Analyse et évaluation des risques liés à la mise à jour des logiciels de la voiture autonome

Celia Oukil, Pascal Krapf, Sébastien Berthier

Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Analyse et évaluation des risques liés à la mise à jour des logiciels de la voiture autonome

Analysis and risks assessment related to the updates of Autonomous car software

OUKIL Celia
Syscience
Villebon-Sur-Yvette, France
celia.oukil@syscience.fr

KRAPF Pascal
Syscience
Villebon-Sur-Yvette, France
pascal.krapf@syscience.fr

BERTHIER Sébastien
Syscience
Villebon-Sur-Yvette, France
sebastien.berthier@syscience.fr

Résumé **—** L'objectif de cette étude est d'identifier et d'analyser les conséquences en termes de risques liés au futur déploiement des véhicules automobiles autonomes VAA. Nous utiliserons pour cela une méthode d'identification, d'analyse, et d'évaluation des risques. Cette méthode est basée sur l'identification et l'étude des dommages potentiels infligés à tous les éléments de l'environnement. Nous montrerons que cette approche permet d'analyser les dommages que peut subir l'environnement au sens large. Nous montrerons aussi que les mises à jour logicielles sont une caractéristique indispensable pour le VAA. Ces mises à jour logicielles comportent des risques que l'on se doit d'étudier.

Mots-clefs — VAA, Risques, Mises à jour logicielles, Durabilité.

Abstract**—** The objective of this study is to identify and analyze the consequences in terms of risks related to the future deployment of autonomous automotive vehicles VAA. We will use a method of identification, analysis and risk assessment. This method is based on the identification and study of the potential damage that are inflicted to the elements of the environment. We will show that this approach makes possible to analyze the damage that the environment may suffer in a global context. We will also show that software updates are an essential feature for the VAA. These software updates carry risks that should be considered.

Keywords — AAV, Risks, Software updates, Durability.

I. Introduction

A. Un système innovant

La voiture autonome est un concept innovant qui fournira la possibilité de rouler sans l'intervention d'un conducteur.

Le concept d'un véhicule autonome au sens d'un automate embarquant sa propre motorisation, et programmable sur un parcours donné, est imaginé et mentionné pour la première fois par Léonard de Vinci au 15 ème siècle. Il présente ce chariot comme un système autonome destiné à des représentations théâtrales. Ce concept a évolué pour donner naissance aux véhicules automobiles que nous connaissons aujourd'hui. Les véhicules actuels intègrent déjà des fonctions d'aide à la conduite, ces fonctions concernent la direction, le contrôle de vitesse et le freinage (le maintien d'une distance de sécurité, le suivi de file, le freinage d'urgence…). En combinant ces différentes aides à la conduite, on peut voir qu'on se rapproche de plus en plus d'une conduite autonome. Dans cette étude, on s'intéressera au véhicule autonome de niveau 5 [1]. Les véhicules automobiles subissent des mise à jour logicielles (par exemple, par la technologie FOTA [2]). Nous nous intéressons plus particulièrement au véhicule autonome, dont les fonctions sont en évolution rapide, et nécessitent par conséquent, de nombreuses mises à jour.

La conception d'un tel système repose sur des capteurs à grand champs de détection qui permettent une meilleure supervision, et une électronique spécifique ainsi que des logiciels embarqués qui aident à la prise de décisions. La voiture autonome en tant que telle assure une meilleure sécurité de conduite que celle d'un humain. Selon certaines estimations le coût de réparation suite à des accidents routiers pourrait être réduit de 90% par les VAA [3]. Ainsi, l'adoption de la voiture autonome permettra d'économiser des milliards de dollars en frais d'assurance aux États-Unis, sans compter le gain énergétique issu de la fluidification du trafic (diminution de la distance inter-véhiculaire, réduction des blocages et autres).

L'une des différences entre l'étude des risques sur un véhicule non autonome et un VAA sont les contraintes liées aux logiciels de prise de décision du VAA. Ces logiciels sont spécifiques à l'aspect autonome du VAA. Pour les deux types de véhicules, le moment de mise à jour de leurs logiciels est restreint à des zones bien précises (zones sans danger).

B. La voiture autonome au sein du développement

L'évolution de la voiture autonome est aujourd'hui limitée par des contraintes liées aux différentes évolutions technologiques, ainsi qu'à la réglementation routière. Cependant, la réglementation évolue afin d'être moins restrictive vis-à-vis de la conduite autonome. Dans un premier temps, on peut supposer que la conduite autonome sera limitée à des zones autorisées. On peut anticiper que dans l'avenir, ces situations de conduite autonomes vont pouvoir s'étendre sur d'autres zones, où les utilisateurs du VAA pourront rouler en mode autonome en toute sécurité. Ce déploiement de la conduite autonome sera possible grâce aux retours des utilisateurs sur l'utilisation du VAA, et leur familiarisation avec ce type de véhicule. Avec l'évolution technologique et celle de la réglementation, l'acceptabilité des utilisateurs sera d'autant plus grande, ils en ressentiront les bénéfices, et intégreront ce mode de transport comme un nouveau besoin.

C. Etat de l'art des méthodes d'identification des risques

Différentes méthodes permettent l'identification et l'analyse des risques de sécurité et de sureté [4]. Nous nous intéressons plus particulièrement dans cette étude aux méthodes d'identification des risques. Parmi ces méthodes, on peut mentionner les approches suivantes : APR [5, 6], HAZOP [5], HAZID [6], AMDE/AMDEC [7, 8], ATBT [9]. La méthode utilisée ici repose sur la méthode SYSCIENCE présentée dans la publication [10]. Nous avons nommé cette dernière PODAM (Potential Damage Analysis Method). Cette méthode fait la jonction entre l'identification et l'analyse des risques de sécurité et de sureté liés aux éléments du système VAA.

