Utilisation d'un atelier d'ingénierie système pour l'Identification des risques d'un véhicule connecté

Pascal Krapf, Serge Rakotosolofo, Sébastien Berthier

Utilisation d'un atelier d'ingénierie système pour l'Identification des risques d'un véhicule connecté

Use of a system engineering workshop to identify the risks of a connected vehicle

Auteurs :
Pascal KRAPF, Serge RAKOTOSOLOFO, Sébastien BERTHIER.
Syscience
15, Avenue de Norvège, 91140 VILLEBON SUR YVETTE
pascal.krapf@syscience.fr

Résumé

Des modèles d'ingénierie système ont été utilisés pour établir une analyse préliminaire de risques d'un véhicule connecté. Les différents modèles utilisés ainsi que les différentes étapes de la démarche ont été illustrés par des exemples concrets. La méthode proposée permet d'englober dans un cadre global à la fois les aspects dysfonctionnels, les mauvais usages, les menaces et agressions, et les risques liés à la sécurité informatique. Nous en avons tiré quelques préconisations très générales sur le développement de véhicules connectés, et en particulier sur la nécessité de mettre en place une gestion des droits d'accès aux données.

Summary

System engineering models have been used to establish a preliminary risk analysis on a connected vehicle. Models used and successive steps of the method have been illustrated by applicative examples. The proposed method allows to encompass in the same frame malfunctions, misuses, threats and aggressions as well as software security. We propose very general recommendations on the development of connected vehicles. Especially we point out the necessity to manage the rights to access critical data.

1. Introduction

1.1. Objectifs

L'Atelier Syscience est un atelier d'ingénierie système permettant de modéliser un système dans son environnement par différents types de diagrammes. Il a été utilisé pour mettre en œuvre une méthode d'identification des risques basée sur des modèles d'ingénierie système. Cette méthode a pour but d'identifier les risques associés à l'introduction d'un nouveau produit ou d'une nouvelle fonctionnalité. Elle intègre les activités de sûreté de fonctionnement et d'analyse de sécurité à l'ingénierie système. Dans ce sens elle favorise une approche globale des différentes problématiques de conception. Le but de cette communication est de montrer que cette approche inclut de façon naturelle les risques liés à la sécurité informatique, au même titre que les risques d'agression, les risques fonctionnels et les risques associés à une mauvaise utilisation.

1.2. Contexte

Notre société et notre environnement sont actuellement l'objet d'un profond processus de transformation numérique. Cette transformation démultiplie notre potentiel de développement, et provoque une explosion des fonctionnalités et de la diversité des produits. Il est nécessaire de se protéger efficacement d'une mauvaise utilisation, voire d'un détournement de ce nouveau potentiel. Cela nécessite tout d'abord d'identifier et d'analyser les risques. Les méthodologies issues de l'ingénierie système constituent une réponse possible à ces nouvelles problématiques.

L'ingénierie système basée sur les modèles (Model Based System Engineering, MBSE) est une démarche de conception souvent utilisée pour développer des systèmes complexes. Le couplage des activités de conception et des analyses de sûreté de fonctionnement est très prometteur pour la réduction des coûts et du temps de développement et l'amélioration de la fiabilité (Mauborgne et al.,2013), (Mauborgne et al.,2015), (Cressent et al.,2012), (David, 2009), (Rauzy et al.,2008).

Cependant l'identification des risques de sécurité est encore assez peu couplée avec les modèles de conception. Un travail supplémentaire est donc nécessaire afin de combler ce manque. Une méthode d'identification de ces risques basée sur les modèles, a été proposée et décrite par Syscience en 2016 (Krapf et al.,2016). Elle sera dans la suite nommée « Méthode Syscience ».

La norme ISO26262 fournit un certain nombre de préconisations pour les systèmes à prédominance logicielle ayant un impact sécuritaire dans l'automobile. L'établissement d'une analyse préliminaire de risques (Mortureux, 2002) s'y inscrit dans la phase d'initialisation de l'analyse de sécurité. Il s'agit d'établir une liste de menaces, d'événements redoutés ou de défaillances impactant potentiellement la sécurité (Avizienis et al.,2001).

L'état de l'art dans le cadre de l'établissement et la mise à jour de cette liste s'appuie sur des approches différentes :

- Une approche fonctionnelle : elle consiste à effectuer une analyse dysfonctionnelle.
- Une approche de type « menaces et agressions » : elle consiste à analyser les effets de d'événements exceptionnels ou anormaux.

- Une approche « mauvais usage fortuit » de l'utilisateur : elle consiste à envisager les différents usages possibles par les utilisateurs. Elle nécessite une analyse des utilisations possibles.
- Une approche de type « résistance à des attaques ciblées » : Une personne ou un groupe explore et utilise de manière détournée les fonctionnalités existantes (atouts/failles), afin de répondre à un but différent de celui initialement prévu par le concepteur.

Plus particulièrement dans le cadre de la transformation numérique, sujet qui nous intéresse ici, les risques liés à la sécurité informatique doivent d'être pris en compte, au travers d'une approche spécifique permettant la recherche des effets des vulnérabilités informatiques.

Le choix de l'approche, la sélection des événements redoutés et l'évaluation des effets d'une défaillance reposent en grande partie sur un jugement d'expert et sur le retour d'expérience (David, 2009). Dans ces conditions, il est difficile de garantir la complétude de l'analyse préliminaire des risques.

1.3. Objet des travaux présentés

La Méthode Syscience (Krapf et al,2016), présentée en 2016, propose d'unifier les différentes approches d'identification des risques par une démarche globale basée sur les modèles d'ingénierie système. Ce travail s'est poursuivi par le développement de l'Atelier Syscience, un outil dédié à l'ingénierie système, qui constitue un support à cette méthode.
Cette publication comporte les points suivants :

- Un rappel de la description de la méthode,
- Une présentation succincte de l'outil que nous avons développé,
- Un cas appliqué permettant d'illustrer la méthode et l'utilisation de l'outil.

