L'UNECE WP.29, une nouvelle règlementation cybersécurité au service d'un secteur automobile hyper-connecté

Sylvie VOTTIER

Consultante expert en stratégie, gouvernance et règlementation cybersécurité
ETAS SAS – ESCRYPT

Le volume de données échangées par les véhicules est en constante augmentation, offrant la possibilité de réaliser le diagnostic à distance, l'optimisation de la conduite, la gestion de flottes, l'émergence de nouveaux services. Dans ce contexte de véhicules hyper-connectés, intelligents et autonomes, le risque de cyber attaques est en pleine croissance. C'est pour cette raison qu'une nouvelle règlementation entrera en vigueur, en Europe, en 2022. Cette réglementation de l'UNECE WP.29 porte sur les exigences organisationnelles et techniques de cybersécurité à implémenter dans l'écosystème automobile, incluant les véhicules, les moyens de production et la supply chain. Cette réglementation impose aux constructeurs automobiles d'obtenir la certification d'un Système de Management de la Cyber Sécurité, d'un Système de Management des Mises à Jour, ainsi que la certification d'une architecture sécurisée par type de véhicule, avant sa mise en circulation.

Le secteur automobile fait face à une transformation digitale sans précèdent pour accélérer l'innovation, adapter la production, maintenir en condition de sécurité les véhicules durant leur cycle de vie et offrir de nouveaux services aux usagers. Cette transformation s'opère simultanément à trois niveaux : dans le cœur même du véhicule, au sein de l'industrie automobile (4.0), tout comme dans l'écosystème hyper-connecté, du véhicule communicant avec les autres véhicules, avec les infrastructures routières et électriques, les buildings, la city jusqu'à l'intermodalité des transports de plus en plus intelligents et les services émergeants impulsés également par la Loi d'Orientation des Mobilités.

Des évolutions qui accroissent les surfaces d'attaques cyber

Les évolutions touchent tout d'abord l'industrie automobile, avec un usage croissant d'appareils mobiles, l'IoT, la robotisation, la réalité augmentée, qui tous contiennent des données et enrichissent les services et processus présents dans le cycle de vie industriel.

A cela s'ajoute la modernisation des véhicules eux-mêmes, avec l'émergence des véhicules autonomes, des véhicules hyperconnectés et de la mobilité partagée, ainsi que la digitalisation de la Supply Chain, soit de l'écosystème automobile dans son ensemble.

Les véhicules comptent aujourd'hui plus de 150 ECU (Electronic Control Units) et environ 100 millions de lignes de code, un nombre qui atteindra les 300 millions en 2030, ce qui engendrera probablement de nombreuses vulnérabilités. A ces composants matériels et logiciels s'ajoutent les flots de données nécessaires au maintien en condition opérationnelle et de sécurité des composants, des systèmes et du véhicule. De nombreuses données sont en partie diffusées à l'extérieur du véhicule à travers des moyens de communications fournis par des tiers, pour être analysées au niveau Backend du constructeur automobile, afin d'assurer par exemple la maintenance prédictive. Les données de diagnostic pourront également être accessibles par l'After Market ou d'autres parties prenantes qui les transformeront en nouveaux services pour les usagers ou d'autres organismes.

Les informations propres au véhicule sont donc partagées avec un nombre de parties prenantes en constante augmentation qui ont des niveaux de maturité et des pratiques cybersécurité très hétérogènes.

Par conséquent, il est essentiel de prendre en compte la cybersécurité de manière transverse et au niveau de l'écosystème ; les analyses de risques tenant compte de toutes les interfaces et des interdépendances, et bien sûr devant être capables d'évaluer la criticité de toutes ces parties prenantes. L'objectif est d'être en mesure d'anticiper, de prévenir et d'éviter la gestion de crise, dans un contexte où la sécurité des personnes est primordiale, où le volume de données est considérable, où les flux de communication et les acteurs impliqués sont de plus en plus nombreux.

La convergence Information Technology (IT) et Operational Technology (OT) est inéluctable pour assurer la sécurité des données, des services émergeants, des fonctionnalités du véhicule, et des processus métier de l'automobile, et in fine la sécurité des personnes, des biens et de l'environnement. Il faut donc désormais imaginer et implémenter la sécurité de cet écosystème de manière globale, intégrant la sûreté (safety) et la cybersécurité, afin d'assurer la continuité d'activité, la résilience en cas d'incidents et la gestion de crise.