Le tableau ci-dessous présente des exemples de méthodes d'identification des risques existantes, ainsi qu'une courte description de celles-ci :

TABLEAU I PRINCIPALES METHODES D'IDENTIFICATION DES RISQUES

Méthode	Objectif	Quantification	Scénario
APR [5, 6]	Identifier les ER susceptible de causer des accidents en présence de danger	Non	Oui
HAZOP [5]	Identifier les dangers suite à une déviation des paramètres d'un procédé	Non	Non
HAZID [6]	Identifier les risques suite à l'occurrence d'un événement initiateur	Non	Non
AMDE/AMDEC [7, 8]	Identifier les effets des modes de défaillance des composants sur le niveau système	Oui (AMDEC)	Non
ATBT [9]	Identifier et considérer tous les incidents et les menaces de sécurité qui peuvent entrainer les mêmes phénomènes indésirable générateur de dommage	Non	Non
PODAM [10]	Identifier les risques à partir des dommages infligés	Non	Oui

D. Problématique

La plupart des constructeurs automobiles ont des projets de développement portant sur des véhicules autonomes. Dans un monde où l'impact sur l'environnement est devenu un enjeu essentiel, il est important d'analyser dans un premier temps l'impact potentiel de l'introduction de la conduite autonome. De nombreux constructeurs ou équipementiers comme Renault [11], Stellantis [12], Tesla [13], BMW [14], Bosch [15] et d'autres, sont des acteurs du développement du VAA, et réalisent des mises à jour de logiciels sur leurs véhicules à distance, et de façon automatique. Cette pratique semble indissociable du maintien au meilleur niveau des fonctionnalités des véhicules qui doivent répondre à des exigences de sécurité qui sont citées dans la norme SOTIF [16], en particulier pour les véhicules autonomes.

La problématique qui se pose est bien d'identifier les risques qui apparaissent avant et/ou après la mise à jour du logiciel de la voiture autonome. Ces risques pourraient engendrer différents types de dommages, qui vont être infligés au conducteur du VAA, aux passagers ou aux personnes extérieurs, ou aux véhicules, ou autres éléments de l'environnement.

E. *Objectifs*

L'objectif est d'identifier plus précisément les risques associés au VAA, et à la mise à jour de ses logiciels. Cette étude vise à identifier non seulement les risques qui entrainent des dommages au conducteur, mais aussi à l'environnement naturel et tout ce qui entoure le VAA.

Par une analyse de risques holistique prenant en compte l'ensemble du cycle de vie, et pas seulement la phase d'utilisation, l'étude aboutit à des conclusions assez nouvelles. Cette étude permet d'aboutir à de nouveaux risques qui n'ont pas pu être identifiés dans d'autres méthodes. Notamment par exemple sur des questions liées à l'obsolescence.

F. *Enjeux de l'étude*

L'étude effectuée répond aux enjeux suivants :

- Identifier les risques liés aux mises à jour des logiciels du VAA.
- Assurer la complétude des risques étudiés dans le périmètre choisi.

II. MÉTHODOLOGIE

La méthode PODAM utilisée est une approche d'analyse des dommages [10], basée sur une analyse de l'environnement dans une approche système.

Cette méthode se base sur 7 étapes, qui sont les suivantes :

- Etape 1 : Formaliser le cycle de vie du système VAA
- Etape 2 : Modéliser l'environnement du VAA
- Etape 3 : Identifier les dommages potentiels
- Etape 4 : Définir le périmètre de l'étude
- Etape 5 : Identifier les scénarios catastrophes
- Etape 6 : Identifier les événements redoutés
- Etape 7 : S'assurer de la complétude de l'analyse

Nous discuterons ces étapes dans les sections suivantes.

A. *Etape 1 : Formaliser le cycle de vie du système VAA*

Cette étape consiste à identifier les différentes phases par lesquelles le VAA va passer au cours de son cycle de vie. On se base pour cela sur le cycle de vie standard de l'ingénierie système. Ce cycle de vie a été décrit à partir de la norme IEEE 15288 [17]. Une représentation de ce cycle de vie est réalisée grâce à un diagramme d'état (Figure 1).

Dans cette partie on définit le cycle de vie du VAA qui est représenté ci-dessous par un diagramme d'état. Dans ce diagramme sont citées les différentes phases par lesquelles le VAA passe tout au long de son existence. La plupart des études de risques se concentrent sur la phase d'utilisation. Une moindre importance est souvent portée à la phase de production (dommages potentiels infligés aux opérateurs de montage), et de maintenance (dommages infligés à l'opérateur de maintenance). Il est beaucoup plus rare de considérer le cycle de vie dans son ensemble. Nous nous efforcerons dans cette étude de conserver tant que possible ce point de vue holistique du cycle de vie.

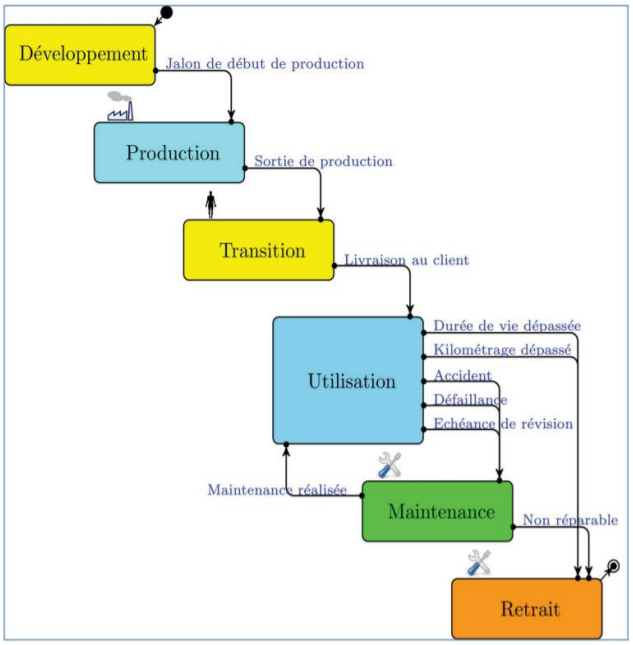

Fig. 1. Cycle de vie du système VAA

B. *Etape 2 : Modéliser l'environnement du VAA*

Cette deuxième étape consiste à définir et modéliser l'environnement du VAA. Dans une approche système nous considérons non seulement les occupants du véhicule et les véhicules alentours, mais aussi l'écosystème naturel, l'infrastructure routière et l'environnement socio-économique.