Les résultats et les diagrammes présentés dans cette communication ont été obtenus à l'aide de l'Atelier Syscience.

2. Méthode

La « Méthode Syscience », présentée au congrès LambaMu 20 (Krapf et al.,2016), est dédiée à l'identification des risques techniques et sécuritaires. Elle consiste à utiliser les approches et les modèles de l'ingénierie système pour identifier les risques par l'analyse de l'environnement du système à développer. Il s'agit ainsi d'une méthode qui répond spécifiquement au processus d'identification des risques selon la norme ISO 31000. Pour appliquer la méthode nous avons utilisé un outil de modélisation des systèmes, **l'Atelier Sysience** qui n'est pas dédié à cette méthode, mais permet de représenter les diagrammes clés utiles à sa mise en œuvre. La nature interdisciplinaire d'une analyse de contexte en ingénierie système permet de prendre en compte les risques issus de domaines techniques, organisationnels ou environnementaux. La méthode a été présentée en 2016, c'est pourquoi les principales étapes sont présentées ici sans discuter l'ensemble de la méthode. La méthode se déroule en plusieurs étapes :

- **Etape 1 : formaliser le cycle de vie.** Cette étape consiste à identifier les différentes phases de vie au travers desquelles le système va transiter. Ce cycle de vie est représenté puis raffiné par des diagrammes d'état. Les phases du cycle de vie ne sont pas nécessairement toutes analysées en détail.
- **Etape 2 : modéliser l'environnement.** Cette étape consiste à modéliser les relations du système avec son environnement, et ce dans différentes phases de vie. Ces éléments extérieurs sont représentés sur un diagramme de blocs. Le système et les éléments de l'environnement dans la phase de vie étudiée sont modélisés par des blocs. Les relations entre le système et chaque élément de l'environnement sont représentés par des liens surmontés d'un texte qui détaille les problématiques associées à la relation.
- **Etape 3 : identifier les dommages potentiels**. Cette étape consiste à identifier pour chaque élément de contexte les dommages qu'il peut subir, de par sa nature, dans tout type d'interaction qu'il peut avoir avec son environnement. Cette liste peut être établie hors contexte à partir des retours d'expérience portant sur tous les types d'interaction dont on aura eu connaissance. Une liste de dommages potentiels est ainsi associée à chaque élément de l'environnement.
- **Etape 4 :** définir le **périmètre de l'étude.** Il s'agit de sélectionner parmi les dommages potentiels identifiés à l'étape 3, les dommages qui vont être analysés de façon détaillée. Certains dommages ne sont pas susceptibles d'être infligés par le système étudié et peuvent être exclus de l'étude. L'ingénieur système prendra soin de noter les justifications pour l'exclusion des dommages pour lesquels l'étude de sécurité n'est pas retenue.
- **Etape 5 : Identifier les scénarios catastrophe**. Un scénario catastrophe est un scénario dont la conséquence est un dommage occasionné à l'un des éléments de contexte. L'aboutissement de chaque scénario catastrophe est donc l'un des phénomènes avec dommages identifié à l'étape précédente. Pour décrire un scénario catastrophe, il faut détailler comment le système évolue à partir d'un état normal pour aboutir à un dommage causé à l'environnement. Les scénarios catastrophe sont modélisés par des diagrammes de séquence.
- **Etape 6 : Identifier les événements redoutés (hazardous event).** Un événement redouté est un événement qui vient s'insérer dans un scénario normal et démarre une cascade d'événements qui aboutit à un dommage. Ce sera le premier événement d'un scénario catastrophe qui créera un écart par rapport à un scénario d'utilisation normal.
- **Etape 7 : S'assurer de la complétude.** Les résultats de l'étude sont comparés aux résultats d'études antérieures, quelle que soit la méthodologie utilisée pour celles-ci. Si des événements redoutés ont pu être mis en évidence par une autre méthode ou un retour d'expérience, c'est que l'environnement du système n'a pas été modélisé de façon exhaustive, ou que le périmètre de l'étude choisi à l'étape 4 était trop restrictif. L'étude peut, le cas échéant, être complétée pour prendre en compte des dommages complémentaires qui n'avaient pas été sélectionnés de prime abord.

Il est remarquable que cette méthodologie permette d'aborder dans une approche unifiée tous les types de risques. En particulier les risques liés à la sécurité informatique (security risk) peuvent être adressés dans la même démarche que les risques liés à l'exploitation d'un produit technique (safety risk). Elle met ainsi l'accent sur la multidisciplinarité indispensable pour aborder les problématiques systèmes de façon globale et d'optimiser la réponse technique pour des problématiques variées.

3. Outil

Syscience a développé un outil d'ingénierie système, **l'Atelier Syscience**, qui a été utilisé dans le cadre de cette publication pour appliquer la démarche décrite ci-dessus afin d'identifier les risques associés à la connectivité d'un véhicule automobile. Cet atelier n'est pas dédié aux études de sécurité mais vise à modéliser de façon collaborative les processus de l'ingénierie système. Il permet de représenter des diagrammes d'états, des diagrammes de contexte, des diagrammes de séquence, des diagrammes d'architecture etc. et de générer automatiquement certaines exigences à partir des diagrammes. Nous détaillons dans ce paragraphe les différentes étapes de la méthode ainsi que les diagrammes utilisés. Les diagrammes présentés ont tous été réalisés par L'Atelier Syscience.

