

Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1373

(03/2017)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION
ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Applications et services sécurisés – Sécurité des
systèmes de transport intelligents

**Capacité de mise à jour sécurisée des logiciels
pour les dispositifs de communication des
systèmes de transport intelligents**

Recommandation UIT-T X.1373

UIT-T



RECOMMANDATIONS UIT-T DE LA SÉRIE X
RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
Recommandations relatives aux infrastructures de clé publique	X.1340–X.1349
Sécurité de l'Internet des objets	X.1360–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1379
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1373

Capacité de mise à jour sécurisée des logiciels pour les dispositifs de communication des systèmes de transport intelligents

Résumé

Au fur et à mesure de l'amélioration des technologies des systèmes de transport intelligents (ITS), les communications entre un véhicule et une autre entité, par exemple les communications de véhicule à véhicule (V2V) et de véhicule à infrastructure (V2I), se généralisent et les dispositifs électriques à l'intérieur d'un véhicule, notamment les unités de commande électroniques (ECU), les systèmes de télépéage (ETC) et les systèmes de navigation routière, sont de plus en plus sophistiqués. Il en résulte qu'une mise à jour appropriée des modules logiciels présents dans ces dispositifs électriques est indispensable afin de corriger les bogues et d'améliorer la performance et la sécurité de manière à éviter des accidents graves.

Pour répondre à ce besoin, la Recommandation UIT-T X.1373 définit des procédures de mise à jour sécurisée des logiciels entre un serveur de mise à jour de logiciels et des véhicules moyennant des contrôles de sécurité appropriés. Concrètement, les constructeurs automobiles et les entreprises s'occupant de systèmes ITS peuvent utiliser cette Recommandation comme un ensemble normalisé de bonnes pratiques.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1373	30-03-17	17	11.1002/1000/13197

Mots clés

Dispositifs de communication, attaque par déni de service (DoS), système intégré, module matériel de sécurité (HSM), système de transport intelligent (ITS), logiciel malveillant, vie privée, analyse du risque, de véhicule à véhicule (V2V), de véhicule à infrastructure (V2I), de véhicule à X (véhicule/infrastructure) (V2X), communications sans fil.

* Pour accéder à la Recommandation, reporter cet URL <http://handle.itu.int/> dans votre navigateur Web, suivi de l'identifiant unique, par exemple <http://handle.itu.int/11.1002/1000/11830-en>.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT avait été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous <http://www.itu.int/ITU-T/ipr/>.

© UIT 2017

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

	Page
1	Domaine d'application 1
2	Références..... 1
3	Définitions 2
3.1	Termes définis ailleurs 2
3.2	Termes définis dans la présente Recommandation 2
4	Abréviations et acronymes 2
5	Conventions 3
6	Modèle de base pour la mise à jour à distance des logiciels 3
6.1	Modules de l'environnement ITS pour la mise à jour des logiciels..... 3
6.2	Modèle de la procédure de mise à jour des logiciels..... 5
7	Spécification de la procédure de mise à jour sécurisée des logiciels 7
7.1	Format général des messages avec des fonctions de sécurité..... 7
7.2	Définition du protocole et format des données..... 7
	Appendice I – Méthodologie d'analyse du risque 25
I.1	Méthodologie d'analyse du risque basée sur les lignes directrices [b-JASO TP15002]..... 25
I.2	Vérification des données au moyen d'algorithmes MAC 32
	Appendice II – Menaces, exigences de sécurité et contrôles de sécurité..... 33
II.1	Définition de la cible de l'évaluation 33
II.2	Identification des principales menaces 35
II.3	Exigences de sécurité pour la cible TOE..... 39
II.4	Contrôles de sécurité 41
	Bibliographie..... 44

Recommandation UIT-T X.1373

Capacité de mise à jour sécurisée des logiciels pour les dispositifs de communication des systèmes de transport intelligents

1 Domaine d'application

Dans le contexte de la mise à jour des modules logiciels des dispositifs électriques des véhicules dans l'environnement de communication des systèmes de transport intelligents (ITS), la présente Recommandation a pour objet de définir une procédure permettant de mettre à jour en toute sécurité les logiciels des dispositifs de communication ITS pour la couche application afin de prévenir les menaces telles que l'altération des dispositifs de communication des véhicules ou l'intrusion malveillante dans ces dispositifs. En particulier, elle définit un modèle de base et des contrôles de sécurité et spécifie un format de données abstrait pour la mise à jour des logiciels.

La procédure relative aux communications à l'intérieur d'un véhicule n'entre pas dans le cadre de la présente Recommandation. A toutes fins utiles, on trouvera dans la présente Recommandation, à titre d'information, une description de la procédure utilisée à l'intérieur d'un véhicule.

La procédure de mise à jour est destinée à s'appliquer aux dispositifs de communication ITS des véhicules pour des communications de véhicule à infrastructure (V2I) au moyen de l'Internet et/ou de réseaux dédiés ITS. Elle fournit des orientations techniques, sans exigences de conformité. Dans la pratique, les constructeurs automobiles et les entreprises s'occupant de systèmes ITS peuvent utiliser la procédure comme un ensemble de processus sécurisés et de contrôles de sécurité.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

- [UIT-T X.509] Recommandation UIT-T X.509 (2012) | ISO/CEI 9594-8:2014, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut.*
- [UIT-T X.1521] Recommandation UIT-T X.1521 (2011), *Système de notation des vulnérabilités courantes.*
- [ISO/CEI 15408-1] ISO/CEI 15408:2009, *Technologies de l'information – Techniques de sécurité – Critères d'évaluation pour la sécurité TI – Partie 1: Introduction et modèle général.*
- [ISO/CEI 27000] ISO/CEI 27000:2014, *Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Vue d'ensemble et vocabulaire.*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise le terme suivant défini ailleurs:

3.1.1 menace [ISO/CEI 27000]: cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un organisme.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 note de risque: note calculée par une méthode d'analyse du risque pour chaque menace.

3.2.2 passerelle mobile de véhicule (VMG, *vehicle mobile gateway*): module qui assure la communication entre les unités de commande électroniques (ECU) du réseau local de commande (CAN) (bus à l'intérieur du véhicule) et les entités extérieures de système de transport intelligent (ITS) du réseau externe.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

CA	autorité de certification (<i>certification authority</i>)
CAN	réseau local de commande (<i>controller area network</i>)
CD	disque compact (<i>compact disc</i>)
CRSS	système de notation du risque basé sur le système CVSS (<i>CVSS based risk scoring system</i>)
CVSS	système de notation des vulnérabilités courantes (<i>common vulnerability scoring system</i>)
DoS	déni de service (<i>denial of service</i>)
DVD	disque numérique polyvalent (<i>digital versatile disc</i>)
ECU	unité de commande électronique (<i>electronic control unit</i>)
ETC	télépéage (<i>electronic toll collection</i>)
FT	arbre de défaillance (<i>fault tree</i>)
GPS	système mondial de localisation (<i>global positioning system</i>)
GUID	identifiant d'utilisateur mondial (<i>global user id</i>)
HSM	module matériel de sécurité (<i>hardware security module</i>)
HTTP	protocole de transfert hypertexte (<i>hypertext transfer protocol</i>)
HTTPS	protocole de transfert hypertexte sécurisé (<i>hypertext transfer protocol secure</i>)
ID	identifiant (<i>identifier</i>)
IT	technologies de l'information, informatique (<i>information technology</i>)
ITS	système de transport intelligent (<i>intelligent transportation system</i>)
LIN	réseau local d'interconnexion (<i>local interconnect network</i>)
MAC	code d'authentification de message (<i>message authentication code</i>)
MOST	transport dans des systèmes orientés média (<i>media oriented systems transport</i>)
OBD	diagnostic à bord (<i>on-board diagnostics</i>)

