact va spécifier s'ils acceptent les modificateurs X dans leur calcul.

3.4.2 Représentation chronologique

La représentation chronologique est utilisée pour représenter le changement du système (ou les impacts sur celui-ci) en fonction du temps. Ceci est accompli à l'aide de graphiques qui représentent chacun un impact. Les graphiques sont séparés en trois parties qui sont dédiées respectivement à l'état initial, à l'attaque et à la réponse. Ces parties, qui s'étendent chacune sur deux secondes, sont utilisées pour représenter les types de la matrice de confusion. De plus, cet intervalle de deux secondes va permettre au système de se stabiliser.

L'intervalle de deux secondes permet à la simulation d'accomplir au moins deux itérations des impacts pour chacune des trois parties. Ce calcul est l'intervalle maximal multiplié par le nombre de messages par itération, puis multiplié par le nombre d'itérations. L'intervalle le plus grand entre les messages d'un PGN est de 100 ms, signifiant dix messages par seconde. Les impacts de chaque itération sont calculés en utilisant les dix derniers messages reçus. Il y a deux itérations; la première pour les impacts et la deuxième pour les effets secondaires.

De 0 à 2 secondes, la simulation se stabilise à l'état initial du système, le VN est représenté. À 2 secondes, la simulation ajoute l'attaque. Entre 2 et 4 secondes, si une attaque a été ajoutée, le FN est représenté; aucune attaque n'a été ajoutée, le VN est représenté de nouveau. À 4 secondes, la simulation ajoute la réponse. Entre 4 et 6 secondes, si une attaque et une réponse ont été ajoutées, le VP est représenté; seulement une réponse a été ajoutée, le FP est représenté.

Un exemple de cette représentation chronologique est montré dans la figure 3.8. Chaque rangée représente un impact identifié à l'aide de son titre. Le titre comprend un identifiant, une description du profil, le MCE impacté (entre parenthèses), le PGN reçu et le modificateur associé. Les identifiants sont les lettres utilisées pour référencer les rangées lors des explications.

L'axe des ordonnées signifie le niveau de détection d'un profil et est normalisé entre les valeurs 0.0 et 1.0, avec un créneau d'incrémentation de 0.1. Dans les graphiques, l'ordonnée s'étale entre -0.1 et 1.1 afin de permettre une visualisation facile des différents niveaux de détection. Ceci a été une observation, où dans certains cas, il était très difficile à différencier la bordure et les valeurs, malgré le choix des couleurs. La ligne pointillée indique le niveau du seuil choisi de 0.7. Nous avons choisi ce seuil afin de pouvoir

progresser pour atteindre le but. Le seuil devrait être choisi en fonction de l'efficacité à l'IDS à pouvoir détecter le profil respectif. Suivant des essaies, lors de l'implémentation, nous avons conclu qu'un seuil de 0.7 est un bon point de départ, mais qu'une analyse en profondeur sur le seuil ferait partie d'un futur travail. Dans ce mémoire, un seuil de 0.7 indique que, pour un profil, ses dix derniers PGN ont au moins 70% de similarité.

L'abscisse représente le temps en secondes. Aux temps 2.0s et 4.0s, il y a une transition entre le système initial, l'attaque, et la réponse. Chaque point dans un profil représente le résultat du calcul de l'impact qui utilise les dix derniers messages reçus du PGN identifié. Dans certains cas, il peut y avoir des régions où aucune valeur n'est représentée, car aucun des messages n'a été envoyé sur le bus. La ligne pointillée représente le seuil de détection de 0.7 (ou 70%).

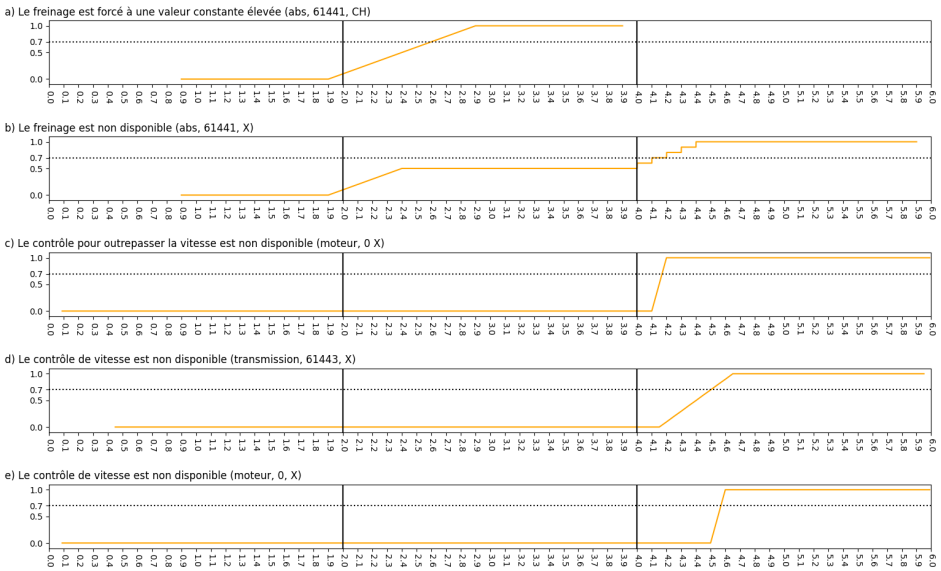

Figure 3.8: **Représentation chronologique**.

Dans ce chapitre, nous avons présenté la solution qui inclut les composantes du système, les méthodes pour calculer les impacts, ainsi que les choix de conceptions utilisés. La solution est représentée sous forme d'une simulation et quatre scénarios ont été établis. Les résultats des simulations de ces scénarios seront présentés dans le chapitre suivant.

4 Résultats

Les résultats des deux cas d'utilisation précédemment identifiés aux sections 3.3.1 et 3.3.2 sont présentés. Pour le premier cas d'utilisation, nous allons discuter deux scénarios selon la présence d'une attaque pour déterminer l'impact pour chaque état de la matrice de confusion. Pour le deuxième cas d'utilisation, nous allons simuler deux réponses similaires pour la même attaque, puis comparer les impacts résultants. La relation entre les cas d'utilisation et les scénarios que nous avons abordés au chapitre 3 est capturé à la table 4.1.

Cas d'utilisation 1 - Impact d'une attaque et d'une réponse → Scénario 1 - Attaque présente → Scénario 2 - Pas d'attaque
Cas d'utilisation 2 - Impact de réponses différentes à une attaque → Réponse 1 - Entrelacé → Réponse 2 - Subséquent

Table 4.1: **Relation hiérarchique**.

4.1 Cas d'utilisation 1 - Impact d'une attaque et d'une réponse

L'objectif du premier cas d'utilisation est de confirmer que le modèle peut considérer les attaques et les réponses pour déterminer l'impact résultant. Pour ce faire, nous allons déterminer l'impact pour chaque état de la matrice de confusion, puis les comparer aux impacts anticipés. Le premier scénario, dont la séquence de messages est représentée à la table 3.7(a), est la présence d'une

attaque et celle d'une réponse. La situation est celle d'un appareil malveillant qui usurpe le PGN 61441 pour lui donner une valeur élevée constante afin d'affecter la valeur de sortie du contrôle du freinage. L'appareil malveillant interrompe le message original du PGN 61441, puis transmet un nouveau message avec le même PGN où le contrôle (valeur de sortie) possède le modificateur CH. En réponse, l'IPS interrompe le message usurpé que l'appareil malveillant a transmis. Le deuxième scénario, dont la séquence de messages est représentée à la table 3.7(b), est la présence d'une réponse uniquement, sans attaque associée. L'IDS fait une mauvaise identification d'une attaque et l'IPS interrompe le message original du PGN 61441 identifié comme étant malveillant.