4. Application de la méthode

4.1. Etape 1 : formaliser le cycle de vie.

Pour cette étude, nous avons choisi de nous baser sur le cycle de vie générique défini dans la norme IEEE15288. Il est représenté par le diagramme d'état figure 1. L'atelier permet au choix de modéliser chaque phase de vie de façon indépendante et de structurer la documentation par rapport à ces phases de vie, ou de regrouper les phases de vies pour les aborder de façon transversale. Pour cette étude, nous avons choisi de séparer les phases de vie et de nous focaliser plus particulièrement notre attention sur la phase de vie « utilisation ». Il s'agit d'un choix destiné à réduire le périmètre de l'étude. Bien entendu cela ne signifie pas que les autres phases de vie ne méritent pas une analyse des risques de sécurité.

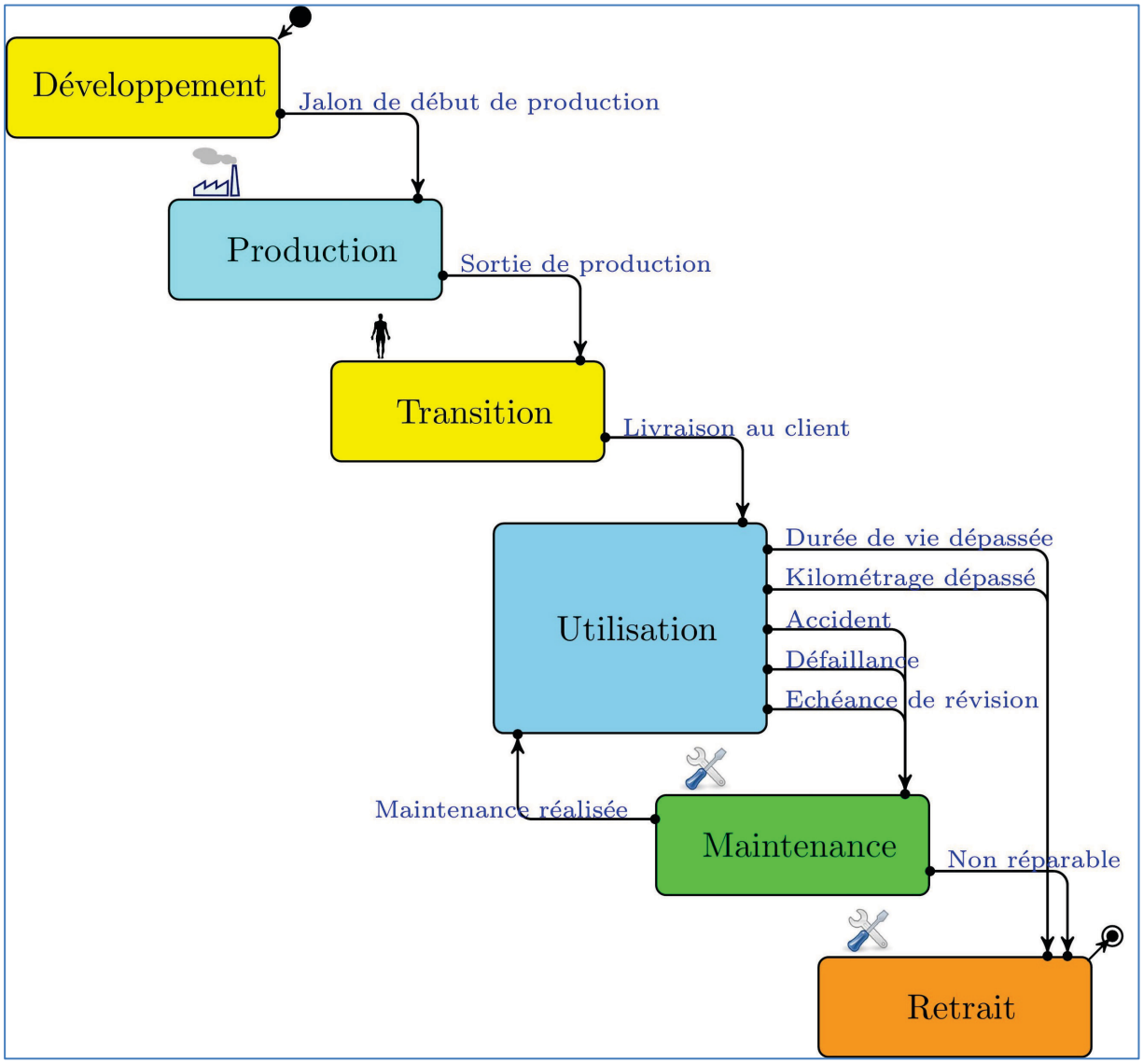

Figure 1: cycle de vie du système étudié

4.2. Etape 2 : modéliser l'environnement.

Pour chaque phase de vie définie à l'étape 1, nous avons représenté les éléments extérieurs en relation directe ou indirecte avec le véhicule connecté sur un diagramme de blocs comme illustré figure 2. Certains éléments de l'environnement sont en interaction fonctionnelle avec le système. Dans ce cas le lien qui relie un élément de l'environnement au système est surmonté d'un texte qui caractérise cette fonction. D'autres éléments de l'environnement sont en relation avec le système de façon contingente, parce qu'ils occupent un espace commun ou parce qu'ils sont en relation indirecte, via un intermédiaire. Il est ainsi utile de représenter l'analyse fonctionnelle de besoin, qui sert de base à l'approche fonctionnelle de la sureté de fonctionnement. La figure 2 montre comment le libellé des relations permet de traduire les fonctions de l'analyse fonctionnelle. Un diagramme de contexte est potentiellement plus riche qu'un tableau de fonctions car il permet de représenter des éléments extérieurs pour lequel la relation avec le système n'est pas toujours de nature fonctionnelle. C'est le cas par exemple des éléments naturels comme l'écosystème naturel. Il est toutefois souvent possible de réintégrer ces éléments dans une approche fonctionnelle en identifiant des fonctions de contrainte ad hoc.