OEM	fabricant d'équipements d'origine (<i>original equipment manufacturer</i>)
PC	ordinateur personnel (<i>personal computer</i>)
RPM	nombre de tours par minute (<i>revolutions per minute</i>)
RSS	système de notation du risque (<i>risk scoring system</i>)
SD	numérique sécurisé (<i>secure digital</i>)
SHA	algorithme de hachage sécurisé (<i>secure hash algorithm</i>)
SSL	couche de connecteurs sécurisés (<i>secure socket layer</i>)
TLS	sécurité dans la couche transport (<i>transport layer security</i>)
TOE	cible de l'évaluation (<i>target of evaluation</i>)
TPM	module de plate-forme fiable (<i>trusted platform module</i>)
TV	télévision
UI	interface utilisateur (<i>user interface</i>)
URL	localisateur uniforme de ressource (<i>uniform resource locator</i>)
USB	bus série universel (<i>universal serial bus</i>)
Usvr	serveur de mise à jour (<i>update server</i>)
V2I	de véhicule à infrastructure (<i>vehicle-to-infrastructure</i>)
V2V	de véhicule à véhicule (<i>vehicle-to-vehicle</i>)
V2X	de véhicule à X (véhicule/infrastructure) (<i>vehicle-to-X (vehicle/infrastructure)</i>)
VMG	passerelle mobile de véhicule (<i>vehicle mobile gateway</i>)
WiFi	fidélité sans fil (<i>wireless-fidelity</i>)
XML	langage de balisage étendu (<i>extended mark-up language</i>)

5 Conventions

Aucune.

6 Modèle de base pour la mise à jour à distance des logiciels

Afin de disposer d'une architecture de sécurité pratique, la présente section décrit un modèle de base d'architecture classique pour la mise à jour des logiciels, et définit les principaux modules et les processus types pour la mise à jour des logiciels.

6.1 Modules de l'environnement ITS pour la mise à jour des logiciels

La Figure 1 montre les principaux modules autour d'un véhicule pour la mise à jour à distance des logiciels dans l'environnement de communication ITS. Les principaux modules sont les dispositifs d'information, les unités de commande électroniques (ECU) et la passerelle mobile de véhicule à bord du véhicule (VMG), ainsi que le serveur de mise à jour (Usvr) et la base de données de journalisation du constructeur automobile et de l'équipementier. La procédure relative aux communications à l'intérieur du véhicule (par exemple, entre les unités ECU et la passerelle mobile de véhicule) n'entre pas dans le cadre de la présente Recommandation. Les modules utilisés pour les communications à l'intérieur du véhicule (notamment l'"interface utilisateur" et les "unités ECU") sont décrits ci-après à titre d'information.

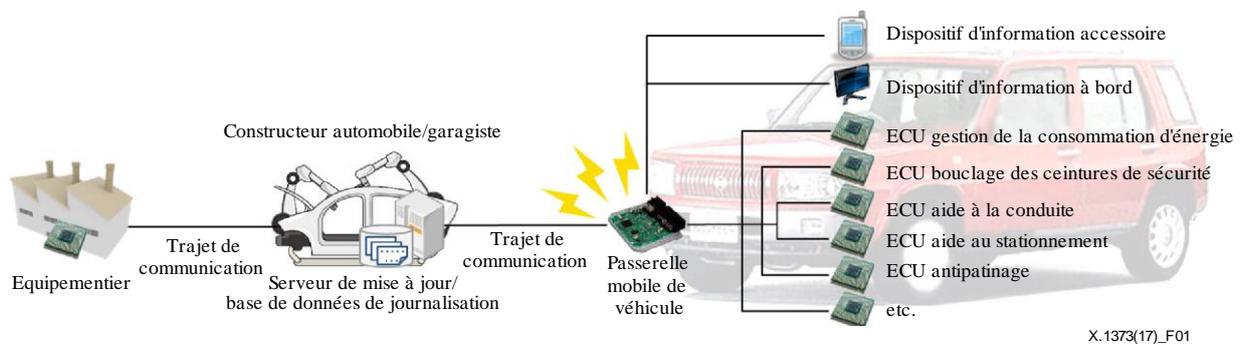


Figure 1 – Principaux modules autour d'un véhicule

6.1.1 Interface utilisateur (à titre d'information)

En règle générale, l'interface utilisateur (UI) dans un véhicule est un dispositif à bord ou un dispositif accessoire permettant d'afficher et de saisir des informations. Ce type de dispositif d'information est connecté directement à d'autres dispositifs du véhicule (par exemple la passerelle VMG ou les unités ECU (voir le § 6.1.2)) de manière à pouvoir obtenir et indiquer diverses informations d'état du véhicule, comme la vitesse, le nombre de tours par minute (RPM), le niveau de carburant, etc. En particulier, dans la présente Recommandation, l'interface utilisateur est utilisée pour informer les automobilistes lorsque des mises à jour sont nécessaires.

6.1.2 Unité de commande électronique (ECU) (à titre d'information)

ECU est un terme générique désignant les ordinateurs qui commandent divers types de dispositifs dans un véhicule. Au départ, l'unité ECU avait pour principales fonctions de commander l'instant d'allumage, l'injection, le réglage du ralenti et le limiteur de moteur afin de réduire la consommation de carburant et les émissions de gaz. Au fur et à mesure de l'informatisation des véhicules, les applications de l'unité ECU se sont multipliées et concernent notamment la gestion de la consommation d'énergie, le bouclage des ceintures de sécurité, l'aide à la conduite, l'aide au stationnement, l'antipatinage, la transmission automatique, etc. Ces dernières années, le nombre d'unités ECU dans un véhicule est passé de 50 à 100, et l'importance des unités ECU s'accroît notamment pour les contrôles et les communications de sécurité. Toutefois, le développement des unités ECU fait intervenir des mises en oeuvre logicielles sophistiquées, si bien que l'augmentation récente du nombre d'unités ECU dans les véhicules impose de lourdes contraintes aux constructeurs automobiles.

6.1.3 Passerelle mobile de véhicule

Une passerelle mobile de véhicule est un module servant d'interface avec le "serveur de mise à jour" (voir le § 6.1.4) pour la mise à jour des logiciels du véhicule. Le processus de mise à jour des logiciels opéré dans le véhicule n'entre pas dans le cadre de la présente Recommandation. La passerelle VMG est une entité théorique qui peut être mise en oeuvre dans la pratique à l'aide d'un ensemble de plusieurs composants. Par exemple, l'entité de gestion de connexion (également appelée "passerelle centrale", "unité principale", "unité principale de communication" ou "passerelle de véhicule (VG)") peut jouer le rôle de passerelle VMG dans ce contexte, et différents dispositifs peuvent aussi être utilisés pour la mise à jour des logiciels. Le trajet de communication entre la passerelle mobile de véhicule et les entités ITS extérieures utilise un réseau cellulaire (réseau mobile) et un réseau fixe avec accès sans fil.

6.1.4 Serveur de mise à jour et base de données de journalisation

Un serveur de mise à jour, installé chez le constructeur automobile ou le garagiste, collecte les informations d'état des modules logiciels du véhicule et distribue les modules de mise à jour des logiciels au véhicule. Par ailleurs, avec les ordinateurs connectés les plus récents tels que les ordinateurs personnels (PC) et les smartphones, l'une des fonctions importantes du serveur de mise à

jour consiste à gérer et à contrôler la totalité des logiciels du véhicule. Afin de gérer automatiquement l'état des logiciels du véhicule, le serveur de mise à jour devrait fonctionner en s'appuyant sur une base de données de journalisation dans laquelle sont stockées les informations d'état des logiciels du véhicule. Il est à noter qu'un serveur de mise à jour peut être installé non seulement chez le constructeur automobile mais aussi chez un équipementier ou un tiers.