Des données qui deviennent des valeurs Métier stratégiques

Le secteur automobile qui était jusqu'à lors concentré autour de la « safety », voit aujourd'hui également des intérêts financiers à monétiser les données présentes dans le véhicule.

Ce changement de paradigme impose de catégoriser et de classifier les données présentes dans le véhicule, *et pas uniquement au regard de la data privacy*, de définir des critères autour des moyens de collecte, de distribution et d'accès à ces données, d'évaluer leur coût.

Des réglementations et des standards pour renforcer la sécurité

Dans ce contexte de complexification et d'élargissement de la surface d'attaque, des efforts sont menés dans le monde entier pour mettre en place des réglementations et définir des standards permettant d'introduire la cybersécurité dans le cycle de vie des véhicules. Pour n'en citer que quelques-unes, il y a des propositions au Congrès américain, la loi sur la cybersécurité (Cybersecurity Act) dans l'UE, le Programme ICV en Chine et les nouvelles directives de JASPAR au Japon. Parmi les standards, l'ISO/SAE DIS 21434 autour de l'ingénierie de la cybersécurité et l'ISO/AWI 24089 spécifique au système de management de la mise à jour des logiciels, auront un effet structurant

pour les constructeurs automobiles et leurs sous-traitants, qui les utiliseront comme guides d'implémentation pour la prise en compte de la cybersécurité sur tout le cycle de vie du véhicule.

La réglementation UNECE WP.29

L'UNECE WP.29* a approuvé en juin 2020 une nouvelle règlementation pour la cyber sécurité dans le monde automobile. Sa publication est attendue en décembre 2020 pour une application en juillet 2022 pour tous les nouveaux véhicules en Europe.

La réglementation porte sur la cybersécurité à la fois des véhicules, des systèmes de production et des systèmes d'information connexes, dont ceux des fournisseurs et prestataires de services. Cette réglementation, issue du groupe de travail WP.29 de l'UNECE, la Commission Economique pour l'Europe des Nations Unies, sera applicable dans les 54 pays signataires de l'accord de l'UNECE de 1958, et notamment dans tous les pays de l'Union Européenne via le règlement européen GSR** (General Safety Regulation) édicté en 2019.

La réglementation s'appliquera aux véhicules des catégories L6 et L7 à quatre roues ainsi qu'aux catégories M des véhicules conçus pour le transport de passagers, N des véhicules à moteur prévus pour le transport de marchandises, et enfin de catégorie O concernant les remorques et semi-remorques, à partir du moment où ils contiennent au moins une unité de commande électronique embarquée (ECU). Les non-conformités des véhicules pourront avoir comme effet un refus de délivrance de certificat par type de véhicule (à partir du 6 juillet 2022), voire une interdiction d'immatriculation des véhicules à partir du 7 juillet 2024. Il est à noter que contrairement à une directive, la réglementation européenne sera appliquée dans tous les pays signataires telle quelle, sans transposition dans le droit national. Cependant, chaque pays aura sa propre autorité de contrôle.

Ce que contient la réglementation UNECE WP.29

Les deux principaux axes de la réglementation portent sur le Cyber Security Management System (CSMS) et la certification du type de véhicule, ainsi que le Software Update Management System (SUMS). A cela s'ajoute l'implémentation de mesures techniques recommandées par le Règlement GSR du 27 novembre 2019, pour assurer la sécurité des informations et des systèmes à bord des véhicules contre une utilisation non-autorisée.

Cyber Security Management System

La réglementation stipule en effet que les constructeurs doivent mettre en place un Système de Management de la Cyber Sécurité (CSMS) couvrant le cycle de vie du véhicule et le cycle de production industrielle. Les constructeurs devront ensuite faire homologuer chaque type de véhicule et prouver à l'organisme certificateur qu'ils ont pris en compte la cybersécurité dès les spécifications, dans l'implémentation puis les tests, la production, les opérations, la maintenance jusqu'à la mise au rebut du véhicule.

Le système de management de la cybersécurité doit inclure des processus pour :

- Gérer la cybersécurité au niveau organisationnel et technique

- Identifier les risques pour les types de véhicules

- Evaluer, classer et traiter les risques identifiés

- Vérifier que les risques identifiés sont gérés de manière appropriée

- Tester la cybersécurité d'un type de véhicule

- Surveiller, détecter et répondre aux cyber-attaques, menaces et vulnérabilités

- Evaluer l'efficacité des mesures mises en œuvre

Le CSMS doit être audité et homologué, pour chaque type de véhicule développé par un constructeur automobile, par les autorités compétentes du pays pour assurer leur mise en œuvre de façon effective.