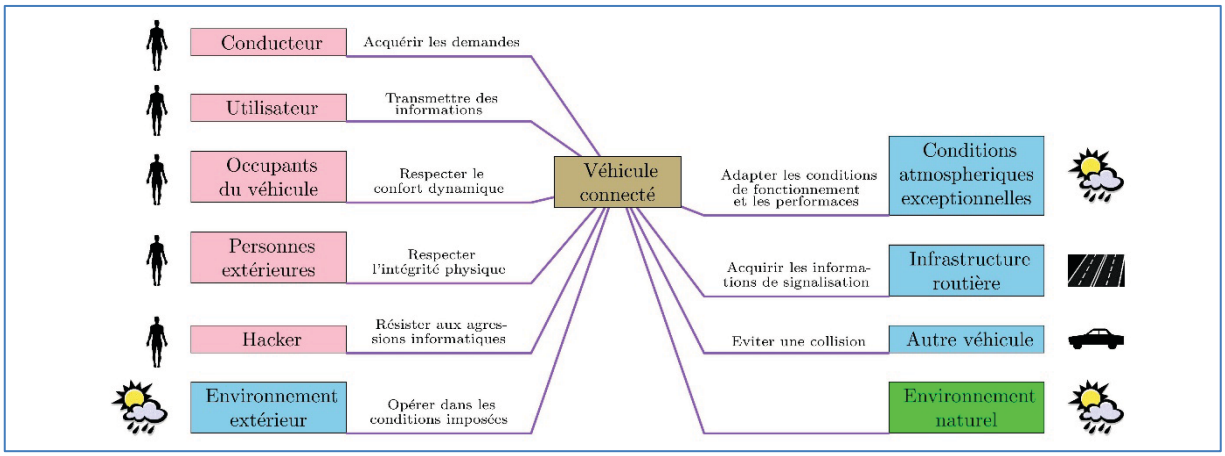

Figure 2: diagramme de contexte du système étudié

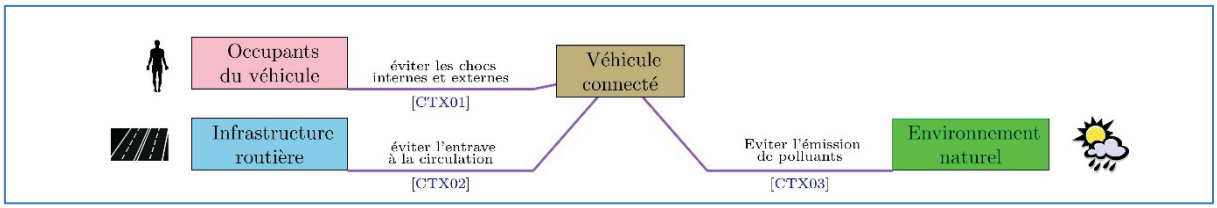

Figure 3: définition du périmètre de l'étude

4.3. Etape 3 : identifier les dommages potentiels.

Cette étape consiste à identifier pour chaque élément de contexte les dommages qu'il peut subir dans tout type d'interaction qu'il peut avoir avec son environnement. Cette liste peut être établie hors contexte à partir des retours d'expérience portant sur tous les types d'interaction dont on aura eu connaissance. Une liste de dommages potentiels est ainsi associée à chaque élément de l'environnement.

La table 1 présente une liste de dommages potentiels pouvant être infligés à un être humain, à l'infrastructure routière et à l'écosystème naturel. Cette liste non limitative comporte certains dommages qui sont rarement étudiés dans une étude de sûreté. Cette table est inspirée de la publication (Krapf et al.,2016). Elle correspond à une sélection de dommages destinés à illustrer notre exemple et est issue d'un catalogue plus général, trop long pour être intégré in extenso à cette publication.

Type d'élément de contexte	Dommages potentiels
Etre humain	Choc avec un objet dur Choc interne (Accélération ou décélération extrême) Coupure, perforation Brûlure thermique Brûlure électrique Brûlure chimique Choc électrique Intoxication gazeuse Empoisonnement Etouffement Vol de biens Vol de données Entrave, enfermement
Infrastructure routière	Entrave à la circulation Dégradation de l'adhérence Encombrement Destruction d'éléments par choc
Environnement naturel	Pollution gazeuse Pollution liquide Pollution solide Empoisonnement d'animaux Destruction de l'habitat naturels

Table 1. Dommages potentiels pour trois types d'éléments de l'environnement

4.4. Etape 4 : définir le périmètre de l'étude.

Il est clair qu'il n'est ni possible ni pertinent de considérer l'ensemble de tous les dommages potentiels pour chaque étude de sécurité. Les dommages qui ne sont pas susceptibles d'être infligés par le système étudié peuvent être exclus de l'étude. Ainsi on réalise une sélection parmi

les éléments de contexte que l'on étudie, et on réalise une seconde sélection sur les dommages que l'on étudie.

Un diagramme de contexte système montre un système dans son ensemble et ses interactions avec des facteurs externes. (Kossiakoff et al.,2011). Il représente toutes les entités externes qui peuvent interagir avec un système. Un tel diagramme représente le système au centre, sans détails sur sa structure intérieure, entouré de son environnement.
Le périmètre de l'étude est représenté par un diagramme de contexte (figure 3) sur lequel on représente les éléments susceptibles de subir des dommages. Le dommage étudié est noté sur le lien entre le système et l'élément. Le texte noté sur le lien commence par le verbe « éviter », suivi du dommage. On peut construire une phrase en lisant le nom du système dans la boîte centrale, suivi du verbe « doit » suivi du texte du lien, suivi de « infligé à » suivi du nom de l'élément de contexte. Par exemple : « Le véhicule connecté doit éviter l'émission de polluants infligée à l'environnement naturel ». On peut alors générer automatiquement des exigences qui concernent la sécurité du système à partir du modèle.