À la figure 4.1, nous avons simplifié l'architecture d'interrelations initialement présentée à de la figure 3.3 afin de l'adapter à ce cas d'utilisation. À gauche, nous voyons le MCE du moteur qui est connecté à la pédale de freinages. Ce MCE transmet le PGN 61441 qui contient deux type de contrôle différents. Le premier est la valeur de sortie qui est reçu par le MCE de l'ABS pour effectuer le freinage. Le deuxième contrôle est une retransmission de la valeur d'entrée reçue vers le MCE de la transmission pour outrepasser (dans le sens du terme anglais *override*) la vitesse lorsque la pédale du freinage est utilisée. Le MCE de la transmission transmet le PGN 0 qui contient de l'information spécifique pour outrepasser la vitesse en cas de freinage. Le MCE du moteur effectue un changement de vitesse lorsque ce PGN 0 est reçu. À partir de ce point-ci, le MCE du moteur va tenir compte de la pédale d'accélération pour effectuer la vitesse. Le MCE du moteur transmet le PGN 61443 au MCE de la transmission pour le contrôle de vitesse. Puis, le MCE de la transmission transmet le PGN 0 au MCE du moteur pour le contrôle de vitesse.

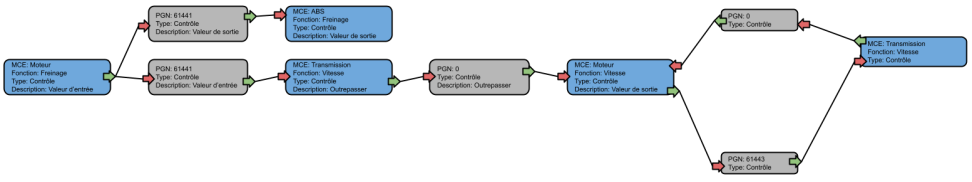

Figure 4.1: **L'architecture d'interrelations pour le premier cas d'utilisation**.

Les profils choisis pour représenter les scénarios ne sont qu'un sous-ensemble des profils disponibles. Nous avons sélectionné cinq profils parce qu'ils représentent le mieux, selon nous, l'attaque et la réponse. Les profils choisis sont les

mêmes pour les deux scénarios du premier cas d'utilisation et ils sont discutés aux figures 4.3 à 4.6. Pour chaque profil, l'impact associé existe sur le véhicule si la valeur dépasse le seuil. L'impact du profil a) est un freinage forcé à une valeur constante élevée. Ce profil représente l'information de contrôle que l'ABS reçoit du PGN 61441. La valeur est anormalement constante et élevée et le freinage agit ainsi. Les profils b) à e) évaluent le taux de messages qui ont un modificateur X parmi les dix derniers messages du même PGN. Le modificateur X représente un message qui n'a pas été transmis sur le réseau, mais qui aurait dû l'être. Dans ce mémoire, ce modificateur est associé à la suppression intentionnelle par l'IPS ou l'appareil malveillant, ou à un effet secondaire d'un impact. La disponibilité d'un PGN peut affecter certaine fonctionnalité si le PGN contient de l'information de contrôle utilisé par le MCE qui reçoit le message. Donc en sachant qu'un PGN n'est pas transmis sur le bus, nous pouvons déduire que la fonctionnalité associée ne serait pas possible. L'impact du profil b) est un freinage non disponible puisque le PGN 61441 est supprimé. L'impact du profil c) est un contrôle non disponible pour outrepasser la vitesse puisque le PGN 0 est supprimé. L'impact du profil d) est un contrôle de vitesse non disponible puisque le PGN 61443 est supprimé. L'impact du profil e) est un contrôle de vitesse non disponible puisque le PGN 0 est supprimé.

Dans la section 2.2, nous avons définit la classe réelle et la classe estimée. Ces classes représentent les différents états de la matrice de confusion (voir figure 2.5) qui sont utilisés dans le premier cas d'utilisation. Nous faisons une mise à jour de la matrice de confusion dans notre contexte spécifique à la figure 4.2. Nous avons précisé la classe estimée pour inclure ce que l'IDS identifie et nous avons ajouté les deux scénarios à la classe réelle. Le premier scénario est la présence d'une attaque, et le deuxième scénario ne contient pas d'attaque. À partir de cet ajout à la figure, nous pouvons observer que le premier scénario contient le VP et le FN, tandis que le deuxième scénario contient le FP et le VN. Finalement, nous avons associé les résultats de chaque état de la matrice de confusion à la section où nous discuterons des résultats respectifs.

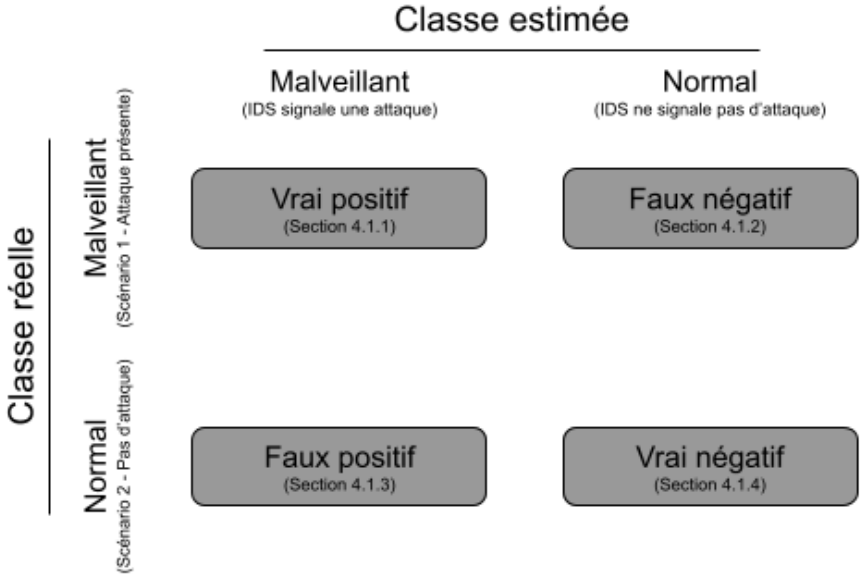

Figure 4.2: **La matrice de confusion - mise à jour**.

4.1.1 Vrai positif

Du Scénario 1 - *Attaque présente*, le VP est un système qui est affecté par l'attaque et la réponse. Cet état est représenté dans la figure 4.3 entre les temps 4.0s et 6.0s. Nous rappelons que l'état initial se passe entre 0.0s et 2.0s, et le FN entre 2.0s et 4.0s. Nous anticipons que le freinage ne sera plus possible.

Les profils de b) à e) dépasseront le seuil et ceci signifiera que le contrôle de vitesse n'est pas disponible. Au temps de 4.0s, la valeur du profil a) disparaît. Ceci est causé par les calculs des profils qui sont effectués lorsqu'un message est transmis. Dans ce scénario, le PGN 61441 est complètement supprimé par l'IPS, donc ce calcul n'est jamais effectué. Pour le profil a), ceci se traduit à avoir aucun impact. Pour les profils de b) à e), un effet cascade est représenté. Dans le profil b), le seuil est atteint au temps de 4.1s. Ceci signifie que le freinage n'est pas disponible, parce que le PGN 61441 est supprimé par l'IPS. Lorsque les impacts sont calculés, la table 3.6 est utilisée pour déterminer les effets secondaires. Dans cette situation, la transmission cesse de recevoir le PGN 61441, puis cesse de transmettre le PGN 0. En utilisant l'architecture d'interrelations de la figure 4.1, nous pouvons commencer à anticiper les effets secondaires suivant la réponse de l'IPS. Dans le profil c), au temps de 4.1s nous pouvons remarquer un changement de valeur, puis un seuil qui est dépassé un peut avant le temps 4.2s. Dans cet effet de cascade,

le profil d) voit sa valeur augmenter près du temps 4.2s et dépasse le seuil au temps 4.5s. Le profil e) voit sa valeur augmenter au temps 4.5s et dépasse le seuil près du temps 4.6s. La réponse de supprimer le PGN 61441 a aussi pour effet d'impacter le contrôle pour outrepasser la vitesse, puis celui de la vitesse directement.