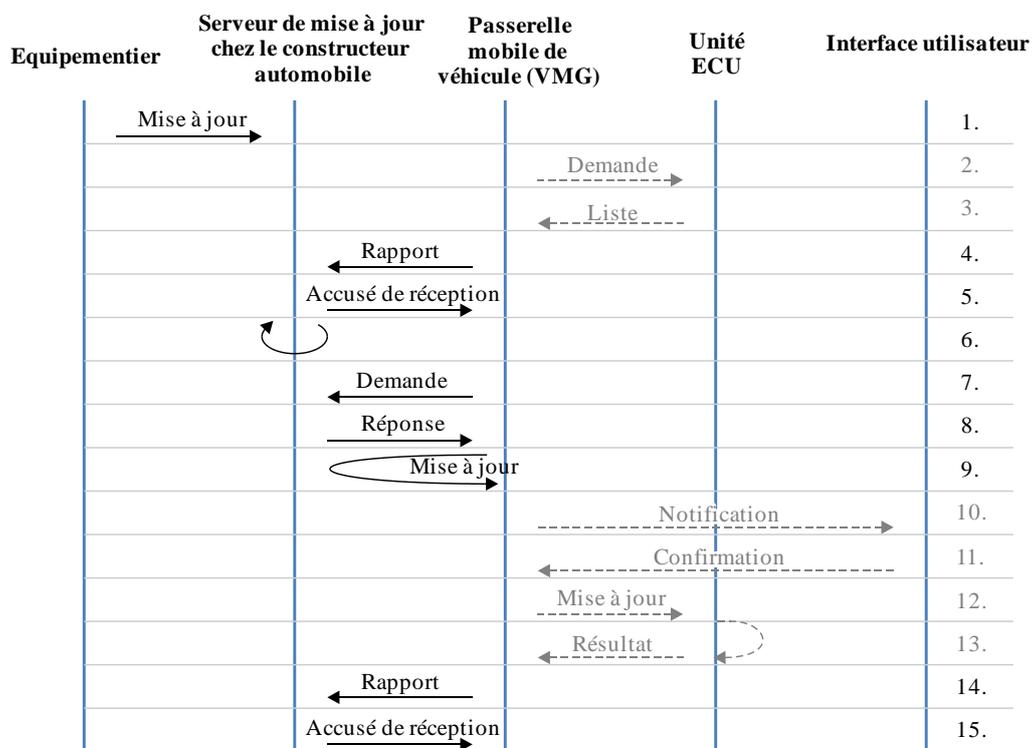
6.1.5 Equipementier

Un véhicule est un assemblage de milliers de pièces automobiles fournies par des équipementiers automobiles. Ces équipementiers fournissent les dispositifs de communication à bord et les unités ECU et le constructeur automobile les assemble tout en prenant en considération les dépendances entre les divers dispositifs. Par conséquent, et en règle générale, les modules de mise à jour des dispositifs de communication à bord ne sont pas produits au préalable par le constructeur automobile, mais par les équipementiers correspondants. Le constructeur automobile teste et évalue avec soin les modules de mise à jour fournis avant de les distribuer au véhicule.

6.2 Modèle de la procédure de mise à jour des logiciels

6.2.1 Procédure générale de mise à jour

La Figure 2 montre un modèle type de la procédure de mise à jour des logiciels, que la passerelle mobile de véhicule lance après avoir vérifié qu'il existe des mises à jour. Etant donné que les communications à l'intérieur du véhicule n'entrent pas dans le cadre de la présente Recommandation, les étapes de la Figure 2 relatives aux communications à l'intérieur du véhicule sont simplement des exemples donnés à titre d'information qui pourront être pris en compte pour la mise en oeuvre pratique de la procédure de mise à jour sécurisée.



X.1373(17) F02

Figure 2 – Modèle de la procédure de mise à jour des logiciels

Les étapes de la procédure de mise à jour sont décrites ci-après, les étapes 2, 3 et 10 à 13 (en italique) étant données à titre d'information:

- 1) En premier lieu, un module de mise à jour est fourni par un équipementier automobile, cette fourniture n'étant pas synchronisée avec les étapes suivantes.
- 2) *Au moment de lancer la procédure de mise à jour, la passerelle mobile de véhicule (VMG) demande aux unités ECU de soumettre leur liste de logiciels.*
- 3) *Chaque unité ECU vérifie l'état de ses logiciels, génère une liste des modules logiciels et la transmet à la passerelle VMG.*
- 4) La passerelle VMG soumet la liste obtenue au serveur de mise à jour pour vérifier s'il existe des mises à jour pour le véhicule.
- 5) Le serveur de mise à jour envoie à la passerelle VMG un accusé de réception de la liste soumise.
- 6) A partir de la liste, le serveur de mise à jour inspecte l'état des logiciels installés dans le véhicule et détermine les mises à jour des logiciels qu'il faut apporter aux unités ECU.
- 7) Etant donné que cette inspection peut durer longtemps, la passerelle VMG vérifie périodiquement si des mises à jour sont nécessaires pour le véhicule.
- 8) S'il existe des mises à jour à apporter, le serveur de mise à jour envoie les URL d'accès aux mises à jour; dans le cas contraire, il envoie uniquement un message d'acquittement.
- 9) S'il existe des mises à jour pour le véhicule, la passerelle VMG se connecte au serveur de mise à jour pour télécharger les modules de mise à jour pour le véhicule.
- 10) *Avant d'installer les mises à jour dans les unités ECU, la passerelle VMG informe le conducteur qu'il doit confirmer l'installation des mises à jour.*
- 11) *Le conducteur confirme et accepte l'installation des mises à jour.*
- 12) *La passerelle VMG transmet les fichiers de mise à jour aux unités ECU correspondantes et leur demande d'installer les mises à jour (voir le § 6.2.3).*
- 13) *Chaque unité ECU installe la mise à jour et rend compte du résultat de l'installation à la passerelle VMG.*
- 14) La passerelle VMG soumet au serveur de mise à jour un rapport sur les résultats de l'installation.
- 15) Enfin, le serveur de mise à jour envoie un accusé de réception des informations de mise à jour. Si l'installation des mises à jour a échoué ou s'il reste certaines mises à jour à installer, de nouvelles tentatives d'exécution des étapes 6 à 14 ont lieu jusqu'au succès de l'installation (voir le § 6.2.2).

6.2.2 Considérations relatives au nombre illimité de nouvelles tentatives

En ce qui concerne le principe des nouvelles tentatives jusqu'à ce qu'il y ait succès, décrit à l'étape 15, il est à noter que, dans certains cas, la procédure n'aboutira jamais, auquel cas on aura un nombre illimité de nouvelles tentatives au niveau de la passerelle VMG. Pour éviter cette situation, il convient de fixer une limite "N" au nombre de tentatives, que l'on peut déterminer sur la base de la politique relative à la procédure de mise à jour. Les modalités de définition de la politique relative à la mise à jour n'entrent pas dans le cadre de la présente Recommandation.

6.2.3 Considérations relatives aux ressources limitées

En ce qui concerne l'installation du logiciel de mise à jour dans un véhicule (étape 12 donnée à titre d'information au § 6.2.1), certains modules dans le véhicule ne disposent pas d'une ressource mémoire suffisante pour mettre en mémoire cache tout un module de mise à jour en une fois. Pour ces modules, il est nécessaire d'utiliser la technologie de mise à jour par flux, et de transmettre les données fragmentées en streaming.

D'une manière générale, quels que soient les modules dans un véhicule et le système de mise à jour les contraintes liées aux ressources limitées des dispositifs, notamment en termes de mémoire, de stockage et de débit du réseau, devraient être dûment prises en considération.

7 Spécification de la procédure de mise à jour sécurisée des logiciels

La présente section définit une procédure pratique et les formats des messages d'application associés entre le serveur de mise à jour et le véhicule (passerelle VMG) pour la mise à jour des logiciels avec des fonctions de sécurité. Il est à noter que la présente Recommandation ne définit pas de fonctions pour la confidentialité des messages. La confidentialité peut être assurée par des protocoles de couche inférieure (par exemple le protocole de transfert hypertexte sécurisé (HTTPS) et le protocole de tunnellation sécurisé, etc.).

La procédure doit tenir compte de la diversité des capacités de sécurité parmi les véhicules. La présente Recommandation prévoit donc que les véhicules utilisant un algorithme de chiffrement asymétrique appliquent la méthode de la signature numérique (§ 7.1.1), tandis que les véhicules n'utilisant pas d'algorithme de chiffrement asymétrique appliquent la méthode reposant sur un code d'authentification de message (MAC) (§ 7.1.2) pour l'échange sécurisé des messages.