Identifiant	Exigence
CTX01	Le véhicule doit éviter les chocs internes et externes infligés aux occupants.
CTX02	Le véhicule doit éviter l'entrave à la circulation infligée à l'infrastructure routière.
CTX03	Le véhicule doit éviter l'émission de polluants infligée à l'environnement naturel.

Table 2. Exigences générées automatiquement

Pour cette étude nous avons retenu les éléments de contexte :

- « Occupants du véhicule » pour lequel sont retenus les dommages suivants : choc avec un objet dur, choc interne (accélération ou décélération extrême). D'autres dommages comme, coupure, perforation, vol de biens, vol de données, entrave, enfermement, peuvent lui être infligés mais ne sont pas abordées ici.
- Infrastructure routière pour lequel est retenu l'événement Entrave à la circulation

Cet élément de contexte et ce dommage sont très rarement étudiés. Cependant dans le cadre du déploiement des véhicules autonomes sans conducteurs, il devient pertinent. En effet, un véhicule autonome sans conducteur qui tombe en panne peut immobiliser la circulation tout comme un véhicule classique. Mais dans le cas d'un véhicule avec chauffeur, ce dernier prend en charge la panne, dégage tant que faire se peut les voies de circulation, signalise son véhicule, et alerte un dépanneur. Ce sont des stratégies d'accommodation qu'un véhicule sans chauffeur doit pouvoir prendre en charge avec le niveau de disponibilité adéquat. Il ne serait certainement pas acceptable, même en phase de tests, qu'un véhicule s'immobilise et se verrouille au milieu d'une autoroute à une heure de pointe. Il serait tout aussi inacceptable qu''il bloque la circulation à un endroit critique (un accès à un hôpital par exemple).

Les justifications pour l'exclusion des dommages pour lesquels l'étude de sécurité n'est pas retenue sont rédigées dans le texte du document de l'étude.

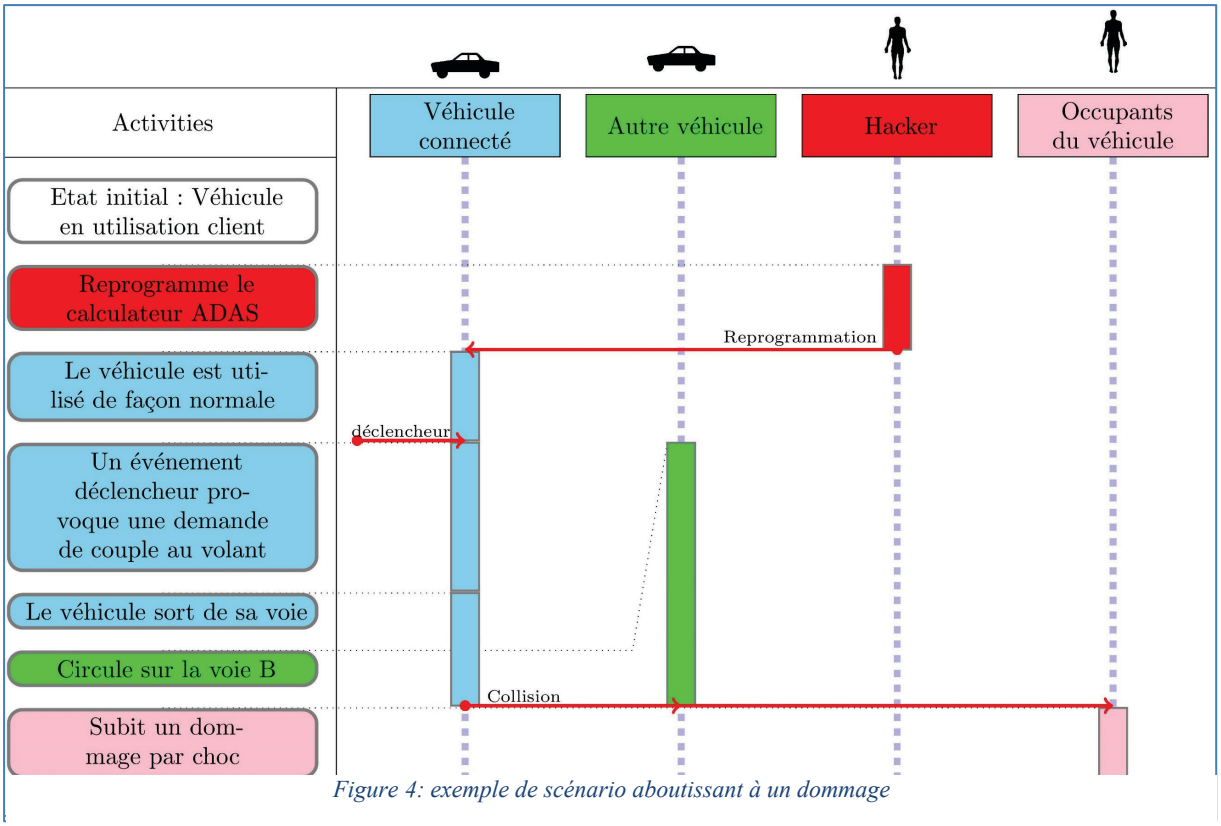

Figure 4: exemple de scénario aboutissant à un dommage

4.5. Etape 5 : Identifier les scénarios catastrophe.

Un scénario catastrophe est un scénario dont la conséquence est un dommage occasionné à l'un des éléments de contexte. L'aboutissement de chaque scénario catastrophe est donc l'un des phénomènes avec

dommages identifié à l'étape précédente. Pour décrire un scénario catastrophe, il faut détailler comment le système évolue à partir d'un état normal pour aboutir à un dommage. Les scénarios catastrophe sont modélisés par des diagrammes de séquence.