L'environnement du VAA est modélisé par des blocs en identifiant tous les acteurs qui sont en relation permanente, ou occasionnelle avec le système VAA. (Figure 2)

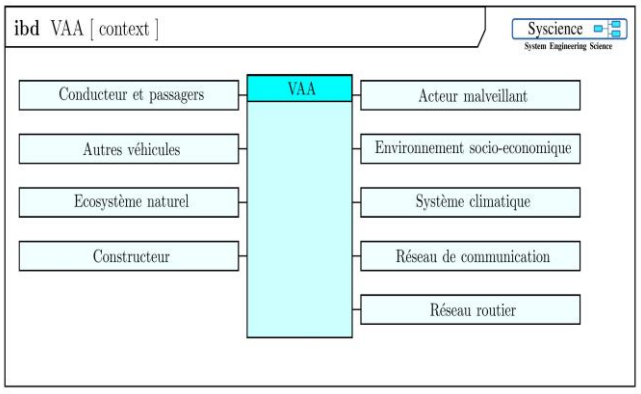

Fig. 2. Environnement du VAA

C. *Etape 3 : Identifier les dommages potentiels*

Cette étape consiste à identifier les dommages qui peuvent être infligés à chaque élément de l'environnement du VAA.

Une liste de dommages est établie pour chaque type d'élément de l'environnement du VAA (Tableau II et III).

Le tableau II fournit les dommages susceptibles d'être infligés à un humain. Ces dommages sont connus et ne nécessitent pas une discussion approfondie.

TABLEAU II. DOMMAGES POTENTIELS POUVANT ETRE INFLIGES A UN HUMAIN

Elément endommagé	Dommages potentiels
Humain (conducteur, passager, piéton…)	Chocs, coupure, brûlure, écrasement, intoxication, empoisonnement, suffocation, entrave, … Chocs psychologique, vol de données,…

La table III détaille les dommages pouvant être infligés aux éléments de l'environnement. Certains sont habituellement peu étudiés dans le cadre des études de sécurité.

TABLEAU III DOMMAGE INFLIGES A L'ENVIRONNEMENT DU VAA

Elément de l'environnement	Dommages potentiels
Système climatique	Diffusion de gaz à effet de serre…
Ecosystème naturel	Pollution des eaux, des sols, de l'air, augmentation des déchets, destruction de milieux naturels, perturbation d'espèces naturelles…
Réseau de communication	Saturation du réseau…
Infrastructure routière	Détérioration de l'infrastructure routière, blocage du trafic routier (création d'embouteillage)…
Autres véhicules	Collision, Aveuglement des capteurs…
Environnement socio-économique	Débits bancaires frauduleux, diffusion de données personnelles (atteinte à la RGPD, et à la protection des données) …

Ces listes pourraient être enrichies par les retours d'expérience tout au long de l'utilisation du système VAA.

D. Etape 4 : Définir le périmètre de l'étude

Les dommages étudiés sont sélectionnés parmi les dommages potentiels qui ont été identifiés dans l'étape précédente. Les dommages qui ne sont pas une conséquence directe du domaine étudié, ne sont pas pris en compte. Cette procédure de sélection et de mise à l'écart de dommages pour lesquels l'étude des risques n'est pas effectuée, sera mise en œuvre par un expert du domaine concerné qui doit avoir une vision globale des impacts potentiels.

Pour définir le périmètre de l'étude de risques que nous allons réaliser, nous commençons par sélectionner les éléments de contextes, et les dommages potentiels que nous souhaitons étudier. Pour réaliser cette phase, on va partir du diagramme de blocs qui a été réalisé précédemment dans l'étape 2 de l'étude (Figure 2), puis on procède à la sélection des éléments que l'on garde dans le périmètre de l'étude. Dans cette étude nous allons étudier plus particulièrement les dommages susceptibles d'être occasionnés à l'écosystème naturel. Nous conservons également l'infrastructure routière et le dommage potentiel de blocage ou de congestion du trafic, ainsi que les dommages par chocs pouvant être occasionnés au conducteur et aux passagers. La Figure 3 résume le périmètre retenu :

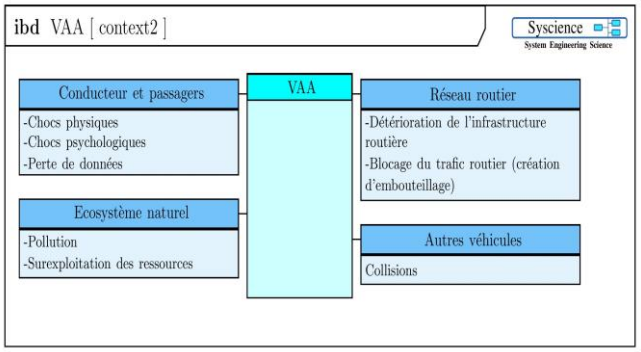

Fig. 3. Périmètre de l'étude

E. Etape 5 : Identifier les scénarios catastrophes

Un scénario catastrophe est une succession d'événements et d'activités dont la conséquence est un ou plusieurs dommages. Les scénarios catastrophes explicitent les enchaînements qui aboutissent à chacun des dommages étudiés. Les scénarios peuvent être représentés par des diagrammes de séquences.