7.1 Format général des messages avec des fonctions de sécurité

Le présent paragraphe décrit le format général des messages avec des fonctions de sécurité, y compris une méthode d'authentification de l'expéditeur d'un message et la vérification de l'intégrité du message. S'agissant de la technique utilisée pour l'intégrité et l'authenticité, on peut appliquer la méthode de la signature numérique avec un algorithme à clé publique et/ou un code d'authentification de message avec un algorithme à clé partagée. Dans la procédure de mise à jour sécurisée des logiciels, il convient d'employer l'une des méthodes de sécurité suivantes pour la construction de chaque message.

7.1.1 Méthode de la signature numérique

Parmi les méthodes de mise en oeuvre, on peut appliquer la signature numérique basée sur la Recommandation [UIT-T X.509] pour l'authentification des entités et la vérification de l'intégrité des messages dans les véhicules dotés d'une capacité de chiffrement asymétrique offerte par un module matériel de sécurité (HSM) (par exemple un module TPM).

7.1.2 Méthode MAC

Etant donné que l'algorithme à clé partagée nécessite une charge de traitement moins importante que l'algorithme à clé publique, il convient pour les dispositifs ayant une faible capacité de traitement. Toutefois, dans l'algorithme à clé partagée, l'expéditeur et le destinataire utilisent la même clé, si bien qu'un grand nombre de dispositifs utilisent la même clé. En cas de fuite de la clé partagée, il faut alors mettre à jour les clés dans tous les dispositifs du système. En outre, étant donné que la clé partagée proprement dite n'assure pas l'authenticité de l'expéditeur, chaque message doit contenir un identifiant de dispositif de l'expéditeur, ce qui suppose l'absence de manipulation incorrecte de l'identifiant du dispositif.

7.2 Définition du protocole et format des données

Le format des données d'application vise à transmettre des messages qui concernent uniquement la mise à jour de logiciels, conformément au format général des messages décrit au paragraphe précédent. Dans le présent paragraphe, on trouvera d'abord une définition des types de message utilisés dans la procédure de mise à jour des logiciels, puis une présentation des spécifications des types de message. Des exemples de messages sont donnés en format XML (langage de balisage étendu) à titre d'information.

7.2.1 Aperçu du protocole

Sur la base du modèle de procédure de mise à jour des logiciels décrit dans la section 6, les messages sont classés en différents types en fonction de leurs objectifs, comme illustré dans la Figure 3. Les procédures de communication à l'intérieur du véhicule n'entrent pas dans le cadre de la présente Recommandation et apparaissent en caractères gris dans la Figure 3.

NOTE – La procédure de communication à l'intérieur du véhicule fait l'objet des normes [b-ISO 14229] et [b-ISO 13440].

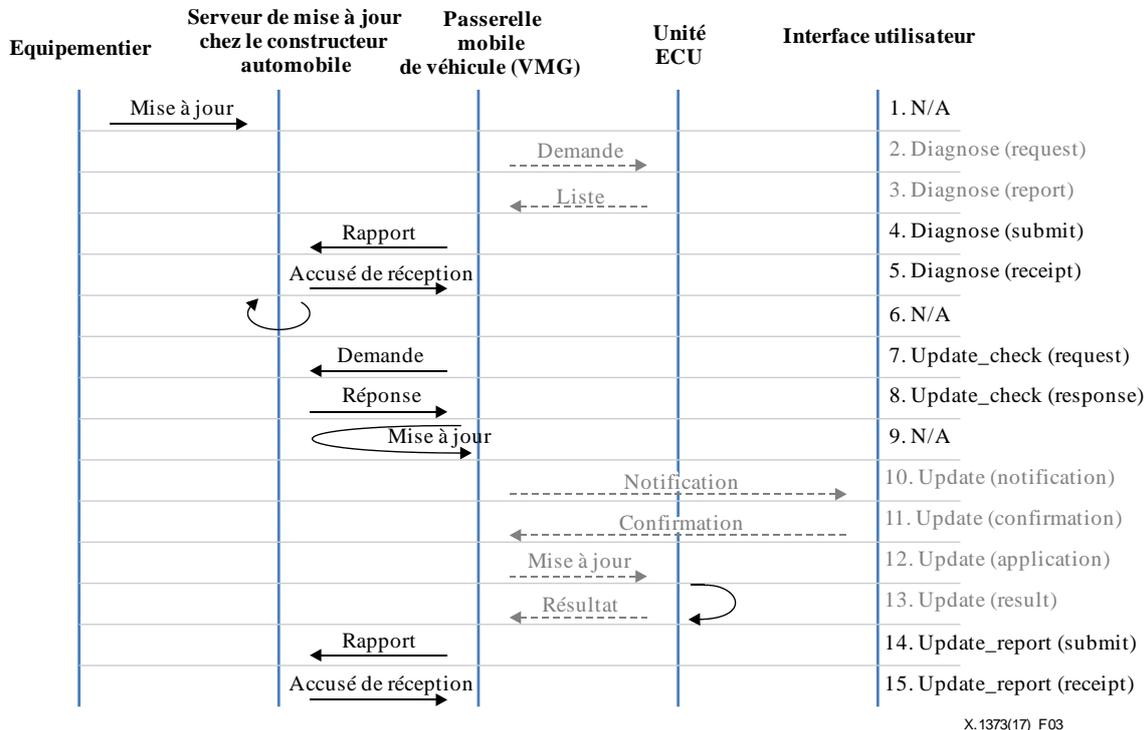


Figure 3 – Définition des types de message

Aux étapes 2, 3, 4 et 5, étant donné que les messages ont pour objet de demander et de transmettre des diagnostics de l'état des logiciels de chaque unité ECU, ils sont classés comme étant de type "diagnose" (*diagnostic*). De la même manière, aux étapes 7 et 8, les messages sont classés comme étant de type "update_check" (*vérification de mise à jour*). Aux étapes 10, 11, 12 et 13, les messages visent à confirmer et installer des mises à jour et sont donc de type "update" (*mise à jour*). Enfin, les résultats des mises à jour sont soumis dans des messages de type "update_report" (*rapport de mise à jour*) aux étapes 14 et 15. Les types, sous-types et codes des messages sont indiqués dans le Tableau 1.

Tableau 1 – Types de message

Type	Sous-type	De	A	Objet
diagnose	<i>request</i>	<i>VMG</i>	<i>ECU</i>	<i>Demande de diagnostic de l'état des logiciels</i>
	<i>report</i>	<i>ECU</i>	<i>VMG</i>	<i>Résultat du diagnostic indiquant l'état des logiciels</i>
	<i>submit</i>	<i>VMG</i>	<i>Usvr</i>	<i>Rapport des résultats pour les unités ECU d'un véhicule</i>
	<i>receipt</i>	<i>Usvr</i>	<i>VMG</i>	<i>Accusé de réception du rapport de diagnostic</i>
update_check	<i>request</i>	<i>VMG</i>	<i>Usvr</i>	<i>Demande de module de mise à jour</i>
	<i>response</i>	<i>Usvr</i>	<i>VMG</i>	<i>Module de mise à jour fourni</i>
update	<i>notification</i>	<i>VMG</i>	<i>UI</i>	<i>Message de notification pour présenter la mise à jour au conducteur</i>
	<i>confirmation</i>	<i>UI</i>	<i>VMG</i>	<i>Message de confirmation du conducteur pour installer la mise à jour</i>
	<i>application</i>	<i>VMG</i>	<i>ECU</i>	<i>Message de demande comprenant le module de mise à jour</i>
	<i>result</i>	<i>ECU</i>	<i>VMG</i>	<i>Résultat de l'installation du module de mise à jour</i>
update_report	<i>submit</i>	<i>VMG</i>	<i>Usvr</i>	<i>Rapport d'installation de la mise à jour</i>
	<i>receipt</i>	<i>Usvr</i>	<i>VMG</i>	<i>Accusé de réception du rapport</i>
* Usvr: Serveur de mise à jour * UI: Interface utilisateur				

NOTE – Dans le Tableau 1, les caractères gris en italique sont utilisés pour indiquer les éléments qui sortent du cadre de la présente Recommandation et qui sont présentés à titre d'information.