La méthode que nous avons retenue pour construire les scénarios catastrophe est de partir du dommage et de construire le scénario à rebours. A chaque étape les éléments de contexte sont envisagés un à un en posant la question suivante « Une activité de cet acteur a-t-elle pu être l'étape précédente dans le scénario catastrophe ? ». L'avantage de cette méthode est que chaque scénario construit de la sorte aboutit effectivement à un dommage. Nous présentons figure 4 un diagramme de séquence correspondant à un scénario construit par cette méthode. Dans les éléments de contexte figure 3 nous avons considéré qu'un pirate informatique pouvait être en relation avec le système. Le scénario présenté figure 4 fait effectivement intervenir un pirate informatique. La sécurité informatique rejoint ici la sécurité générale du produit : un véhicule dont une personne mal intentionnée pourrait prendre le contrôle serait un danger pour tous. La couverture des scenarios catastrophe est bien sur limitée par la connaissance que l'on peut avoir des systèmes et de leurs environnements. De plus, elle dépend du périmètre définit par le modélisateur dans le cadre de son étude.

4.6. Etape 6 : Identifier les événements redoutés (hazardous event).

Un événement redouté est un événement qui vient s'insérer dans un scénario normal et démarre une cascade d'événements qui aboutit à un dommage. C'est le premier événement d'un scénario catastrophe qui crée un écart par rapport à un scénario d'utilisation normal. Cette notion d'événement redouté n'est pas différente de celle que l'on rencontre habituellement au niveau d'une analyse préliminaire des risques. L'étape initiale d'un scénario peut parfois être une étape intermédiaire dans un scénario plus long. Il n'est alors pas évident de déterminer si cette étape initiale doit être considérée comme un événement redouté ou s'il faut construire un scénario où elle apparait comme étape intermédiaire.
Dans le scénario construit au paragraphe précédent, l'événement redouté serait l'intervention d'un pirate informatique. Cependant l'existence de pirates informatiques est un fait avéré et il n'est pas possible de l'éviter. En revanche un pirate informatique ne peut intervenir que si une faille existe dans la protection du système. L'événement redouté serait donc plutôt l'introduction d'une faille de sécurité. Nous pouvons parcourir de façon systématique les diagrammes de contexte de chaque phase de vie pour identifier quel élément pourrait être à l'origine d'une faille. Les failles potentielles sont multiples et il est difficile d'en établir une liste exhaustive. Mais il est certainement utile d'identifier les sources les plus évidentes afin de ne pas être vulnérable à des failles simples. Deux sources simples de failles sont présentées dans la table 3.
Il est ainsi pertinent de réexaminer les scénarios catastrophe pour voir s'il est possible de les compléter ou de les généraliser en considérant l'état initial comme un état intermédiaire d'un scénario plus élaboré. Il est tout à fait normal d'aboutir par cette démarche à une liste similaire à celle que l'on obtient par une analyse dysfonctionnelle doublée d'une analyse des mauvais usages et des risques de dommages et agressions. La plus-value est avant tout de s'assurer que cette nouvelle vue ne fait pas apparaitre de risque non identifié.

Identifiant	Exigence
ER1	Un pirate informatique a accès à un moyen de modifier le logiciel d'un calculateur lors d'une reprogrammation.
ER2	Un pirate informatique intervient lors du développement du logiciel et parvient à identifier (voire insérer) une faille de sécurité.

Table 3. Exemples simples de failles possibles

4.7. Etape 7 : S'assurer de la complétude.

Nous avons présenté ici un échantillon d'exemple d'application de la méthode et de l'outil Syscience. Cette présentation ne peut pas se prévaloir d'un quelconque argument de complétude. Cependant l'approche peut être développée jusqu'à documenter chaque élément du diagramme de contexte et chaque dommage retenu pour l'étude. Les résultats de l'étude peuvent être comparés aux résultats d'études antérieures, quelle que soit la méthodologie utilisée pour celles-ci. Tous les événements redoutés mis en évidence par une autre méthode ou un retour d'expérience, doivent être identifiés si l'analyse a été assez poussée. Si ce n'est pas le cas, il convient de vérifier que l'environnement du système a été modélisé de façon exhaustive, et que le périmètre de l'étude choisi à l'étape 4 n'était pas trop restrictif. Cette dernière étape de vérification de la complétude nous semble indispensable pour rester dans une démarche d'amélioration permanente et ne pas se laisser abuser par un caractère systématique qui pourrait masquer les insuffisances d'une analyse de contexte ou omettre une utilisation du système qui n'aurait pas été identifiée dans les scénarios d'utilisation standard. On voit que la complétude est obtenue via un développement très détaillé de la méthode. La discussion du paragraphe suivant s'attachera à définir dans quelle mesure cet objectif est réalisable et comment cela est possible sans introduire une complexité et une lourdeur contre-productives.

5. Discussion

5.1. Méthode inductive versus déductive

Une méthode usuelle pour établir un scénario catastrophe consiste, à partir des fonctions du système et pour chacune d'entre elles, à construire des scénarios qui comportent l'absence, la perte, le déclenchement intempestif, la non désactivation, un comportement erroné permanent ou erratique de la fonction. Cette méthode est parfois appelée « méthode inductive ». Elle ne suppose pas l'existence d'un dommage, mais consiste à examiner les modes de fonctionnement connus afin de déterminer s'ils peuvent aboutir à un dommage ou à un événement redouté identifié par retour d'expérience. Dans ce cadre, la complétude de l'étude suppose d'une part que l'on ait envisagé tous les types de dysfonctionnements possibles et que l'on ait analysé toutes leurs conséquences, et d'autre part que l'on ait pris en compte de façon systématique :

- Les mauvais usages - ce qui est difficilement possible concernant de nouveaux systèmes
- Les menaces et agressions non fonctionnelles - ce qui n'est possible que si la technologie est bien connue.