La démarche part du dommage qui peut être infligé à l'un des éléments du système. On remonte le cours des événements (activité et messages réalisés par les acteurs) qui ont abouti au dommage considéré. Les acteurs ont été identifiés dans la phase de définition du périmètre de l'étude (étape 4). Cette démarche permet d'identifier un enchaînement d'évènements déclenché par un évènement redouté. La partie construction des scénarios de la méthode PODAM est similaire de celle de la méthode MOSAR [18].

F. Etape 6 : Identifier les événements redoutés

Un événement redouté représente le premier événement qui déclenche un scénario catastrophe. Cet événement s'insère dans un scénario normal d'utilisation du système et déclenche une cascade d'événements qui aboutissent à un dommage. Ces évènements redoutés sont mentionnés dans le tableau IV. Les événements redoutés sont liés à des éléments du diagramme de contexte réalisé dans l'étape d'identification du périmètre du VAA (Figure 3). L'analyse des scénarios catastrophes permet de s'approcher de l'origine de la faille, et ainsi définir l'élément redouté.

Ci-dessous est présentée une liste des événements redoutés, ainsi que les dommages qui peuvent en résulter, et les scénarios dans lesquels ces ER (Evénements Redoutés) se trouvent.

TABLEAU IV. LISTE DES EVENEMENTS REDOUTES

ER	Dommages	Scénario
Impossibilité de mettre à jour le véhicule	Pollution (création de déchets)	Fig. 4
Faille dans le logiciel	Débits bancaires frauduleux / dommage corporel / blocage du trafic routier	Fig. 5
Faille dans le protocole de téléchargement et de mise à jour	Débits bancaires frauduleux / dommage corporel / blocage du trafic routier	Fig. 6
Faille découverte et refus d'installation des mises à jour par certains conducteurs	Débits bancaires frauduleux / dommage corporel / blocage du trafic routier	Fig. 7
Installation du logiciel dans une zone dangereuse	Dommage par choc.	Fig. 8

G. Etape 7 : S'assurer de la complétude de l'analyse

Les événements redoutés pourraient être comparés à ceux obtenus par d'autres approches afin d'être la plus complète possible. Par exemple, cette analyse pourrait être avantageusement complétée par une analyse des attaques pouvant être tentées contre les véhicules autonomes. Cette recherche de failles peut s'effectuer grâce à des opérations de « bug bounty » par des hackers éthiques. Ces opérations contribuent au développement du logiciel. Cependant nous n'avons pas réalisé cette analyse dans le cadre de cette étude.

III. IDENTIFICATION DES DOMMAGES

Les résultats principaux sont obtenus dans l'étape 5. C'est pourquoi cette étape est détaillée dans ce paragraphe. Les scénarios catastrophes sont décrits par des diagrammes de séquence.

Dans cette étape on recherche les enchaînements d'activités qui aboutissent aux dommages infligés aux éléments de l'environnement. L'approche système permet d'avoir une vision holistique du système étudié (le VAA), ainsi que de son environnement. Cette approche sert à enrichir l'analyse des risques par de nouveaux risques qui concernent non seulement les dommages infligés à l'humain, mais aussi ceux infligés à l'environnement (pollution, dégradation…).

Ci-dessous seront présenté les scénarios catastrophes, avec leurs dommages en rouge et leurs ER en orange. Ces scénarios ont été construits par une analyse à rebours dans le temps en partant du dommage. Cependant pour leur description nous utilisons le sens chronologique pour faciliter leur compréhension.

Dommage à l'écosystème naturel

Dans cette étude nous nous somme intéressés à un périmètre original qui inclut l'écosystème naturel du VAA, afin d'identifier les impacts engendrés par le VAA lors de sa fin de vie. Néanmoins, d'autres études liées à la phase d'utilisation du VAA, et qui engendre une dégradation de l'environnement pourraient être réalisées. Nous nous proposons d'étudier les scénarios qui aboutissent à un dommage sur l'écosystème naturel. Dans une étude d'identification des risques de sécurité, ce type de dommage n'est pas traité dans une approche de type APR. Pourtant en considérant le cycle de vie dans son ensemble, ce type de dommage peut être identifié par l'approche PODAM. Par exemple, on considère le dommage à l'écosystème qui est la production de déchets (Figure 4). Ces déchets peuvent être issus de la mise au rebut de véhicules lié à la réduction de leur durée de vie. La fin de vie d'un véhicule, ou de tout produit manufacturé, entraine potentiellement la production de déchets, et cela quelle que soit la technologie utilisée.