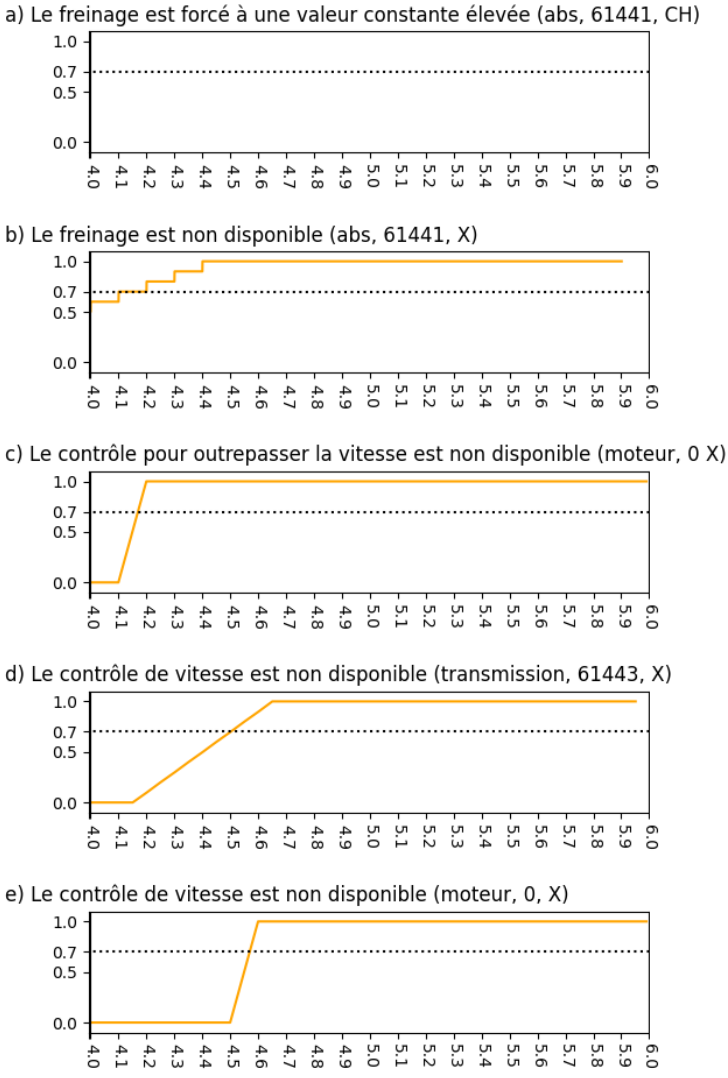

Figure 4.3: **Vrai positif**.

Les profils c) et e) représentent la disponibilité du contrôle de vitesse et l'outrepassage de celle-ci. Ils ont le même PGN 0, par contre leur disponibilité n'est pas affectée au même moment. Ceci est causé par la source qui affecte le PGN. Si l'appareil malveillant ou l'IPS supprime un PGN directement, tous ces PGN sont supprimés. Lorsqu'un PGN est affecté par l'impact d'un profil, il est unique. Ceci est une limitation de la simulation où chaque combinaison du PGN, du type et de la description est unique.

Nous avions anticipé que le freinage ne serait plus possible et ceci est supporté par l'absence de données du profile a). Les profiles b) à e) indiquent que le contrôle de vitesse est aussi affecté. L'interprétation de cette information est que la pédale du freinage n'a plus d'effet sur le contrôle de vitesse. Par exemple, si l'utilisateur utilise la pédale de freinage, la vitesse du véhicule sera inchangée et ne se synchronisera pas à la réduction de vitesse demandée.

4.1.2 Faux négatif

Toujours du Scénario 1 - *Attaque présente*, le FN représente un système qui est uniquement affecté par l'attaque; aucune réponse n'est émise car l'attaque n'est pas détecté (classe estimée). Cet état est représenté dans la figure 4.4 entre les temps 2.0s et 4.0s. Nous anticipions que le profil a) serait le seul à dépasser le seuil, et qu'il n'y aura pas d'effet secondaire suite à l'attaque. Au temps de 2.0s, la valeur du profil a) commence à s'accroître, et le seuil est dépassé au temps de 2.6s. Ceci indique que le freinage est forcé à une valeur constante élevée. La valeur du profil b) s'accroît, par contre, elle se stabilise près du milieu. Dans ce scénario, pendant la période de l'attaque, la moitié des messages sont supprimés et l'autre contient le modificateur CH. Pour les profils de c) à e), leur valeur ne change pas puisque leur PGN respectif n'est pas affecté ou supprimé.

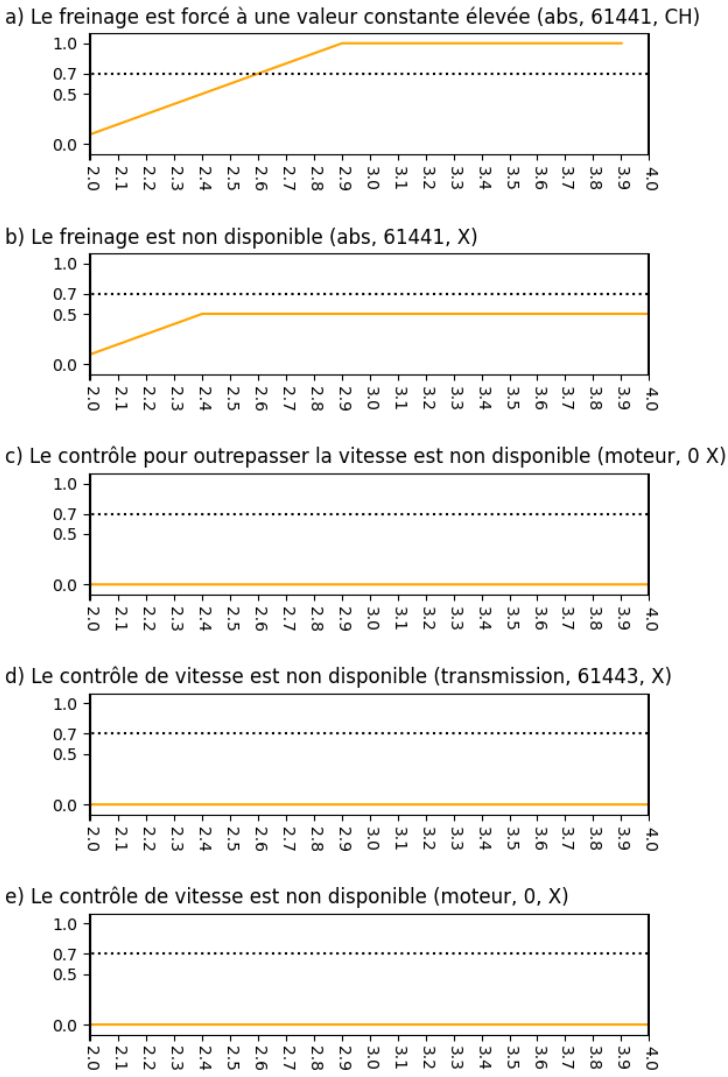

Figure 4.4: **Faux négatif**.