7.2.2 Messages diagnose

Afin de déterminer les modules de mise à jour nécessaires pour un véhicule, des messages diagnose sont utilisés entre un serveur de mise à jour et la passerelle VMG pour charger dans le serveur de mise à jour des informations sur les logiciels du véhicule.

7.2.2.1 Message diagnose (submit)

Après avoir rassemblé les résultats de diagnostic du véhicule, la passerelle VMG soumet une liste d'informations sur les logiciels au serveur de mise à jour situé chez le constructeur (ou chez le garagiste). Le message diagnose (submit) inclut l'identité du véhicule (vid) et une liste d'informations sur les logiciels qui est extraite des messages diagnose (report).

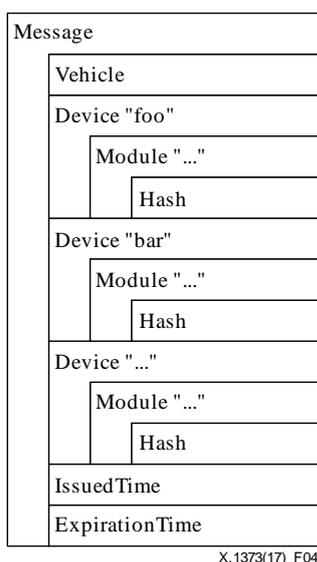


Figure 4 – Structure du message diagnose (submit)

Tableau 2 – Eléments du message diagnose (submit)

Elément	Attribut de l'élément	Description
Message	–	Conteneur du message.
	protocol	Toujours "1.0".
	version	Numéro de version de l'expéditeur du message.
	type	Type de message (toujours "diagnose").
	subtype	Sous-type de message (toujours "submit").
	sessionid	L'identifiant de session est un identifiant d'utilisateur mondial (GUID) aléatoire associé à la session de diagnostic. Un même identifiant de session est utilisé pour une série de messages diagnose (request, report, submit et receipt).
	trustlevel	Le niveau de confiance est déterminé sur la base de la capacité de sécurité et de l'exigence de sécurité du dispositif qui a généré ce message.
	ownerid	Identifiant du propriétaire fourni par le constructeur automobile/l'équipementier.
	messageid	L'identifiant de message est un identifiant GUID aléatoire associé à un message spécifique.
Vehicle	–	Conteneur d'informations sur le véhicule. Il contient plusieurs éléments de module.
	name	Nom du véhicule, le cas échéant.
	model	Nom du modèle du véhicule fourni par le constructeur automobile.
	modelid	Nom du modèle du véhicule.
	vehicleid	Identifiant du véhicule défini par le constructeur automobile/l'équipementier.
	locale	Informations de localisation du véhicule
Device	–	Conteneur d'informations sur le dispositif. Il contient plusieurs éléments de module.

Tableau 2 – Eléments du message diagnose (submit)

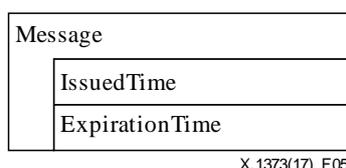
Elément	Attribut de l'élément	Description
	name	Nom du dispositif, le cas échéant.
	type	Nom du type de dispositif, par exemple "ECU gestion de la consommation d'énergie", "ECU bouclage des ceintures de sécurité", etc.
	model	Nom du modèle du dispositif.
	deviceid	Identifiant du dispositif défini par le constructeur automobile/l'équipementier.
	hwversion	Version de ce module matériel
Module	–	Conteneur d'informations sur le module, qui contient un élément de hachage.
	moduleid	L'identifiant de module est un identifiant unique fourni par le constructeur automobile/l'équipementier.
	version	Version de ce module logiciel.
	nextversion	Version de la mise à jour du module en cours, principalement utilisée pour envoyer un message de réponse pendant une mise à jour.
Hash	–	Conteneur dans lequel figurent une valeur de hachage et des informations sur l'algorithme de hachage.
	algorithm	Algorithme de la fonction de hachage (par exemple SHA-3, SHA-256, etc.).
IssuedTime	–	Heure de génération de ce message.
ExpirationTime	–	Heure d'expiration de ce message.

Tableau 3 – Exemple de message diagnose (submit)

```
<message protocol="1.0" version="1.0.2" type="diagnose" subtype="submit"
sessionid="{7316A97D-8C04-428B-B498-0F51087A1093}" ownerid="oid987239487"
messageid="{BBCE3B0B-2A10-443A-97D0-EF4650457422}" trustlevel="3">
  <Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale="CH"/>
  <Device name="device1" type="ECU" model="modell1" id="did0987234"
hwversion="HB-01">
    <Module moduleid="{66E6F81E-F293-4531-B2FC-A93F177373AA}"
version="1.3.23.0" nextversion=""/>
    <Hash algorithm="SHA-256">hash data here</Hash>
  </Module>
  <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion=""/>
    <Hash algorithm="SHA-256">hash data here</Hash>
  </Module>
</Device>
  <Device name="device2" type="ECU" model="modell1" id="did0987234"
hwversion="HC-02">
    <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion=""/>
    <Hash algorithm="SHA-256">hash data here</Hash>
  </Module>
</Device>
  <IssuedTime "1903-07-01T00:00:00Z"/>
  <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

7.2.2.2 Message diagnose (receipt)

Après le chargement des informations sur les logiciels du véhicule à l'aide d'un message diagnose (submit), le serveur de mise à jour envoie un accusé de réception à l'aide d'un message diagnose (receipt) afin d'indiquer au véhicule que la soumission a été menée à bien et que le véhicule peut passer à l'état suivant (update_check).



X.1373(17)_F05

Figure 5 – Structure du message diagnose (receipt)

Tableau 4 – Eléments du message diagnose (receipt)

Elément	Attribut de l'élément	Description
Message	–	Conteneur du message.
	protocol	Toujours "1.0".
	version	Numéro de version de l'expéditeur du message.
	type	Type de message (toujours "diagnose").
	subtype	Sous-type de message (toujours "receipt").
	sessionid	L'identifiant de session est un identifiant GUID aléatoire associé à la session de diagnostic. Un même identifiant de session est utilisé pour une série de messages diagnose (request, report, submit et receipt).

Tableau 4 – Éléments du message diagnose (receipt)

Élément	Attribut de l'élément	Description
	trustlevel	Le niveau de confiance est déterminé sur la base de la capacité de sécurité et de l'exigence de sécurité du dispositif qui a généré ce message.
	ownerid	Identifiant du propriétaire fourni par le constructeur automobile/l'équipementier.
	messageid	L'identifiant de message est un identifiant GUID aléatoire associé à un message spécifique.
	status	Acquittement du rapport soumis dans le message diagnose (submit)
IssuedTime	–	Heure de génération de ce message.
ExpirationTime	–	Heure d'expiration de ce message.

Tableau 5 – Exemple de message diagnose (receipt)

```

<message protocol="1.0" version="1.0.2" type="diagnose" subtype="receipt"
sessionid="{7316A97D-8C04-428B-B498-0F51087A1093}" ownerid="oid987239487"
messageid="{E313159C-2081-4A10-B61D-4F81D074D54F}" trustlevel="3"
status="yes">
  <IssuedTime "1903-07-01T00:00:00Z"/>
  <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>