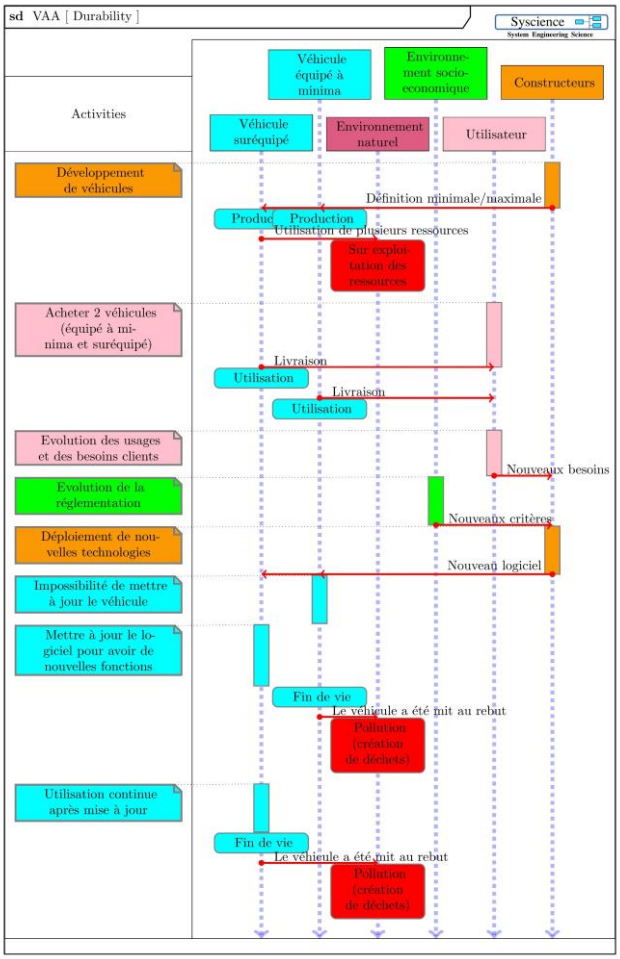

Fig. 4. Durabilité du VAA

Dans ce scénario (Figure 4), on ne peut pas proprement parler d'événement redouté qui déclenche une succession d'événements indésirables. Cependant il est possible d'identifier des causes potentielles d'une augmentation des dommages à l'environnement, et que l'une des cause pourrait être le fait que le constructeur du VAA ne prend pas en compte les évolutions technologiques et équipe le véhicule à minima. De ce fait, et avec l'apparition de nouveaux modèles de VAA, les anciens modèles verront leur durée de vie réduite ce qui va impacter l'écosystème naturel par l'augmentation des déchets et l'accroissement de l'exploitation des ressources.

Blocage du réseau routier

Un blocage de la circulation peut être infligé au réseau routier. Ce blocage se produit localement à chaque fois qu'un véhicule est en panne, ou qu'un accident se produit dans une zone à forte circulation et où le délestage est difficile. Ce dommage peut être très localisé. Une faille de conception du VAA pourrait créer un fonctionnement inapproprié des véhicules, et en conséquence, engendrer ce dommage de façon massive. La notion de faille peut ici être vue au sens large : il peut s'agir d'un défaut de conception, d'une situation normale qui n'aurait pas été prise en compte, ou même de l'existence d'une faille informatique qui permettrait à un pirate informatique d'accéder aux données du véhicule autonome, ou de l'immobiliser, voire d'en prendre le contrôle. Une faille peut exister dans tout développement, cependant, celle-ci pourrait ne pas avoir de conséquence.

Une faille peut être exploitée par des pirates informatique. L'exploitation d'une faille informatique peut avoir des conséquences graves. On imagine sans mal les conséquences de la panne simultanée de quelques centaines de véhicules sur une artère majeure de circulation à une heure de pointe. Les conséquences financières sont extrêmement importantes, sans parler du risque encouru à cause des difficultés d'accès de véhicules d'urgences à différentes zones d'intervention. Une faille informatique peut même être utilisée comme une arme.

Afin d'éviter ce genre de dommage, le constructeur du VAA devra maintenir une surveillance technologique de toutes sortes de failles pouvant être présente sur ses véhicules (les VAA), et ce de manière permanente, de telle manière à réaliser des mises à jour correctives dans les plus brefs délais.

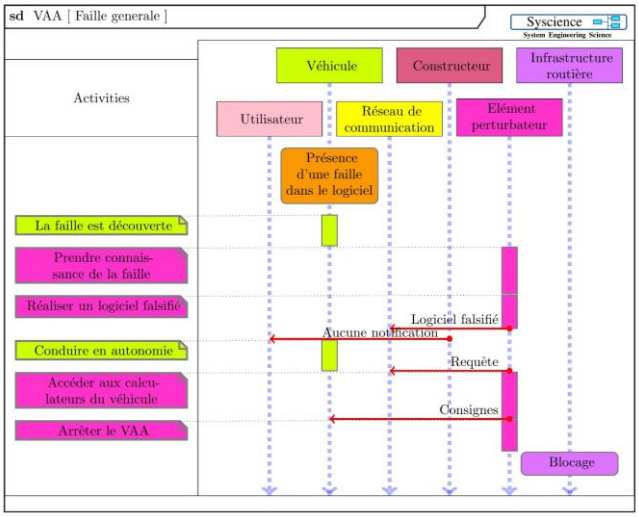

Fig. 5. Scénario de faille intrinsèque du logiciel du VAA

Faille de mise à jour du logiciel du VAA

Les mises à jour logicielles faites à distance permettent de corriger certaines failles, mais ouvrent également des possibilités d'attaques. Le scénario ci-dessous (Figure 6) décrit le cas où un pirate informatique interrompt l'envoi d'une mise à jour fournie par le constructeur du VAA, et injecte sa propre version corrompu du logiciel. Le conducteur procédera au téléchargement et à l'installation de la nouvelle version sans se rendre compte qu'elle est corrompue. Une fois la nouvelle version installée, l'élément perturbateur prend le contrôle du VAA, ce qui lui permet de réaliser les actions qu'il désire (débiter le compte du conducteur, arrêter le VAA et ainsi bloquer le trafic routier, causer un accident).