Tel qu'anticipé, seulement le profile a) est affecté; la valeur de sortie pour l'ABS. Aucun effet secondaire en lien avec la vitesse n'est ressenti sur le reste du système. Dans la table 3.3 et dans la figure 4.1, le PGN 61441 communique avec deux destinations différentes qui sont l'ABS et le moteur. Dans le modèle que nous avons développé, nous avons séparé le contenu des messages en utilisant une fonction et une description additionnelle. Dans le PGN 61441, le

contrôle possède deux contenus. Le premier est une valeur de sortie qui affecte l'ABS et le second une valeur d'entrée qui affecte la transmission. L'appareil malveillant de ce scénario a seulement changé la valeur de sortie. Ceci insinue que cet appareil à récolter tout le contenu du PGN 61441, puis a seulement changé la partie du contenue qui affecte l'ABS. Le véhicule voit son freinage actionné sans que le contrôle de vitesse s'adapte à ce changement, et cet impact n'est pas reflété dans la simulation. Ceci est une limite de la simulation qui détermine seulement les impacts en fonction de ce qui est échangé sur le réseau.

4.1.3 Faux positif

Du Scénario 2 - *Pas d'attaque*, le FP représente un système qui est uniquement affecté par la réponse, puisque l'IDS a détecté une attaque par erreur. Cet état est représenté à la figure 4.5 entre les temps 4.0s et 6.0s. Nous anticipons que l'impact résultant sera le même que pour le VP, discuté à la section 4.1.1. Au temps 4.0s, la valeur du profil a) disparaît. Ceci est causé par le fait que les calculs des profils sont effectués lorsqu'un message est transmis. Dans ce scénario, le PGN 61441 est complètement supprimé par l'IPS, donc ce calcul n'est jamais effectué. Pour les profils de b) à e), un effet cascade est représenté. Dans le profil b), le seuil est atteint au temps de 4.6s. Ceci signifie que le freinage n'est pas disponible, parce que le PGN 61441 est supprimé par l'IPS. Lorsque les impacts sont calculés, la table 3.6 est utilisée pour déterminer les effets secondaires. Dans cette situation, la transmission cesse de recevoir le PGN 61441, puis cesse de transmettre le PGN 0. En utilisant l'architecture d'interrelations de la figure 4.1, nous pouvons commencer à anticiper les effets secondaires suivant la réponse de l'IPS. Dans le profil c), au temps de 4.6s nous pouvons remarquer un changement de valeur, puis un seuil qui est dépassé un peut avant le temps 4.7s. Dans cet effet de cascade, le profil d) voit sa valeur augmenter près du temps 4.7s et dépasse le seuil au temps 5.0s. Le profil e) voit sa valeur augmenter au temps 5.0s et dépasse le seuil près du temps 5.1s. Suivant la réponse de supprimer le PGN 61441, ceci aussi pour effet d'impacter le contrôle pour outrepasser la vitesse, puis celui de la vitesse directement.

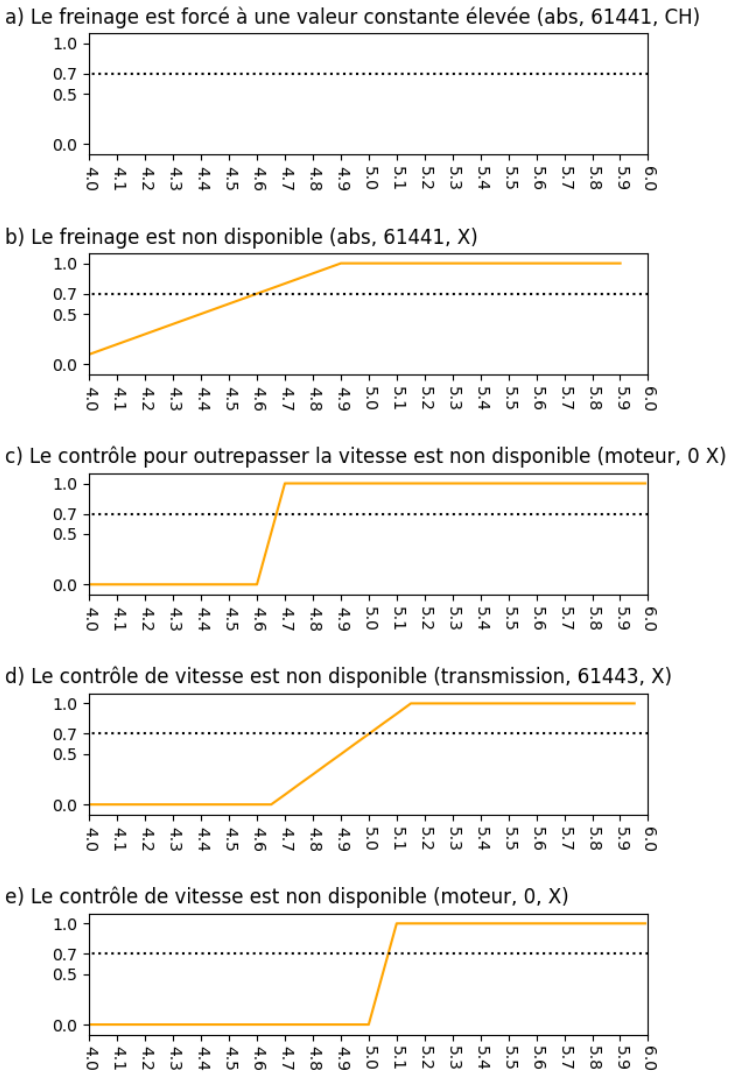

Figure 4.5: **Faux positif**.

Tel qu'anticipé, l'impact est le même que celui du VP. La différence principale est que les impacts sont décalés de 0.5s.

4.1.4 Vrai négatif

Finalement, du Scénario 2 - *Pas d'attaque*, le VN représente un système qui n'est pas affecté par une attaque ni par une réponse. Cet état est représenté dans la figure 4.6 entre les temps 2.0s et 4.0s. Nous anticipions qu'aucun impact sera observé. Le système simulé ne contient aucun impact tel qu'anticipé. Pour un véhicule, ceci indique que la configuration du système est stable. Les valeurs des profils commencent à s'afficher lorsque dix messages sont transmis. L'intervalle de transmission est inscrit dans la table 3.7 pour chacun des scénarios. Les profils a) et b) suivent le PGN 61441 avec un intervalle de 100 ms. Le dixième message de ce PGN est transmis au temps de 0.9 seconde. La même logique est utilisée pour les profils c) et e) où l'intervalle du PGN 0 est de 10 ms, et pour le profil d) où l'intervalle du PGN 61443 est de 50 ms.