Une autre méthode consiste à partir du dommage que l'on souhaite étudier pour construire le scénario à rebours. Cette méthode est appelée « méthode déductive » car elle repose sur une analyse des enchaînements logiques à rebours en partant du dommage infligé. La méthode inductive présente l'avantage d'être simple et naturelle,

mais elle ne permet pas de garantir que toutes les situations possibles sont étudiées. La méthode déductive se veut systématique dans l'examen des éléments de contexte et des scénarios d'utilisation standard, mais elle est moins naturelle et son caractère systématique n'est valable que si les scénarios d'utilisation standard sont suffisamment bien connus et décrits. Elle présente aussi l'inconvénient de devoir choisir les scénarios à étudier car la combinatoire crée un nombre de scénarios possible trop grand. Ainsi l'argument de complétude peut sembler plus abordable que pour la méthode inductive, au moins concernant les nouveaux systèmes et les nouvelles technologies. Cependant un argument rigoureux de complétude nécessiterait un travail énorme et devient très difficile à réaliser en pratique.
Afin de proposer une approche efficace qui se rapproche de la complétude sans en avoir une démonstration formelle il est possible de combiner les deux approches en construisant un premier scénario de façon déductive, puis en analysant la possibilité de créer d'autres scénarios de façon inductive à partir de celui-ci. Ce rapprochement des deux types de méthodes a déjà été souligné dans le domaine du nucléaire (Claisse et al.,2017). L'une des leçons que nous tirons de notre étude est que ce type d'approche combinée semble le plus prometteur en termes d'efficacité sur un périmètre nouveau où le retour d'expérience reste à construire. Cette combinaison des méthodes permet de s'affranchir des lourdeurs qu'impose une approche unidirectionnelle (déductive ou inductive) que l'on cherche à pousser jusqu'à obtenir un niveau de complétude. Notre préconisation est donc d'utiliser cette approche combinée dans l'étape 7.

5.2. Sécurité informatique versus sécurité générale du produit

Que l'on considère la sécurité informatique d'un véhicule ou la sécurité au sens de la sûreté de fonctionnement, il est clair que les dommages potentiels pouvant être causés sont les mêmes : une perte de contrôle du véhicule entraine les mêmes conséquences, qu'elle soit provoquée par l'intervention d'un pirate informatique ou par la défaillance d'un composant du système. Jusqu'à un certain point, ce sont également les mêmes interfaces qui seront en jeu. Ainsi une interface de pilotage d'un actionneur critique doit être protégée à la fois contre une défaillance technique et contre l'intrusion d'un pirate informatique. Inversement un pirate informatique qui cherche à causer un dommage ou à obtenir une rançon pourrait avantageusement s'appuyer sur une étude de sécurité du produit pour identifier les interfaces à contrôler dans le but d'infliger des dommages.
L'approche que nous proposons consiste à partir du dommage pour construire un scénario catastrophe, puis à identifier d'autres événements qui pourraient aboutir au même scénario catastrophe. L'intervention d'un pirate informatique est un événement qui peut déclencher la plupart des scénarios. Ainsi un scénario catastrophe technique fournit un angle d'attaque sur le système pour une attaque informatique. La sécurité informatique est souvent abordée comme un sujet à part, traité par des spécialistes. Peut-être serait-il intéressant de sensibiliser les concepteurs techniques à ces risques spécifiques afin qu'ils puissent proposer des architectures intrinsèquement robustes. Nous en tirons les points clés suivants :

- Le développement des logiciels est un point sensible. La qualité du développement doit être garantie et le risque de failles minimisé.
- La reprogrammation des calculateurs est une étape qui peut contenir des failles. Elle doit être sécurisée avec le plus grand soin.
- La diffusion des études de sûreté du produit doit être limitée à des personnes autorisées et qualifiées afin de réduire le risque qu'elles soient utilisées pour attaquer le système.
- Les droits d'accès et de modification aux éléments techniques (droit d'accès aux études de sûreté, écriture des logiciels, reprogrammation des calculateurs…) doivent être définis et gérés pour chaque entité d'un projet.

Il s'agit certes de préconisations générales, mais il serait souhaitable que tous les intervenants d'un processus de conception d'un système cyber-physique comme le véhicule autonome prennent en considération le risque d'une attaque volontaire sur leur système non pas comme une possibilité mais comme une certitude. Et ces attaques utiliseront les données techniques disponibles.

5.3. Avantages et limites de la méthode

Le premier avantage de la méthode est la réutilisation des données et des modèles de l'ingénierie système. Il n'est pas nécessaire de faire une analyse fonctionnelle de besoin si cette analyse a déjà été formalisée dans la démarche de conception. Il en résulte d'une part un gain de temps associé aux activités qui ne sont pas dupliquées, et d'autre part une collaboration renforcée entre l'ingénieur système et l'expert en sûreté de fonctionnement.
Un second avantage est qu'elle suppose de balayer de façon systématique tous les éléments de contexte et tous les dommages qui peuvent leur être causés. Elle permet ainsi d'envisager des dommages éventuels qui n'auraient pas été mis en évidence par un retour d'expérience. Elle permet d'envisager ainsi des risques nouveaux ou atypiques, comme l'entrave à la circulation par un véhicule autonome en panne.
Enfin un troisième avantage est que cette approche permet d'embrasser dans une approche générale et unifiée les mauvais usages, les dysfonctionnements, les menaces et agressions physiques et la sécurité informatique.