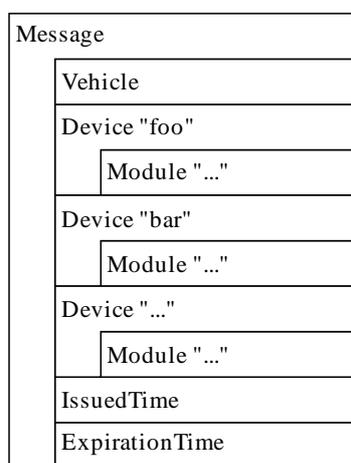
```

7.2.3 Messages update_check

Après que des informations sur les logiciels ont été chargées dans le serveur de mise à jour à l'aide de messages diagnose, le serveur de mise à jour commence l'analyse pour déterminer les modules de mise à jour nécessaires pour le véhicule, ce qui peut prendre beaucoup de temps. Des messages update_check sont envoyés périodiquement pour obtenir des renseignements sur la décision du serveur de mise à jour. Il existe deux sous-types de message update_check, request et response, qui sont transférés entre la passerelle VMG et le serveur de mise à jour.

7.2.3.1 Message update_check (request)

Le message update_check (request) est transféré de la passerelle VMG au serveur de mise à jour pour vérifier si des mises à jour sont nécessaires. Ce message comprend des informations sur les modules à inspecter, qui sont très similaires à celles figurant dans le message diagnose (receipt).



X.1373(17)_F06

Figure 6 – Structure du message update_check (request)

Tableau 6 – Eléments du message update_check (request)

Elément	Attribut de l'élément	Description
Message	–	Conteneur du message.
	protocol	Toujours "1.0".
	version	Numéro de version de l'expéditeur du message.
	type	Type de message (toujours "update_check").
	subtype	Sous-type de message (toujours "request").
	sessionid	L'identifiant de session est un identifiant GUID aléatoire associé à la session de vérification des mises à jour. Un même identifiant de session est utilisé pour une série de messages update_check (request et response).
	trustlevel	Le niveau de confiance est déterminé sur la base de la capacité de sécurité et de l'exigence de sécurité du dispositif qui a généré ce message.
	ownerid	L'identifiant de propriétaire est fourni par le constructeur automobile/l'équipementier.
	messageid	L'identifiant de message est un identifiant GUID aléatoire associé à un message spécifique.
Vehicle	–	Conteneur d'informations sur le véhicule. Il contient plusieurs éléments de module.
	name	Nom du véhicule, le cas échéant.
	model	Nom du modèle du véhicule fourni par le constructeur automobile.
	modelid	Nom du modèle du véhicule.
	vehicleid	Identifiant du véhicule défini par le constructeur automobile/l'équipementier.
	locale	Informations de localisation du véhicule
Device	–	Conteneur d'informations sur le dispositif. Il contient plusieurs éléments de module.
	name	Nom du dispositif, le cas échéant.

Tableau 6 – Eléments du message update_check (request)

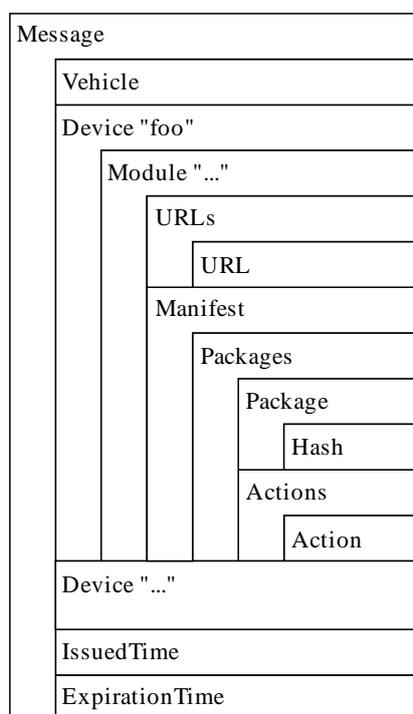
Elément	Attribut de l'élément	Description
	type	Nom du type de dispositif, par exemple "ECU gestion de la consommation d'énergie", "ECU bouclage des ceintures de sécurité", etc.
	model	Nom du modèle du dispositif.
	deviceid	Identifiant du dispositif défini par le constructeur automobile/l'équipementier.
	hwversion	Version de ce module matériel
Module	–	Conteneur d'informations sur le module, qui contient un élément de hachage.
	moduleid	L'identifiant de module est un identifiant unique fourni par le constructeur automobile/l'équipementier.
	version	Version de ce module logiciel.
	nextversion	Version de la mise à jour du module en cours, principalement utilisée pour envoyer un message de réponse pendant une mise à jour.
IssuedTime	–	Heure de génération de ce message.
ExpirationTime	–	Heure d'expiration de ce message.

Tableau 7 – Exemple de message update_check (request)

```
<message protocol="1.0" version="1.0.2" type="update_check" subtype="request"
sessionid="{19622672-A025-4500-B26A-BB626BC61C62}" ownerid="oid987239487"
messageid="{4604A6C9-F72F-452B-ABA5-94168CCD8FD6}" trustlevel="3">
  <Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale="CH"/>
  <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion="HB-01">
    <Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}"
version="1.3.23.0" nextversion=""/>
    <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion=""/>
  </Device>
  <Device name="device2" type="ECU" model="model1" id="did0987234"
hwversion="HC-02">
    <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion=""/>
  </Device>
  <IssuedTime "1903-07-01T00:00:00Z"/>
  <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

7.2.3.2 Message update_check (response)

En réponse à un message update_check (request), le serveur de mise à jour retourne le résultat de l'inspection. Si des mises à jour sont nécessaires pour certains modules du véhicule, le message update_check (response) donne les adresses URL à utiliser pour obtenir les modules de mise à jour. Il est à noter que ce message ne contient pas de fichier binaire du module de mise à jour proprement dit, mais que la passerelle VMG télécharge le module à l'aide d'une autre connexion basée sur les informations de ressource figurant dans le message update_check (response).



X.1373(17) F07

Figure 7 – Structure du message update_check (response)

Tableau 8 – Eléments du message update_check (response)

Elément	Attribut de l'élément	Description
Message	–	Conteneur du message.
	protocol	Toujours "1.0".
	version	Numéro de version de l'expéditeur du message.
	type	Type de message (toujours "update_check").
	subtype	Sous-type de message (toujours "response").
	sessionid	L'identifiant de session est un identifiant GUID aléatoire associé à la session de vérification des mises à jour. Un même identifiant de session est utilisé pour une série de messages update_check (request et response).
	trustlevel	Le niveau de confiance est déterminé sur la base de la capacité de sécurité et de l'exigence de sécurité du dispositif qui a généré ce message.
	ownerid	Identifiant du propriétaire fourni par le constructeur automobile/l'équipementier.
	messageid	L'identifiant de message est un identifiant GUID aléatoire associé à un message spécifique.
Vehicle	–	Conteneur d'informations sur le véhicule. Il contient plusieurs éléments de module.
	name	Nom du véhicule, le cas échéant.
	model	Nom du modèle du véhicule fourni par le constructeur automobile.
	modelid	Nom du modèle du véhicule.

Tableau 8 – Eléments du message update_check (response)

Elément	Attribut de l'élément	Description
	vehicleid	Identifiant du véhicule défini par le constructeur automobile/l'équipementier.
	locale	Informations de localisation du véhicule
Device	–	Conteneur d'informations sur le dispositif. Il contient plusieurs éléments de module.
	name	Nom du dispositif, le cas échéant.
	type	Nom du type de dispositif, par exemple "ECU gestion de la consommation d'énergie", "ECU bouclage des ceintures de sécurité", etc.
	model	Nom du modèle du dispositif.
	deviceid	Identifiant du dispositif défini par le constructeur automobile/l'équipementier.
	hwversion	Version de ce module matériel
Module	–	Conteneur d'informations sur le module, qui contient un élément de hachage.
	moduleid	L'identifiant de module est un identifiant unique fourni par le constructeur automobile/l'équipementier.
	version	Version de ce module logiciel.
	nextversion	Version de la mise à jour du module en cours, principalement utilisée pour envoyer un message de réponse pendant une mise à jour.
	status	Etat de l'inspection des mises à jour. Mis à "noupdate" s'il n'existe pas de mises à jour pour ce module et à "ok" s'il en existe.
URLs	–	Conteneur d'éléments d'adresse URL s'il existe des mises à jour. Cet élément figure dans un élément de module lorsque l'état est "ok".
URL	–	Adresse URL du fichier de mise à jour. Il devrait y avoir au moins deux éléments d'adresse URL, afin d'indiquer le serveur de secours correspondant à la première adresse URL. Le nombre maximal d'éléments d'adresse URL devrait être déterminé avec soin, compte tenu des ressources de calcul de la passerelle VMG.
	codebase	Emplacement du fichier de mise à jour.
Manifest	–	Décrit le module à installer, et les actions à réaliser avec les fichiers en question.
	version	Numéro propre à la nouvelle version de ce module logiciel.
Packages	–	Ensemble des fichiers à installer. Ne contient pas d'attributs. Contient un ou plusieurs éléments enfants.
Package	–	Un seul fichier à installer pour le module.
	name	Décrit le nom du fichier du module de mise à jour.
	size	Donne la taille en octets du module de mise à jour.
	description	Description du module de mise à jour.
Hash	–	Conteneur dans lequel figurent une valeur de hachage et des informations sur l'algorithme de hachage.