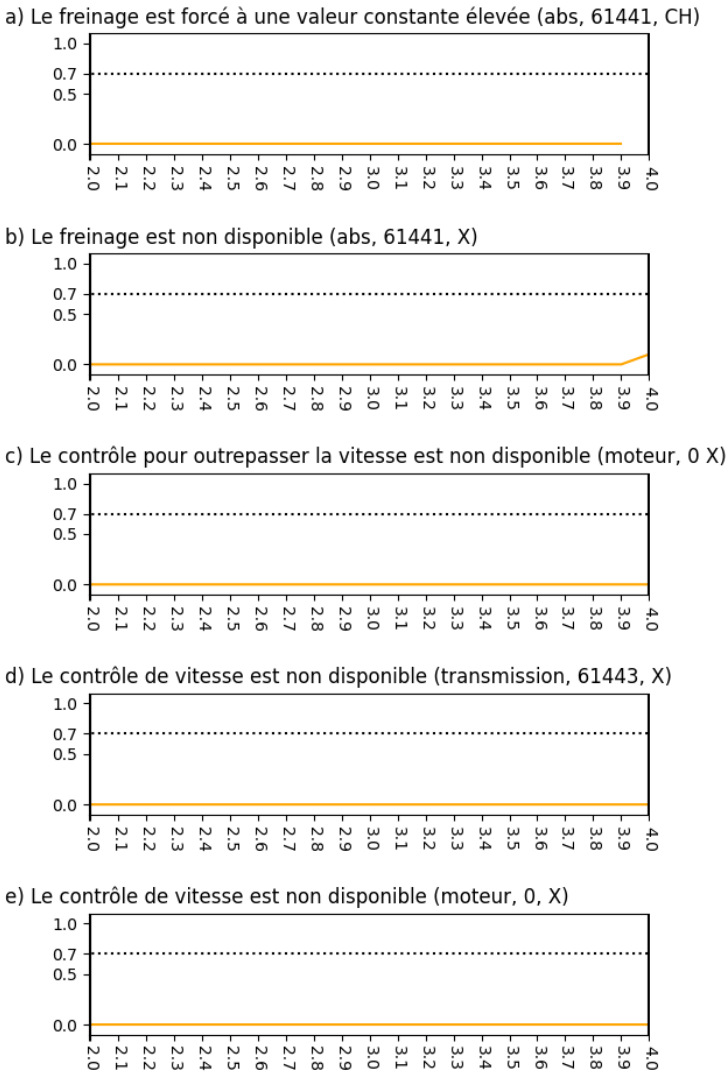

Figure 4.6: **Vrai négatif**.

4.1.5 Sommaire du Cas d'utilisation 1

Nous avions anticipé les impacts résultants pour la majorité des états de la matrice de confusion. Les exceptions sont reliés à la limitation de la simulation, tel que pour le FN où le véhicule voit son freinage actionné sans que le contrôle de vitesse s'adapte à ce changement. Dans ce cas, le conflit de contrôle entre le

freinage et la vitesse pourrait créer un impact physique qui n'est pas représenté dans le réseau. Nous avions anticipé que le VP et FP aient le même impact, par contre il y a un décalage de 0.5s.

4.2 Cas d'utilisation 2 - Impact de réponses différentes à une attaque

L'objectif du deuxième cas d'utilisation est d'évaluer si le modèle peut déterminer des impacts résultants différents pour des situations similaires. Pour récapituler, la situation illustrant ceci est un appareil malveillant qui essaie de contrôler ou de noyer le PGN 0 en envoyant trois messages additionnels à la suite du message original. Ces messages auront le modificateur CH en but de forcer une augmentation de vitesse. L'IPS réagit en envoyant trois autres messages pour tenter de contrer les effets des messages malveillants. Ces messages auront le modificateur CL en but de contrer cette augmentation de vitesse en forçant une vitesse basse. Nous implémentons deux réponses à l'attaque qui vont chacune transmettre leurs trois messages. La Réponse 1 - *Entrelacé* va entrelacer ces messages parmis ceux qui sont malveillants. La Réponse 2 - *Subséquent* va transmettre ces messages après les messages malvaillants. Les scénarios sont représentés dans la table 3.8.

Nous simplifions l'architecture d'interrelations de la figure 3.3 à la figure 4.7 afin de l'adapter à ce cas d'utilisation. Le MCE du moteur va tenir compte de la pédale d'accélération pour signifier la vitesse. Le MCE du moteur transmet le PGN 61443 au MCE de la transmission pour le contrôle de vitesse. Puis, le MCE de la transmission transmet le PGN 0 au MCE du moteur pour le contrôle de vitesse.

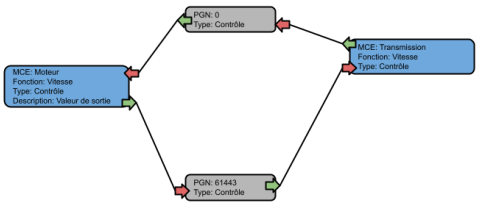

Figure 4.7: **L'architecture d'interrelations pour le deuxième cas d'utilisation**.

Les profils illustrés ne sont qu'un sous-ensemble des profils disponibles. Nous avons sélectionné ces six profils parce qu'ils représentent le mieux, selon nous,

l'attaque et la réponse. Les profils choisis sont les mêmes pour les deux scénarios du Cas d'utilisation 2. Pour chaque profil, l'impact associé existe sur le véhicule si la valeur dépasse le seuil. L'impact du profil a) et b) est une vitesse forcée à une valeur constante faible. Ces profils représentent l'information de contrôle que le moteur ou la transmission reçoivent des PGN 0 et 61443 respectivement. L'impact du profil c) et d) est une vitesse forcée à une valeur constante élevée. Ces profils représentent l'information de contrôle que le moteur ou la transmission reçoivent des PGN 0 et 61443 respectivement. L'impact du profil e) est une réduction de temps de mise à jour pour la vitesse. Ce profil représente une valeur constante ou inchangée comparativement à sa valeur précédente. Ceci peut aussi être utilisé pour déterminer l'impact d'une attaque par rejeu. L'impact du profil f) est l'augmentation dangereuse de stress physique du moteur. Ce profil représente une fluctuation entre des valeurs basses et élevées.

4.2.1 Attaque

L'attaque est représenté à la figure 4.8. Au temps de 2.0s, l'attaque est ajoutée. Lorsque l'attaque est en cours, les valeurs de tous les profils commencent a changer. Le profil b) se stabilise au temps 2.45 et le profil f) se stabilise immédiatement après le temps 2.0s. Au temps de 2.0s, les profils a), c) et e) sont directement affectés par l'attaque sur le PGN 0 et se stabilise au temps 2.35. Au temps de 2.35, le profil d) dépasse le seuil qui a pour effet de modifier les profils a), c) et e). Tous les profils se stabilisent après ce temps. Avec la représentation chronologique des profils, une période de transition est observée au temps de 2.35 où le système essaie de se stabiliser lorsqu'un changement est appliqué sur le système. Durant cette période de transition, un impact est temporairement détecté pour le profile e). Cet impact temporaire, qui n'est pas présent à la fin de la période de temps, devra être inclue lorsque nous discutons de l'impact de l'attaque. Le terme *impact résultant* sera utilisé pour inclure tous les impacts détectés durant la totalité du temps tel que les impacts temporaires. Le terme *impact final* sera utilisé pour spécifier l'impact présent à la fin de la simulation.