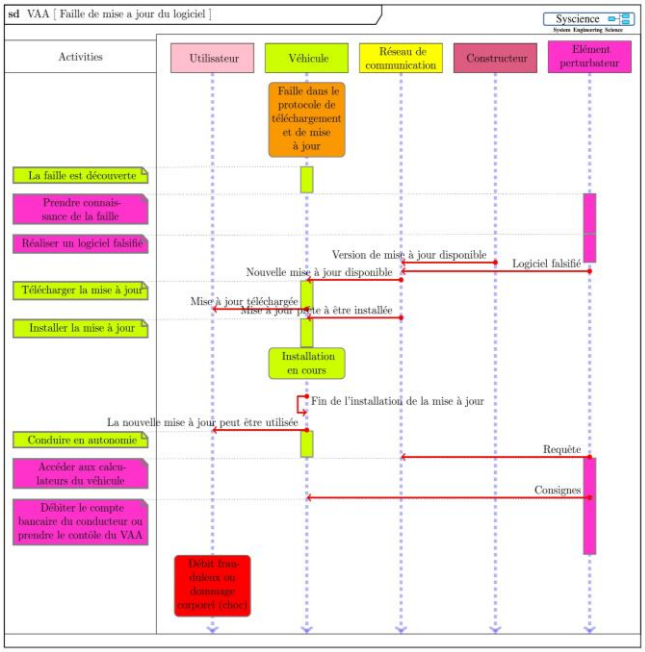

Fig. 6. Scénario de faille de mise à jour du logiciel du VAA

Correction non prise en compte

Lorsque le constructeur est averti d'une faille dans son logiciel, il doit mettre à disposition une mise à jour corrective (Figure 7). C'est le cas en particulier lorsqu'une faille devient découverte et accessible par un pirate informatique. Le système du VAA télécharge automatiquement la mise à jour, et envoie une notification au conducteur pour lancer l'installation de la mise à jour corrigée. Cependant l'utilisateur peut refuser la mise à jour du logiciel, en refusant les notifications de demande d'installation. Il suffit de quelques utilisateurs refusant la mise à jour, pour mettre en danger les autres utilisateurs. Ainsi la mise à jour régulière du logiciel du VAA est un enjeu de sécurité pour tous les usagers.

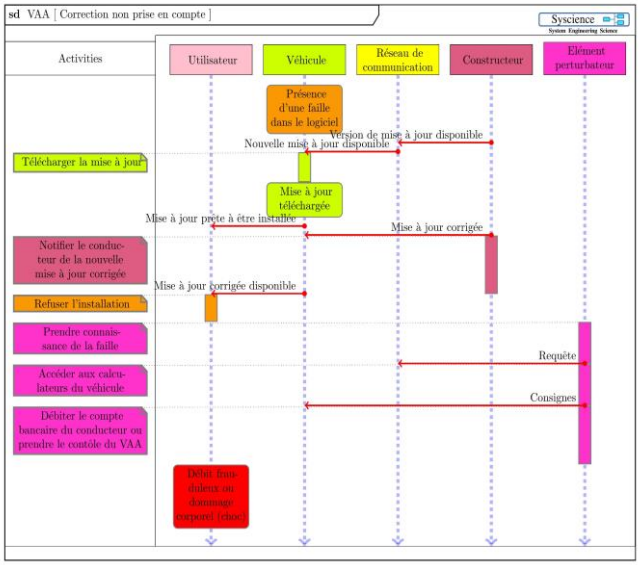

Fig. 7. Scénario de non prise en compte d'une mise à jour

Mise à jour en zone dangereuse

Par sécurité, le système du VAA exige de lancer les installations des mises à jour logicielles uniquement lorsque le véhicule est immobilisé (ce qui évite la perte de fonctionnalité durant la conduite). Mais dès que le véhicule est à l'arrêt (Figure 8), l'installation peut être lancée. Durant l'installation, l'utilisation du véhicule n'est pas possible. Il est immobilisé pendant un certain temps. En conséquence, le VAA pourrait être impliqué dans un accident du fait de son immobilisation en zone dangereuse. Cela peut engendrer des dommages corporels au conducteur. Cette situation pourra être évitée en limitant le lancement des installations de nouvelles mises à jour dans des zones de stationnement bien définies. La définition, le choix et la reconnaissance de ces zones par le logiciel embarqué deviennent donc des enjeux de sécurité.

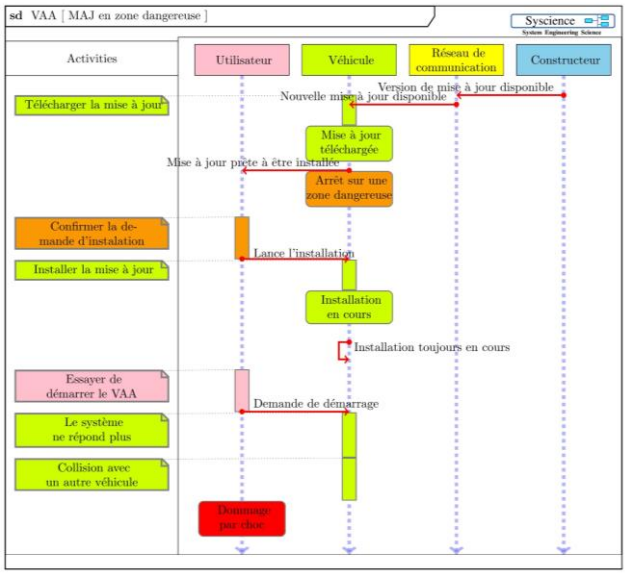

Fig. 8. Scénario de mise à jour logicielles sur une zone dangereuse

IV. EVALUATION DES RISQUES DE MISE A JOUR LOGICIELLE : PRINCIPES DE COTATION ET RESULTATS

Dans cette partie, on va concevoir une grille de cotation des risques d'attaques. Cette grille va permettre d'évaluer quelques risques déjà identifiés. Dans cette phase, on s'intéresse uniquement aux attaques pouvant être réalisées sur le logiciel du VAA. Dans un premier temps, on va étudier la faisabilité des attaques que le VAA pourrait subir. Cette étape consiste à dire à quel niveau de faisabilité une certaine attaque se situe, et ainsi donner une cotation liée à ce critère. Dans un deuxième temps, on viendra coter la criticité des risques d'attaques.

A. Faisabilité des attaques

La faisabilité correspond à l'effort qu'un attaquant doit fournir pour exploiter une faille. La présence d'une faille dépend de la qualité du logiciel et du processus de développement et de vérification. Ce critère prend en compte, l'expérience de l'attaquant, l'accessibilité de la faille, et les enjeux de l'attaque.

Nous avons utilisé une échelle de 1 à 10 pour nous rapprocher de l'approche AMDEC. Dans le tableau V sont mentionnés les statuts de faille qui peuvent exister. Le tableau V reprend les niveaux de cotation des attaques mentionnés dans la norme ISO 21434 [19].