Software Update Management System

La réglementation impose également l'implémentation d'un Système de Management des Mises à jour des Softwares (SUMS) présents dans le véhicule, les mises à jour pouvant être réalisées à distance : Over-The Air (OTA).

Le Système de Management des Mises à jour des Softwares présents dans le véhicule assure la mise en place de processus permettant de :

- Identifier les composants logiciels et matériels

- Vérifier la compatibilité d'une version logicielle avec un système/véhicule cible

- Evaluer l'impact sur la sûreté des occupants d'une mise jour logicielle

- Assurer l'intégrité et l'authenticité des mises à jour

- Assurer la possibilité de revenir à une version antérieure si une mise à jour ne s'est pas faite correctement.

Des mesures techniques relevant du GSR

Au-delà de la mise en place des systèmes de management, des mesures techniques doivent aussi être implémentées pour assurer la sécurité de l'information et des systèmes à bord des véhicules contre une utilisation non-autorisée.

Le règlement européen GSR stipule notamment que *« La connectivité et l'automatisation des véhicules augmentent la possibilité d'accès non autorisé à distance aux données embarquées et la modification illégale de logiciels réalisée sans fil. »* et préconise donc une application des normes internationales de cybersécurité.

Le GSR donne aussi une liste de prescriptions devant être prises en compte dans le périmètre à sécuriser, notamment les systèmes à bord des véhicules.

Modalité de mise en conformité et homologation

La mise en conformité porte à la fois sur le CSMS et sur les véhicules. Les exigences de sécurité seront déportées par les constructeurs sur l'ensemble des sous-traitants (Tier 1 et Tier 2).

Certification de CSMS

La certification est délivrée par une autorité d'approbation chargée d'évaluer la conformité à la réglementation, du CSMS implémenté par le constructeur. Cette certification est valable 3 ans (renouvelée sur 3 ans en fonction des résultats de l'évaluation tri-annuelle).

Demande d'homologation d'un type de véhicule

L'homologation d'un type de véhicule passe les étapes suivantes :

- Documentation fournie par le constructeur à l'autorité d'approbation : caractéristiques du véhicule, résultats des analyses des risques, identification des éléments critiques du véhicule et de son environnement, dispositifs de sécurité en place pour mitiger les risques, résultats des tests, éléments de sécurisation de la supply chain, numéro du certificat de conformité pour le CSMS, vérification de ces éléments par l'autorité d'approbation,

- Tests du véhicule par l'autorité d'approbation,

- Contrôle sur site possible par l'autorité d'approbation.

Relation avec les autres standards de cybersécurité

La réglementation UNECE WP.29 préconise l'application des autres réglementations et standards dès leur entrée en vigueur. Parmi les autres standards applicables, on peut citer ISO/SAE 21434 (publication début 2021) and ISO/AWI 24089 (publication mars 2022) et la série ISO 27K qui permet ensuite de couvrir complètement les exigences de la règlementation en intégrant les processus relevant de la partie IT Backend ainsi que les Plans de Continuité et de Reprise d'Activités.

Au-delà de la réglementation, la transformation à venir et la sécurité dans les véhicules

La réglementation UNECE et les standards de sécurité applicables aux véhicules et aux systèmes d'information et de production contribue au développement des bonnes pratiques de sécurité chez les constructeurs et l'ensemble des acteurs de la chaine de valeur. Cet élan engendrera l'émergence de nouveaux services tels que des SOC spécialisés pour les véhicules. Il permettra aussi une généralisation et une systématisation des tests d'intrusion sur les voitures et les systèmes de l'écosystème.

Parallèlement, la protection des données collectées par les véhicules, et échangées avec des tiers pour la maintenance du véhicule et la création de nouveaux services, devient un enjeu stratégique business qui conduit d'ores et déjà les constructeurs automobiles, à imaginer de nouvelles architectures internes aux véhicules et les infrastructures externes associées. La convergence IT /OT est en marche !

---

* UNECE WP.29 https://www.unece.org/trans/main/welcwp29.html

** https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019R2144&from=CS