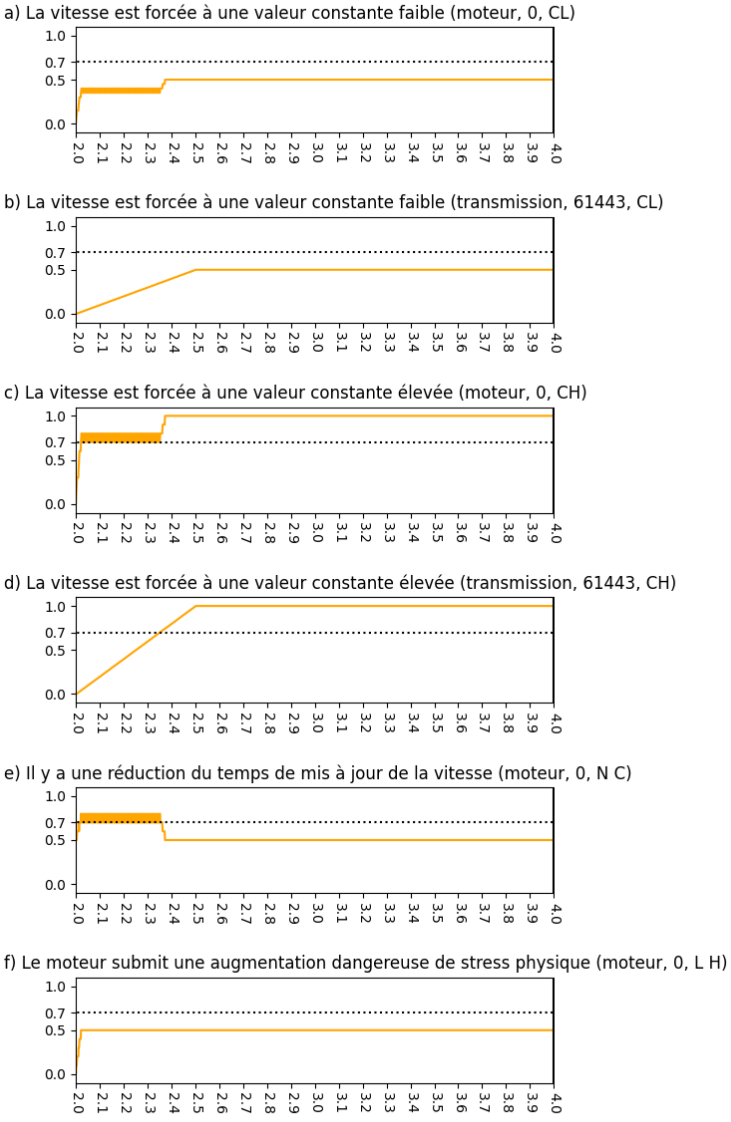

Figure 4.8: **Attaque**.

4.2.2 Réponses

Les Réponse 1 - *Entrelacé* et Réponse 2 - *Subséquent*, sont représentés aux figures 4.9 et 4.11 respectivement.

La Réponse 1 - *Entrelacé* représente un IPS qui transmet un message CL directement après l'injection du message malveillant CH. L'intention est de contrer la valeur élevée par une valeur basse. La première réponse est observée au temps de 4.0s. Les profils b), d) et e) restent inchangés. Le profil a) voit sa valeur augmenter, puis dépasse ainsi le seuil. Le profil c) voit sa valeur diminuer, mais il reste au-dessus du seuil. Les bornes de la fluctuation de données observées pour les profils a) et c) sont au-dessus du seuil, donc l'impact est continuellement présent. Au temps de 4.0s, le profil f) dépasse le seuil soudainement, puis redescend ensuite. La valeur fluctue entre le 0.5 et 0.7, qui est assez pour atteindre le seuil de manière récurrente, mais pas continuellement. L'impact résultant de la première réponse est la vitesse forcée à une valeur constante faible a) et constante élevée c), ainsi que l'augmentation dangereuse de stress physique du moteur.

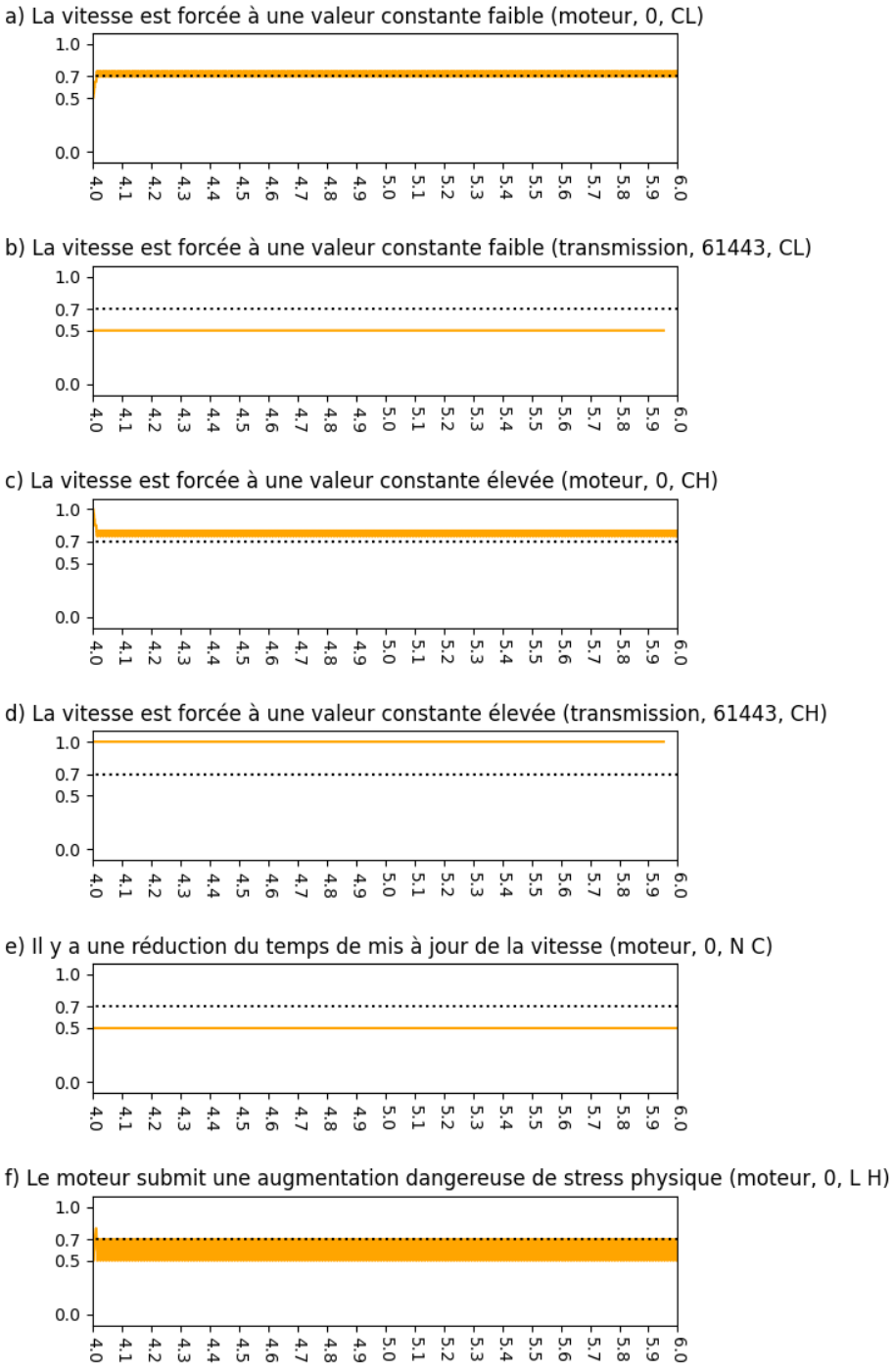

Figure 4.9: **Réponse 1 - *Entrelacé***.

Les profils a) et c) devraient avoir des valeurs opposées parce qu'une valeur basse et élevée ne devraient pas exister pour le même PGN. Cette situation est une limitation du calcul des impacts. Les impacts sont calculés en comparant les modificateurs des dix derniers messages transmis avec le profile d'entrée. Un exemple du calcul est représenté à la figure 4.10. Le calcul est une convolution matricielle entre les dix derniers modificateurs et l'entrée des données pour un profile choisi. Dans la partie du bas à gauche, nous calculons la convolution entre l'entrée des données du profile a) contre lui-même pour déterminer sa valeur maximale de 20. Dans la partie du haut à gauche, nous calculons la convolution entre l'entrée des données du profile a) contre les dix derniers modificateurs. Ces derniers sont cinq CL entrelacé avec cinq CH (estimation) dont la valeur la plus élevé est 15. Le ratio de 15/20 ou 0.75 atteint le seuil de 0.7. Lorsque le calcul est effectué pour le profile c), nous obtenons aussi une valeur de 0.75. La méthode de calcul utilisé est une limitation, car dans ce cas, nous identifions deux impacts qui devraient être opposés.