Dans ce qui suit, l'étude va se focaliser sur les attaques venant d'éléments malveillants, car ces derniers risquent d'être très fréquents, et peuvent engendrer de nombreux dommages (explicités dans les scénarios à risque). Le tableau ci-dessous représente une grille de cotation :

TABLEAU V. FAISABILITE DES ATTAQUES [19]

Faisabilité de l'attaque	**Description**	**Cotation**
Elevé	La trajectoire d'attaque peut être accomplie en utilisant un faible effort	2
Moyen	La trajectoire d'attaque peut être accomplie en utilisant un effort moyen	4
Faible	La trajectoire d'attaque peut être accomplie en utilisant un effort élevé	6
Très faible	La trajectoire d'attaque peut être accomplie en utilisant un effort très élevé	10

La grille qui a été réalisée permet de coter la faisabilité des attaques liées à la mise à jour logiciel du VAA.

B. Calcul de la criticité

Par ailleurs, la faisabilité n'est pas le seul critère qui rentre dans la cotation des risques. Parmi les critères qui seront utilisés dans notre étude, on retrouve les trois critères classiques :

- La gravité (GR) du dommage.
- L'exposition (EX) : ou la présence de conditions à risques.
- La contrôlabilité (CTR) : la possibilité laissée au conducteur de contrôler la situation afin d'éviter les

dommages. Cela inclut le temps de réaction du conducteur pendant la conduite.

Les approches d'analyse des risques permettent couramment de calculer la criticité des risques. Elles font le produit des trois critères déjà évoqués :

CR = GR x EX x CTR

Dans cette étude nous avons considéré que pour les attaques informatiques, l'exposition EX correspond à la faisabilité d'une attaque. Nous avons multiplié ce critère par l'indice de contrôlabilité du risque d'attaquer. Le résultat de ce produit sera ensuite multiplié par la gravité du risque d'attaque pour prendre en compte le niveau de sévérité de chaque attaque. La norme ISO 26262 [20] contient des tables de cotation de ces trois facteurs (gravité ou sévérité, exposition, et contrôlabilité).

Le tableau ci-dessous montre une attribution de niveaux des trois critères (GR, EX, CTR), ainsi qu'une quantification de ces critères de cotation (Tableau VI) en utilisant les tables de cotation de la norme ISO 26262 :

TABLEAU VI. GRILLE DE COTATION DES RISQUES PROPOSEE

Grandeur d'évaluation	**Niveau**	**Cotation**
Gravité (GR)	Faible (pas de blessures) (S0)	4
	Moyen (blessures légères et modérées) (S1)	6
	Fort (blessures sévères mettant la vie du conducteur en danger) (S2)	8
	Très fort (blessures mortelles) (S3)	10
Fréquence d'Exposition (EX)	Improbable (E0)	2
	Très faible probabilité (E1)	4
	Faible probabilité (E2)	6
	Probabilité moyenne (E3)	8
	Probabilité forte (E4)	10
Contrôlabilité (CTR)	Contrôlable (C0)	4
	Moyennement contrôlable (C1)	6
	Peu contrôlable (C2)	8
	Difficilement contrôlable (C3)	10

On applique ensuite la grille réalisée sur les événements redoutés abordés dans notre étude. Le tableau ci-dessous représente une cotation des ER liés aux attaques.

TABLEAU VII COTATION DES ER

ER	**GR**	**EX**	**CTR**	**CR**
Faille dans le logiciel	10	8	10	800
Faille découverte et refus d'installation des mises à jour par certains conducteurs	6	8	8	384
Installation du logiciel dans une zone dangereuse	10	4	10	400

Dans ce tableau sont cotés les ER liés aux risques d'attaques des logiciels du VAA. Selon cette cotation le risque lié à une faille dans le logiciel du VAA devrait être traité en priorité, au vu de la valeur élevée de sa criticité. Pour les autres risques, ils seront traités selon un ordre décroissant de leur valeur CR.

V. DISCUSSION ET PERSPECTIVES

Dans cette discussion nous considérons le scénario correspondant à un dommage causé à l'environnement par l'exploitation des ressources et la production de déchets. La réalisation d'une fonction du VAA repose sur la combinaison d'une infrastructure matérielle qui rassemble dans le cas de la voiture autonome les différents capteurs, actionneurs, et les calculateurs, ainsi qu'une infrastructure logicielle qui va permettre de gérer le système VAA.

Selon le niveau d'équipement du véhicule, de nouvelles fonctionnalités peuvent être proposées sans nécessairement changer de véhicule, mais en installant des logiciels qui proposent de nouveaux services, ou qui autorisent le fonctionnement autonome dans un plus grand nombre de situations. L'absence de cette possibilité de mise à jour entraine une accélération de l'obsolescence et donc une diminution de la durée de vie. Il en résulte une augmentation globale des déchets et de l'exploitation des ressources car les véhicules obsolètes seront remplacés. Sans parler des dommages à l'image de marque du constructeur si des concurrents proposent ces mises à jour. Tout scénario qui empêche l'actualisation des fonctionnalités du véhicule autonome, cause potentiellement un dommage. C'est le cas par exemple si le nombre de mises à jour logicielles est limité, ou si la mémoire des calculateurs est insuffisante. En effet de nombreux constructeurs ont tendance à équiper leurs véhicules au plus juste en termes de capteurs. C'est-à-dire que les capteurs installés sur le véhicule permettent de réaliser les fonctions demandées à l'achat, sans aucune possibilité d'augmenter ces fonctionnalités par un abonnement à un nouveau service par exemple. Cette stratégie a pour but de diminuer le prix d'achat des véhicules. Une autre stratégie serait d'équiper les véhicules avec le maximum de capteurs et d'actionneurs, de façon à permettre l'intégration de nouvelles fonctions à venir. Cette intégration pourrait se faire uniquement par des mises à jour logicielles.