La principale limitation de la méthode réside dans la qualité de la modélisation de l'environnement et dans la sélection des dommages que l'on étudie : une modélisation incomplète de l'environnement peut entraîner une prise en compte incomplète des risques. La complétude d'une étude ne peut être garantie que dans la limitation des choix effectués.
Une autre limitation réside dans la construction « à rebours » des scénarios. Cette construction n'est pas le sens naturel de perception d'un événement. Or le raisonnement humain est plus efficace lorsqu'il correspond au sens naturel des événements. C'est pourquoi l'étape 7 de la méthode a été ajoutée à sa description initiale : La méthode Syscience fournit un cadre d'intégration unifié pour les approches de sûreté de fonctionnement et de sécurité des données, mais elle ne remplace pas les méthodes existantes.
.

6. Conclusion

Des modèles d'ingénierie système ont été utilisés pour établir une analyse préliminaire de risques d'un véhicule connecté. Les différents modèles utilisés ainsi que les différentes étapes de la démarche ont été illustrés par des exemples concrets. Les arguments de complétude mènent à une comparaison entre une approche déductive et une approche inductive. Les deux types d'approches sont complémentaires et s'enrichissent l'une l'autre pour assurer une meilleure couverture de l'analyse. La méthode proposée permet d'englober dans un cadre global à la fois les aspects dysfonctionnels, les mauvais usages, les menaces et agressions, et les risques liés à la sécurité informatique. La plus-value de notre communication n'est pas dans l'identification d'un risque nouveau et original, mais dans la synergie des

approches. Nous en avons tiré quelques préconisations très générales sur le développement de véhicules connectés, et en particulier sur la nécessité de mettre en place une gestion des droits d'accès aux données. En effet ces données peuvent être utilisées dans le cadre d'une attaque informatique. Il est essentiel que les concepteurs techniques soient conscients de ce risque.

Il est souhaitable que les véhicules autonomes et les technologies intégrées au sein de « Smart City » soient protégés dès leur phase de conception contre des intrusions informatiques susceptibles de ternir le succès de ces technologies. Il semble indispensable d'éviter les dérives qui ont pu se produire au début de l'internet des objets pour lesquels les aspects sécurité informatiques ont été pris en compte après les premières intrusions avérées.
La leçon à tirer de notre analyse est que l'ingénieur système doit avoir une sensibilisation à la fois à la sureté de fonctionnement et aux risques liés à la sécurité informatique.

Une seconde leçon à tirer de nos travaux est que les modèles utilisés en ingénierie système pour la collecte des besoins peuvent être utilisés pour déterminer des risques techniques ou des cibles de pirates informatiques. Utiliser les modèles de l'ingénierie système plutôt que de faire une analyse fonctionnelle dédiée à la réalisation d'une APR apporte un gain de temps considérable pour le spécialiste de la sûreté de fonctionnement. Cela apporte aussi une réduction du risque d'incohérence entre la définition du produit et l'étude de sécurité qui peut se produire lorsque les démarches sont menées indépendamment. Enfin cela apporte une meilleure implication des ingénieurs système dans les activités de sûreté de fonctionnement et au final une meilleure garantie de sécurité du produit.

Les gains potentiels du rapprochement de la sûreté de fonctionnement et de l'ingénierie système ne s'arrêtent pas à la collecte des besoins et à l'APR. Nous avons commencé à travailler sur le rapprochement de la définition des architectures sûres de fonctionnement à l'aide de diagrammes d'architecture. Syscience ambitionne en particulier de générer automatiquement les exigences de sécurisation des interfaces et des messages à partir des diagrammes d'architecture. Nous espérons présenter cette nouvelle brique de notre développement lors d'une future communication.

7. Références

A. Avizienis, JC Laprie, B. Randell, 2001, Fundamental Concepts of Dependability, University of Newcastle upon Tyne, Computing Science, 19/04/2001.

A. Claisse, J. Averous, 2017, La méthode ROOTS® - une nouvelle méthode de référence pour les analyses de sûreté des laboratoires, usines et installations en démantèlement, Livre blanc Cleanuc, Document de reference 2017-01, janvier 2017.

R. Cressent, P. David, V. Idaziak, F. Kratz, 2012, Designing the database for a reliability aware Model-Based System Engineering process. Reliability Engineering and System Safety.

P. David, 2009, Contribution à l'analyse de sûreté de fonctionnement des systèmes complexes en phase de conception : application à l'évaluation des missions d'un réseau de capteurs de présence humaine, Thèse de doctorat.

P. Krapf, D. Loise, 2016, Méthode d'identification des risques basée sur les modèles, 20e congrès de maitrise des risques et de sûreté de fonctionnement, Saint-Malo, Octobre 2016.

A. Kossiakoff, W. N. Sweet, 2011. Systems Engineering: Principles and Practices p. 266, 2011.

P. Mauborgne, S. Deniaud, E. Levrat, E. Bonjour, P. Lamothe, D. Loise, JP. Micaëlli, 2013, Comment relier l'ingénierie système et la sûreté de fonctionnement ? 10e Congrès international de Génie Industriel, La Rochelle, Juin 2013.

P. Mauborgne, D. Loise, 2015, Vers une ingénierie de systèmes sûrs de fonctionnement basée sur les modèles en conception innovante, Séminaire Francilien de Sûreté de Fonctionnement, mars 2015.

Y. Mortureux, 2002, La Sûreté de fonctionnement : méthodes pour maîtriser les risques. Techniques de l'ingénieur.

A. Rauzy, Z. Brik, E. Arbaretier. 2008, Sûreté de Fonctionnement et Analyse de Performance. Actes du 16ème Congrès Lambda Mu, Avignon, octobre 2008.