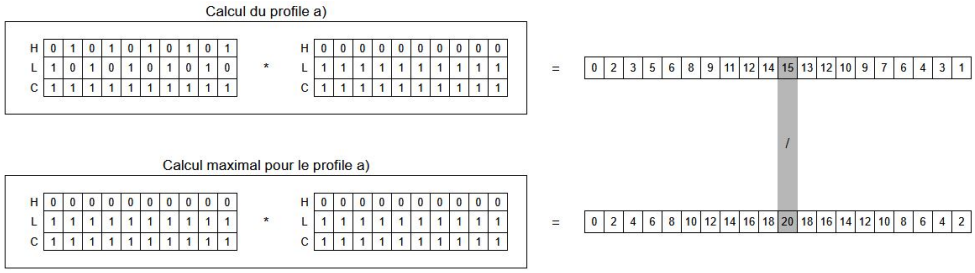

Figure 4.10: **Caclul du profile a)**.

Les profils de la Réponse 2 - *Subséquent* sont représentés à la figure 4.11. Cette réponse est associé avec un IPS qui transmet trois messages CL après l'injection des trois messages malveillants CH. L'intention est de contrer la valeur élevée par une valeur basse. Au temps de 4.0s, la première réponse est ajoutée. Les profils b), d) et e) restent inchangés. Le profil a) voit sa valeur augmenter, puis sa valeur commence à fluctuer de chaque côté du seuil. L'impact est intermittent. Le profil c) voit sa valeur diminuer, mais il reste au-dessus du seuil. Pour ce profil, les bornes de la fluctuation de données observées se passent au-dessus du seuil, donc l'impact est continuellement présent. Au temps de 4.0s, le profil f) commence à fluctuer, mais le seuil n'est jamais dépassé. L'impact résultant de la Réponse 2 - *Subséquent* est la vitesse

forcée à une valeur constante faible intermittente et à une valeur constante élevée continuellement. Ceci est la même situation qu'avec la Réponse 1 - *Entrelacé* pour les profiles a) et c).

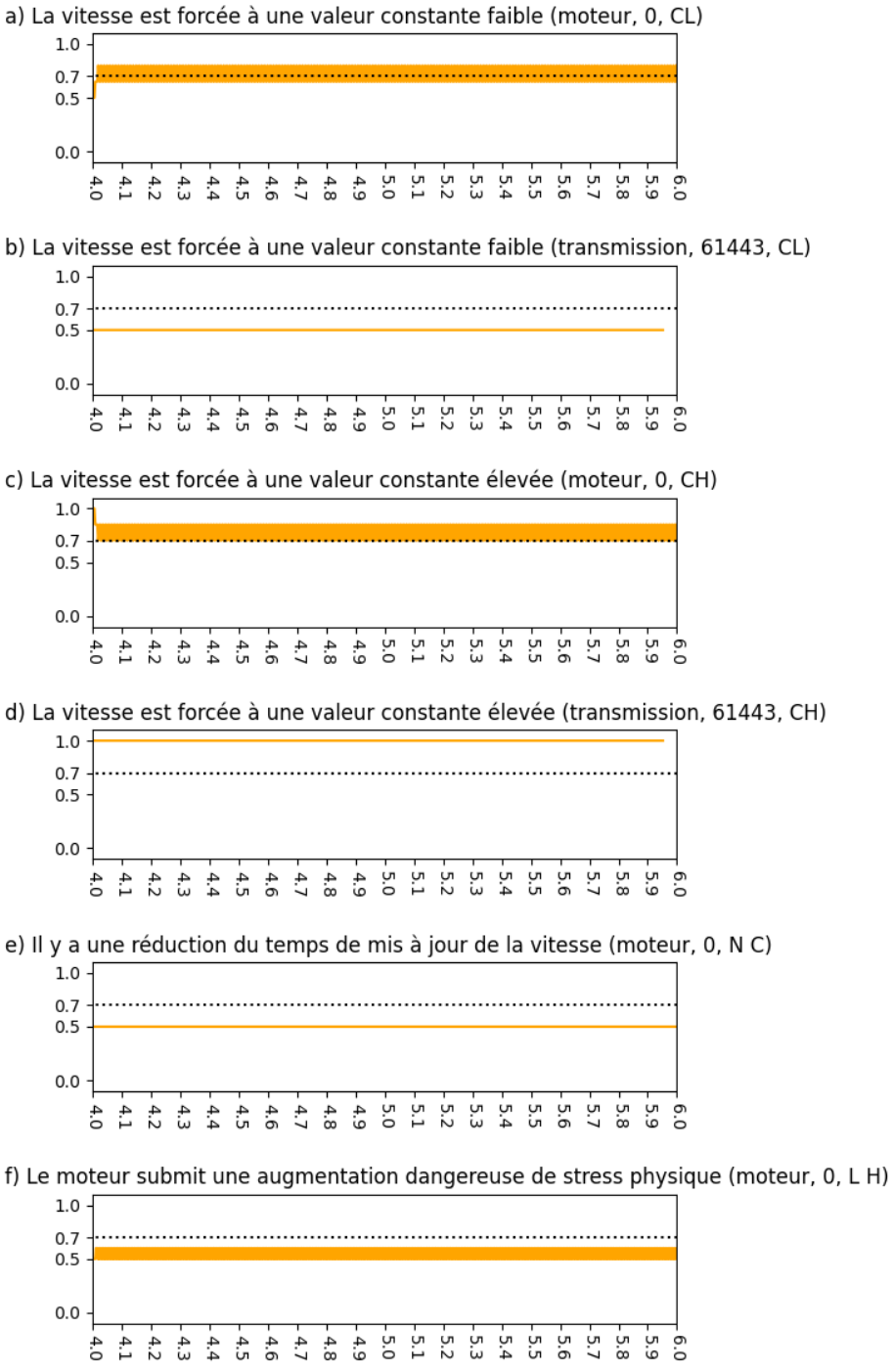

Figure 4.11: **Réponse 2 - *Subséquent***.

4.2.3 Comparaison

Nous allons comparer les deux réponses qui sont représentées aux figures 4.9 et 4.11. Pour le profil a), la différence principale est que la Réponse 2 - *Subséquent* n'atteint pas le seuil continuellement. L'impact associé à ce profil fluctue constamment, tandis que l'impact de la Réponse 1 - *Entrelacé* est continuel. Pour le profil b), les deux réponses ont la même valeur qui ne dépasse pas le seuil. Pour le profil c), les deux réponses dépassent le seuil continuellement bien que la fluctuation de la Réponse 2 - *Subséquent* est plus grande. Pour le profil d), les deux réponses ont la même valeur qui dépasse le seuil. Pour le profil e), les deux réponses ont la même valeur qui ne dépasse pas le seuil. Pour le profil f), la fluctuation de la Réponse 1 - *Entrelacé* est plus étendue et atteint la limite du seuil, et la Réponse 2 - *Subséquent* fluctue sous le seuil.