Dans cette étude, nous mentionnons ces deux stratégies. Leur comparaison est un problème complexe. La discussion pourrait être complétée par une étude quantitative. Il faudrait prendre en compte des contraintes telles que le poids du VAA, son volume, le nombre d'équipements qu'il contient etc, qui vont déterminer sa consommation énergétique, et augmenter la probabilité d'apparition de défaillances dans le système (VAA).

VI. CONCLUSION

Cette étude a été réalisée en utilisant la méthode PODAM d'identification et d'analyse des risques à partir des dommages que ces risques infligent. Cette méthode a permis d'identifier les risques pouvant apparaître au cours d'une mise à jour logicielle du VAA. Ces risques ont été évalués grâce à une grille de cotation des risques (VI). Cette cotation va servir à l'étude des solutions à mettre en place pour éviter ces risques ou diminuer leur impact.

Le constructeur du VAA, devra surveiller le software de ses véhicules afin d'identifier toutes faille ou risque d'intrusion au

système, et en conséquence, lancer de nouvelles mises à jour logicielles correctives.

L'approche utilisée dans cette étude consiste à adopter une vision globale, qui permet d'identifier les risques liés à la mise à jour du logiciel du VAA. Cette approche a permis d'identifier, en plus des risques de sécurité, des risques concernant une dégradation de l'environnement du VAA. Nous avons discuté l'impact possible de deux stratégies pouvant être choisies par les constructeurs quant à l'équipement des véhicules. Nous avons montré que ce choix peut entrainer des dommages pour l'environnement par son impact sur la durée de vie des véhicules.

REFERENCES

[1] P. Lakomicki, Y. Tourbier, B. Castanier, A. Grall, "Encadrement de la fiabilité du véhicule autonome pour guider les tests de validation", Congrès de maîtrise des risques et de sûreté de fonctionnement lambdamu21, 2018.

[2] H. Mansor, K. Markantonakis, R. N. Akram, and K. Mayes, "Let's Get Mobile: Secure FOTA for Automotive System", Information Security Group, Smart Card Centre, Royal Holloway, University of London, 2008.

[3] H. W. Kaas, D. Mohr, P. Gao, N. Muller, D. Wee, R. Hensley, M. Guan, T. Moller, G. Eckhard, G. Bray, S. Beiker, A. Brotschi, D. Kohler, "Automotive revolution – perspective towards 2030", McKinsey&Company, January 2016.

[4] T. Oueidat, J. M. Flaus, F. Massé, "Classification des principales méthodes d'analyse des risques combinant la sécurité et la sûreté", Congrès de maîtrise des risques et de sûreté de fonctionnement lambdamu22, 2020.

[5] M. H. Mazouni, "Pour une meilleure approche du management des risques: de la modélisation ontologique du processus accidentel au système interactif d'aide à la décision", Mémoire de thèse, L'institut national polytechnique de Lorraine, 2009.

[6] A. Desroches, A. Leroy, F. Vallée, "La gestion des risques, Hermes Science publications", 2003.

[7] T. Lombard, "Gestion des risques a priori : application de la méthode AMDEC à la production des médicaments anticancéreux au CHU de Grenoble", Mémoire de thèse, Université Grenoble Alpes, 2015.

[8] J. Kélada, "L'AMDEC, En ligne". Montréal : École des hautes études commerciales (HEC) - Centre d'étude en qualité totale, p 17. < neumann.hec.ca/sites/cours/6-510- 96/AMDEC.pdf >. 1998.

[9] H. Abdo, M. Kaouk, J. M. Flaus, F. Masse, "A new approach that considers cyber security within industrial risk analysis using a cyber bow-tie analysis", 2017.

[10] P. Krapf, S. Rakotosolofo, S. Berthier, "Utilisation d'un atelier d'ingénierie système pour l'Identification des risques d'un véhicule connecté", Congrès de maîtrise des risques et de sûreté de fonctionnement lambdamu21 Reims (16-18/10/2018).

[11] G. G. Abellan, Renault SYMBIOZ Demo car : l'expérience de demain commence aujourd'hui - autonome, électrique et connectée, Communication Renault, 2017.

[12] Stellantis et le projet de conduite automatisée L3Pilot, https://www.stellantis.com/fr/technologie/conduite-autonome, 2021.

[13] E. Mica R. "Autonomous Driving Systems: A Preliminary Naturalistic Study of the Tesla Model S". Journal of cognitive Engineering and decision making, 11(3), 225-238, 2017.

[14] M. Hartwig, "La voiture autonome, une chance pour une mobilité plus sûr, plus efficace, et durable pour tous ?", Perspectives, nécessité d'agir et de réglementer, E-Book, 10/01/2020, https://www.bmw.com/fr/innovation/livre-electronique-voiture-autonome-chances-pour-une-mobilite-durable.html

[15] R. Bosch GmbH, "Bosch Automotive Electrics and Automotive Electronics", Systems and Components, Networking and Hybrid Drive, 5th Edition, 2007.

[16] Norme ISO/PAS 21448 (SOTIF), 2022.

[17] ISO/IEC/IEEE 15288 : 2015, "Systems and software engineering — System life cycle processes", "Ingénierie des systèmes et du logiciel — Processus du cycle de vie du système", 2015-05-15.

[18] F. Munoz Giraldo, "Utilisation de l'ensemble méthodologique MADS/MOSAR pour l'évaluation des systèmes de barrières de sécurité : application au secteur minier colombien", Mémoire de thèse, L'institut national polytechnique de LORRAINE, 29/03/2018.

[19] ISO/SAE 21434:2021 - Véhicules routiers, p46, 08/2021.

[20] ISO 26262:2018 Functional Safety Standard for Modern Road Vehicles, 2018.