Tableau 8 – Eléments du message update_check (response)

Elément	Attribut de l'élément	Description
	algorithm	Algorithme de la fonction de hachage (par exemple SHA-3, SHA-256, etc.).
Actions	–	Actions à réaliser pour installer le module une fois que tous les fichiers requis (packages) ont été téléchargés avec succès.
Action	–	Une seule action à réaliser dans le cadre du processus d'installation.
	event	Chaîne fixe indiquant quand cette action doit être exécutée. Mis à "preinstall", "install", "postinstall" ou "update".
	arguments	Arguments à transmettre au processus d'installation.
IssuedTime	–	Heure de génération de ce message.
ExpirationTime	–	Heure d'expiration de ce message.

Tableau 9 – Exemple de message update_check (response)

```
<message protocol="1.0" version="1.0.2" type="update_check" subtype="response "
sessionid="{19622672-A025-4500-B26A-BB626BC61C62}" ownerid="oid987239487"
messageid="{4604A6C9-F72F-452B-ABA5-94168CCD8FD6}" trustlevel="3">
  <Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale="CH"/>
  <Device name="device1" type="ECU" model="modell1" id="did0987234"
hwversion="HB-01">
    <Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}"
version="1.3.23.0" nextversion="" status="ok">
      <Urls>
        <Url
codebase="http://update1.server/this/is/an/example/url/" />
        <Url
codebase="http://update2.server/this/is/an/example/url/" />
        <Url
codebase="http://update3.server/this/is/an/example/url/" />
      </Urls>
      <Manifest version="1.4.0">
        <Packages>
          <Package name="module1.bin" size="589" description="This
update provides...">
            <Hash algorithm="SHA-256">hash data here</Hash>
          </Package>
        </Packages>
        <Actions>
          <Action arguments="--argument-for-installation"
event="install" />
        </Actions>
      </Manifest>
    </Module>
    <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion="" status="noupdate">
    </Module>
  </Device>
  <Device name="device2" type="ECU" model="modell1" id="did0987234"
hwversion="HC-02">
    <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion="" status="noupdate">
    </Module>
  </Device>
  <IssuedTime "1903-07-01T00:00:00Z" />
  <ExpirationTime "1903-07-01T00:00:00Z" />
</message>
```

7.2.4 Messages update

Le processus de mise à jour effectué dans le véhicule n'entrant pas dans le cadre de la présente Recommandation, celle-ci ne contient ni définition ni spécification des messages update.

7.2.5 Messages update_report

La dernière étape de la procédure de mise à jour consiste pour la passerelle VMG à soumettre au serveur de mise à jour tous les rapports collectés sur l'installation des mises à jour dans les dispositifs de manière à ce que le serveur de mise à jour puisse avoir accès aux informations sur chaque véhicule depuis un site distant et puisse gérer ces informations. La passerelle VMG envoie un rapport au serveur de mise à jour via le message update_report (submit). Enfin, le serveur de mise à jour envoie un accusé de réception du rapport (message update_report (receipt)) à la passerelle VMG pour lui indiquer la fin de la procédure globale de mise à jour.

7.2.5.1 Message update_report (submit)

Après avoir collecté les rapports sur l'installation des mises à jour auprès des dispositifs, la passerelle VMG envoie un message update_report (submit) au serveur de mise à jour. Ce message comprend les résultats de l'installation des mises à jour ainsi que l'état actuel des logiciels comme dans le message diagnose (submit).

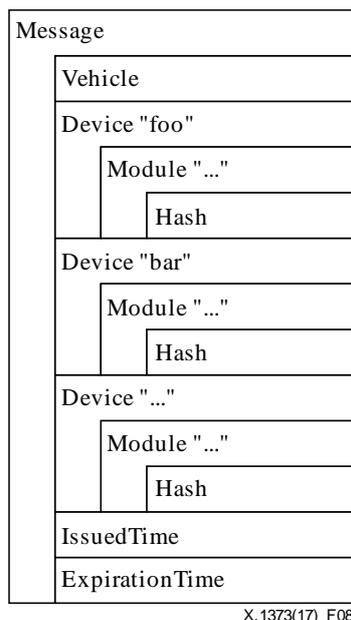


Figure 8 – Structure du message update_report (submit)

Tableau 10 – Eléments du message update_report (submit)

Elément	Attribut de l'élément	Description
Message	–	Conteneur du message.
	protocol	Toujours "1.0".
	version	Numéro de version de l'expéditeur du message.
	type	Type de message (toujours "update_report").
	subtype	Sous-type de message (toujours "submit").
	sessionid	L'identifiant de session est un identifiant GUID aléatoire associé à la session relative au rapport de mise à jour. Un même identifiant de session est utilisé pour une série de messages update_report (submit et receipt).
	trustlevel	Le niveau de confiance est déterminé sur la base de la capacité de sécurité et de l'exigence de sécurité du dispositif qui a généré ce message.
	ownerid	Identifiant du propriétaire fourni par le constructeur automobile/l'équipementier.
	messageid	L'identifiant de message est un identifiant GUID aléatoire associé à un message spécifique.
Vehicle	–	Conteneur d'informations sur le véhicule. Il contient plusieurs éléments de module.
	name	Nom du véhicule, le cas échéant.
	model	Nom du modèle du véhicule fourni par le constructeur automobile.

Tableau 10 – Eléments du message update_report (submit)

Elément	Attribut de l'élément	Description
	modelid	Nom du modèle du véhicule.
	vehicleid	Identifiant du véhicule défini par le constructeur automobile/l'équipementier.
	locale	Informations de localisation du véhicule
Device	–	Conteneur d'informations sur le dispositif. Il contient plusieurs éléments de module.
	name	Nom du dispositif, le cas échéant.
	type	Nom du type de dispositif, par exemple "ECU gestion de la consommation d'énergie", "ECU bouclage des ceintures de sécurité", etc.
	model	Nom du modèle du dispositif.
	deviceid	Identifiant du dispositif défini par le constructeur automobile/l'équipementier.
	hwversion	Version de ce module matériel
Module	–	Conteneur d'informations sur le module, qui contient un élément de hachage.
	moduleid	L'identifiant de module est un identifiant unique fourni par le constructeur automobile/l'équipementier.
	version	Version de ce module logiciel.
	nextversion	Version de la mise à jour du module en cours, principalement utilisée pour envoyer un message de réponse pendant une mise à jour.
	status	Résultat de l'installation de ce module.
Hash	–	Conteneur dans lequel figurent une valeur de hachage et des informations sur l'algorithme de hachage.
	algorithm	Algorithme de la fonction de hachage (par exemple SHA-3, SHA-256, etc.).
IssuedTime	–	Heure de génération de ce message.
ExpirationTime	–	Heure d'expiration de ce message.