La table 4.2 contient le bilan des impacts indiquant si le seuil est atteint continuellement ou de façon intermittente. Les profils b) à e) sont identiques et les profils a) et f) sont différents en termes d'impact résultant. Les deux réponses implémentées similairement possèdent un impact résultant différent ainsi que pour l'impact final. La différence majeure est le profil f) où la Réponse 1 - *Entrelacé* force un stress physique au système en entrelaçant des messages à valeur basse avec des messages à valeur élevée.

profil	Réponse 1 - *Entrelacé*	Réponse 2 - *Subséquent*
a)	continuel	intermittent
b)	-	-
c)	continuel	continuel
d)	continuel	continuel
e)	-	-
f)	intermittant	-

Table 4.2: **Bilan des impacts**.

5 Conclusion

Pour récapituler, le but de cette recherche est de concevoir un modèle afin de considérer les impacts des attaques et des réponses à celles-ci sur un réseau SAE J1939. Pour ce faire, nous avons développé un modèle, basé sur la simulation, pour déterminer l'impact d'une attaque survenue sur un réseau véhiculaire SAE J1939 ainsi que celui d'une réponse à cette attaque. Nous avons présenté deux cas d'utilisation afin de soutenir le but.

Le Cas d'utilisation 1 - *Impact d'une attaque et d'une réponse* est utilisé pour explorer l'implémentation du modèle que nous avons présenté à la section 4.1. Son objectif est de confirmer que le modèle peut considérer les attaques et les réponses pour déterminer l'impact résultant. Nous avons déterminé l'impact résultant pour chaque état de la matrice de confusion, puis nous les avons comparés aux impacts anticipés. Nous avions anticipé les impacts résultants pour la majorité des états de la matrice de confusion. Une des limitations identifiées est que l'impact résultant ne considère pas le conflit de contrôle pour deux fonctions qui sont reliées. Ici, nous faisons références au FN à la section 4.1.2 où le freinage est activé sans que le contrôle de la vitesse s'adapte au changement.

Le Cas d'utilisation 2 - *Impact de réponses différentes à une attaque* est utilisé pour explorer la sensibilité de l'implémentation du modèle que nous avons présenté à la section 4.2. Son objectif est d'évaluer si le modèle peut déterminer des impacts résultants différents pour des situations similaires. Nous avons simulé deux réponses similaires pour la même attaque, puis nous avons comparé les impacts résultants. La différence majeure sur l'impact résultant est la présence d'un stress physique pour la Réponse 1 - *Entrelacé*.

5.1 Travaux futurs

Au cours du mémoire, nous avons fait quelques observations qui pourront être utilisées afin d'approfondir le travail.

1. L'architecture du système pourrait accroître afin d'inclure la totalité des messages PGN. Dans ce mémoire, une fraction des messages ont été utilisés, et l'ajout des messages pouvant être manipulés par l'appareil malveillant ou l'IPS pourrait impacter la bande passante qui, à son tour, peut affecter la disponibilité. De plus, les fonctions et le contenu des messages pourraient être décrits à un niveau plus détaillé. Ce niveau de détail permettra d'inclure une plus grande gamme d'impact et d'effet secondaire.
2. La méthode pour calculer les impacts pourrait être améliorée. L'amélioration pourrait être au niveau du nombre de messages utilisés pour déterminer l'impact ou au niveau de l'implémentation des calculs des impacts. L'utilisation des dix derniers messages pour déterminer l'impact a permis d'explorer un changement graduel où tous les profils ont fini par se stabiliser. Le nombre de messages utilisé pourrait varier en fonction du système. Nous anticipons des résultats plus volatils avec un nombre inférieur de messages. De plus, le calcul des impacts avait des limites. Un exemple est le calcul des impacts pour les profils du Cas d'utilisation 2 - *Impact de réponses différentes à une attaque* où les valeurs des CL et CH étaient similaires lorsqu'elles devraient avoir une plus grande différence.
3. La simulation du réseau pourrait être améliorée en se rapprochant le plus possible à un vrai bus. Ceci inclut la transmission des messages par des MCE en parallèle et indépendants des autres, puis la simulation du bus pour chaque bit transmis. Une autre serait l'implémentation des erreurs et de leurs compteurs respectifs. Ceci permettrait d'examiner le comportement du réseau lorsque des messages sont supprimés, et ceci pourrait avoir des répercussions au niveau de la disponibilité. La gestion des erreurs peut aussi affecter la longueur d'un message transmis qui dépend de l'implémentation de la suppression du message.

Pour conclure, le modèle que nous avons présenté nous a permis d'approfondir nos connaissances vis-à-vis la considération d'attaques et de réponses pour obtenir des observations sur l'impact à un réseau SAE J1939.

Liste des ouvrages de référence

[1] "CAN high / CAN low." [Online]. Available: https://support.squarell.com/index.php?/Knowledgebase/Article/View/94/7/can-high--can-low

[2] R. Bosch GmbH, "CAN Specification version 2.0," *Postfach*, vol. 300240, 1991.

[3] "J1939 Protocol." [Online]. Available: https://www.typhoon-hil.com/documentation/typhoon-hil-software-manual/References/j1939_protocol.html#j1939_protocol___section_c4g_gzk_fpb

[4] "The OSI model explained: How to understand (and remember) the 7 layer network model." [Online]. Available: https://www.networkworld.com/

[5] "Serial Control and Communications Heavy Duty Vehicle Network - Top Level Document," 2013. [Online]. Available: http://standards.sae.org/j1939_201308

[6] C. S. S. Electronics, "J1939 Explained - A Simple Intro (2020)," May 2020, library Catalog: www.csselectronics.com. [Online]. Available: https://www.csselectronics.com/screen/page/simple-intro-j1939-explained/language/en

[7] C. Young, J. Zambreno, H. Olufowobi, and G. Bloom, "Survey of automotive controller area network intrusion detection systems," *IEEE Design & Test*, vol. 36, no. 6, pp. 48–55, 2019, publisher: IEEE.

[8] "National Institute of Standards and Technology (NIST) Cybersecurity Framework."

[9] S.-F. Lokman, A. T. Othman, and M.-H. Abu-Bakar, "Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review," *EURASIP Journal on Wireless Communications and*

Networking, vol. 2019, no. 1, p. 184, Jul. 2019, number: 1. [Online]. Available: https://doi.org/10.1186/s13638-019-1484-3

[10] S. Mukherjee, "SAE J1939-Specific Cyber Security for Medium and Heavy-Duty Vehicles," PhD Thesis, Colorado State University, 2023.

[11] "SAE J1939 Address Claim Procedure - SAE J1939/81 Network Management," Feb. 2017. [Online]. Available: https://copperhilltech.com/blog/sae-j1939-address-claim-procedure-sae-j193981-network-management/

[12] S. Abbott-McCune and L. A. Shay, "Intrusion prevention system of automotive network CAN bus," in *2016 IEEE International Carnahan Conference on Security Technology (ICCST)*, Oct. 2016, pp. 1–8, iSSN: 2153-0742.

[13] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," *black hat USA*, vol. 2014, p. 94, 2014.

[14] S. Anwar, J. Mohamad Zain, M. F. Zolkipli, Z. Inayat, S. Khan, B. Anthony, and V. Chang, "From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements, and Future Directions," *Algorithms*, vol. 10, no. 2, p. 39, Jun. 2017, number: 2 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/1999-4893/10/2/39

[15] K. Alsubhi, Y. Alhazmi, N. Bouabdallah, and R. Boutaba, "Rule Mode Selection in Intrusion Detection and Prevention Systems," in *2011 IEEE Global Telecommunications Conference - GLOBECOM 2011*, Dec. 2011, pp. 1–6, iSSN: 1930-529X.

[16] F. Bernier, "Banque de données SAE J1939 du Centre de recherche et développement pour la défense Canada (RDDC) Valcartier, QC."