# Chapitre 1

# La sécurité dans le monde de l'automobile

*Ce travail fût présenté en partie à la conférence des sourds-muets unijambistes à Quibéron en avril 1994.*

Maxime Ayrault

## 1.1 La révolution logicielle

Le logiciel embarqué est une des innovations clé dans le monde automobile. D'après l'article de Robert Charette (Charette 2009) paru dans IEEE Spectrum, la première voiture embarquant un logiciel était la Oldsmobile Toronado de General Motors en 1977. La Toronado avait une unité de contrôle électronique (ECU) qui gérait la synchronisation de l'allumage des bougies (spark timing). En 1978, General Motors proposait, en option sur ses Cadillacs, un ordinateur de bord qui pouvait afficher la vitesse, le niveau du réservoir d'essence, les informations sur l'état du véhicule. Ce logiciel s'exécutait sur une version modifiée du processeur Motorola 6802 et faisait 50.000 lignes de code. Depuis, de plus en plus de fonctions ont été réalisées par du logiciel. Afin de limiter le nombre de câbles dans une voiture, les capteurs ont été décentralisés et connectés à un réseau interne (réseau CAN). Le logiciel a également permis de créer de nouvelles fonctions pour les voitures.
Une voiture actuelle est maintenant devenue une plate-forme logiciel sur roues. Une voiture grand public contient entre 30 et 50 unités de contrôle électronique effectuant la gestion de multiples systèmes (voir 1.1).

| | | |
|---|---|---|
| Air bag | ABS | Système d'alarme |
| La climatisation | Le régulateur de vitesse | Le régime moteur |
| Les clignotants | Les feux | Le klaxon |
| La gestion des sièges | Le système de navigation | Le système audio |
| La pression des pneus | La gestion des portes et vitres | ... |

TABLE 1.1 – Système logiciel dans une voiture

En 2009, Alfred Katzenbach, le directeur des Technologies Informatique Chez Daimler, a annonçé que le système navigation et audio sur une Mercedes-Benz S-class contient plus 20 millions de lignes de code et que la voiture contienait pratiquement autant d'unité électronique qu'un Airbus A380 (si on exclut le système de divertissement en vol) (CHARETTE 2009). Les logiciels dans une voiture grossissent à une vitesse exponentielle en taille et en complexité. En 2010, certaines voitures avaient 10 millions de lignes de code ; an dix ans, ceci a augmenté par un facteur 15, pour environ 150 millions de lignes. Aujourd'hui, le Model S de Tesla est équipée d'un écran tactile de 17 pouces basé sur un système d'exploitation Linux qui contrôle quasiment toute les fonctions de la voiture, de la performance moteur au système audio et de navigation. En fait, il n'y a plus que 2 boutons manuel sur un Model S ; le bouton pour les feux de détresse et le bouton de la boîte à gants.
Aujourd'hui, le coût du logiciel et de l'électronique représente entre 35 à 40% du coût d'une voiture.
Il n'est pas rare que les manuels utilisateurs des voitures fassent maintenant plus de 500 pages pour expliquer l'ensemble des fonctions logiciel. On estime qu'un conducteur moyen n'utilise pas plus de 20Ceci a aussi d'importantes conséquences sur la façon d'entretenir et de réparer une voiture. On estime que plus de 50% des unités électroniques remplacées n'ont pas d'erreur (logiciel ou matériel). Le garagiste remplace la pièce simplement car il ne sait pas quelle est la cause principales de la panne. La principale activité des garagiste consiste à téécharger les nouvelles versions du logiciel. Sur les voitures Tesla, les mises à jour logiciel, qui incluent les corrections du logiciel et les nouvelles fonctionnalités sont téléchargées dans la voiture via le réseau cellulaire sans intervention d'un garagiste.

**Todo list 1** *Introduire Automotive Open System Architecture (AUTOSAR). Une solution pour réduire le coût du logiciel en augmentant l'interopérabilité entre les constructeurs.*

L'introduction du logiciel a permis d'avoir des voitures plus sûrs et moins polluantes mais a également introduit une nouvelle menace ; la *sécurité informatique des voitures.*

## 1.2 Principes de la sécurité informatique

La sécurité informatique est construite sur 3 piliers (CIA triad).


FIGURE 1.1 – Les pilers de la sécurité informatique

— La *confidentialité*. L'objectif est de protéger ou de minimiser les accés non authorisés aux données et/ou ressources sensibles (ie lecture). La technique utilisée pour garantir la confidentialité est le chiffrement. Les données sont chiffrées avec une clef connue que par les parties ayant l'autorisation de lire les données.
— L'*intégrité*. L'objectif est de protéger ou de minimiser les altérations non authorisées des données et/ou ressources sensibles (ie écriture). La technique utilisée pour garantir l'intégrité est la signature des données. Cette signature peut être effectuée en utilisant un algorithme de hash (fonction non inversible) ou une signature digitale (nécissant une clé de chifrement).
— La *disponibilité*. L'objectif est de maintenir le système opérationel pour rendre le service aux l'utilisateurs. Différentes techniques peuvent être utilisées pour garantir le systéme en opération. Elles sont regroupées sous le nom de *tolérance aux fautes*.

Dans le reste de la thèse non nous concentrerons sur la disponibilité des systèmes embarqés.

## 1.3 Le risque cybersécurité pour l'automobile

L'ajout de logiciels et de connectivité....

**Todo list 2** `https://www.nytimes.com/2015/09/27/business/complex-car-software-html` *Fear of Hacking Andy Greenberg steered a 2014 white Jeep Cherokee down a highway in St. Louis, cruising along at 70 miles per hour. Miles away, two local hackers, Charlie Miller and Chris Valasek, sat on a leather couch at Mr. Miller's house, laptops open, ready to wreak havoc.*

*As Mr. Greenberg sped along, both hands on the wheel, his ride began to go awry. First, the air-conditioning began blasting. Then an image of the hackers in tracksuits appeared on the digital display screen. Rap music began blaring at full volume, and Mr. Greenberg could not adjust the sound. The windshield wipers started and cleaning fluid sprayed, obstructing his view. Finally, the engine quit. Mr. Greenberg was on a highway with no shoulder. A big rig blew past, blaring its horn.*

*"I'm going to pull over," Mr. Greenberg said. " Because I have PTSD."*

*The episode was in fact a stunt orchestrated by the hackers and Mr. Greenberg, a writer for Wired magazine, to demonstrate the Jeep's very real vulnerabilities. The article appeared on July 21.*

*Days later, Fiat Chrysler, the maker of Jeep, announced a recall of 1.4 million vehicles to fix the flaws the hackers had identified - the first known recall intended to address a possible hacking threat.*