Tableau 11 – Exemple de message update_report (submit)

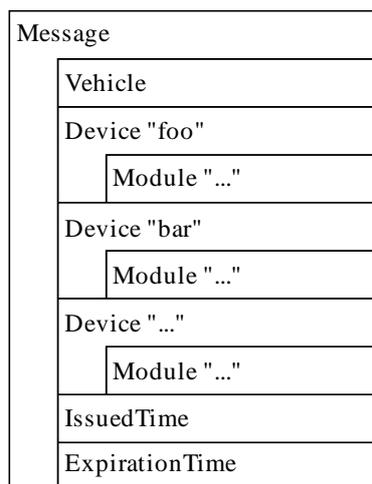
```

<message protocol="1.0" version="1.0.2" type="update_report" subtype="submit"
sessionid="{9AFFEB5A-F36B-4E05-819F-5BDCD3A0E3EC}" ownerid="oid987239487"
messageid="{3F7A6438-8306-447E-A1BB-99CED4C2B6AD}" trustlevel="3">
  <Vehicle name="vehicleName" modelid="mid34987130" type="ECU"
model="modelName" vid="vid0987234" locale="CH"/>
  <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion="HB-01">
    <Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}"
version="1.4.0" nextversion="" status="ok">
      <Hash algorithm="SHA-256">hash data here</ModuleHash>
    </Module>
    <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion="" status="ok">
      <Hash algorithm="SHA-256">hash data here</ModuleHash>
    </Module>
  </Device>
  <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion="HB-02">
    <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion="" status="ok">
      <Hash algorithm="SHA-256">hash data here</ModuleHash>
    </Module>
  </Device>
  <IssuedTime "1903-07-01T00:00:00Z"/>
  <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>

```

7.2.5.2 Message update_report (receipt)

A la fin de la procédure, le serveur de mise à jour envoie un message update_report (receipt) à la passerelle VMG de manière à indiquer au véhicule la fin de la procédure globale de mise à jour. Le format du message update_report (receipt) est pratiquement le même que celui du message diagnose (receipt).



X.1373(17)_F09

Figure 9 – Structure du message update_report (receipt)

Tableau 12 – Eléments du message update_report (receipt)

Elément	Attribut de l'élément	Description
Message	–	Conteneur du message.
	protocol	Toujours "1.0".
	version	Numéro de version de l'expéditeur du message.
	type	Type de message (toujours "update_report").
	subtype	Sous-type de message (toujours "receipt").
	sessionid	L'identifiant de session est un identifiant GUID aléatoire associé à la session relative au rapport de mise à jour. Un même identifiant de session est utilisé pour une série de messages update_report (submit et receipt).
	trustlevel	Le niveau de confiance est déterminé sur la base de la capacité de sécurité et de l'exigence de sécurité du dispositif qui a généré ce message.
	ownerid	Identifiant du propriétaire fourni par le constructeur automobile/l'équipementier.
	messageid	L'identifiant de message est un identifiant GUID aléatoire associé à un message spécifique.
Vehicle	–	Conteneur d'informations sur le véhicule. Il contient plusieurs éléments de module.
	name	Nom du véhicule, le cas échéant.
	model	Nom du modèle du véhicule fourni par le constructeur automobile.
	modelid	Nom du modèle du véhicule.
	vehicleid	Identifiant du véhicule défini par le constructeur automobile/l'équipementier.
	locale	Informations de localisation du véhicule
Device	–	Conteneur d'informations sur le dispositif. Il contient plusieurs éléments de module.
	name	Nom du dispositif, le cas échéant.
	type	Nom du type de dispositif, par exemple "ECU gestion de la consommation d'énergie", "ECU bouclage des ceintures de sécurité", etc.
	model	Nom du modèle du dispositif.
	deviceid	Identifiant du dispositif défini par le constructeur automobile/l'équipementier.
	hwversion	Version de ce module matériel.
Module	–	Conteneur d'informations sur le module, qui contient un élément de hachage.
	moduleid	L'identifiant de module est un identifiant unique fourni par le constructeur automobile/l'équipementier.
	version	Version de ce module logiciel.
	nextversion	Version de la mise à jour du module en cours, principalement utilisée pour envoyer un message de réponse pendant une mise à jour.
	status	Acquittement du rapport pour ce module.

Tableau 12 – Eléments du message update_report (receipt)

Elément	Attribut de l'élément	Description
IssuedTime	–	Heure de génération de ce message.
ExpirationTime	–	Heure d'expiration de ce message.

Tableau 13 – Exemple de message update_report (receipt)

```

<message protocol="1.0" version="1.0.2" type="update_report" subtype="receipt"
sessionid="{9AFFEB5A-F36B-4E05-819F-5BDCD3A0E3EC}" ownerid="oid987239487"
messageid="{B5585708-6BDA-4B07-B2CB-5E9241F63271}" trustlevel="3">
  <Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale="CH"/>
  <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion="HB-01">
    <Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}"
version="1.4.0" nextversion="" status="ok"/>
    <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion="" status="ok"/>
  </Device>
  <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion="HB-02">
    <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion="" status="ok"/>
  </Module>
</Device>
  <IssuedTime "1903-07-01T00:00:00Z"/>
  <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>

```

Appendice I

Méthodologie d'analyse du risque

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

I.1 Méthodologie d'analyse du risque basée sur les lignes directrices [b-JASO TP15002]

Le présent appendice fournit des informations détaillées relatives à l'Appendice II, sur la base des lignes directrices concernant la sécurité des données automobiles [b-JASO TP15002].

La sécurité des données est devenue importante dans la conception des systèmes intégrés. Dans le domaine des systèmes informatiques, des exemples de diverses attaques contre la sécurité sont connus, et le savoir-faire pour évaluer un risque se développe au fur et à mesure de la conception de systèmes informatiques. Les concepts de sécurité de base nécessaires pour l'évaluation de produits informatiques sont donnés dans la norme [ISO/CEI 15408-1]. Dans le contexte de l'évaluation, la norme [ISO/CEI 15408-1] emploie l'expression "cible de l'évaluation (TOE)". Certains actifs sont des entités que le propriétaire de la cible TOE considère comme importantes. La norme [ISO/CEI 15408-1] vise à fixer des objectifs de sécurité pour une cible TOE, constituant une déclaration de l'intention de lutter contre les menaces identifiées et/ou de satisfaire aux politiques ou hypothèses de sécurité de l'organisation identifiées. Les menaces entraînent des risques pour les actifs, qui sont fonction de la probabilité de mise en oeuvre d'une menace et de l'impact sur les actifs lorsque cette menace est mise en oeuvre. Toutefois, la norme [ISO/CEI 15408-1] ne spécifie pas comment identifier les menaces et analyser le risque.

S'agissant des systèmes intégrés, le présent appendice décrit les menaces identifiées et présente une analyse du risque, conformément au cadre défini dans la norme [ISO/CEI 15408-1]. L'objectif ici est que l'analyse du risque ne dépende pas du savoir-faire en matière de conception de la sécurité. Par conséquent, la présente Recommandation utilise la méthode d'analyse du risque CRSS [b-JASO TP15002] pour calculer le niveau de risque associé à une menace contre un système intégré. Cette méthode est caractérisée par les étapes suivantes: (1) la formulation des résultats de l'étape de définition du modèle de système et de l'étape d'analyse des menaces; (2) la détermination de la valeur des paramètres au moyen des informations obtenues lors de l'étape précédente.

Le processus d'évaluation de la sécurité [b-JASO TP15002] se compose des phases suivantes:

Phase 1: Définition de la cible de l'évaluation

Phase 2: Identification des menaces

Phase 3: Analyse du risque

Chaque phase est expliquée ci-après.

I.1.1 Phase 1: Définition de la cible de l'évaluation

On définit la cible en vue de l'identification des menaces dans la phase suivante.

La phase 1 comprend les quatre étapes suivantes:

Etape 1: Etablissement de connaissances communes

Sur la base de la documentation générale relative au système, et afin que tous les membres du projet disposent de connaissances communes sur le cycle de vie du système cible, et sur la structure du système, des informations sont préparées, concernant par exemple une figure de la structure du système, les fonctions du système et les données utilisées par le système.

Etape 2: Elaboration d'une figure du modèle de la cible de l'évaluation

Une "figure du modèle de la cible de l'évaluation" est élaborée, dans laquelle on indique les composants du système et les flux d'information entre ces composants.

Etape 3: Définition d'un descriptif des fonctions des modules

Pour chaque module composant décrit dans la figure du modèle de la cible de l'évaluation, on indique les fonctions assurées et les actifs protégés. On élabore ainsi un tableau descriptif des fonctions des modules.

Pour décrire les menaces de sécurité, on peut se demander qui sont les agents de menace, quels sont les effets indésirables et quels sont les actifs concernés dans le système cible de l'évaluation. Outre les informations, qui, par convention, sont considérées comme un actif à protéger, les actifs des systèmes intégrés pour automobiles comprennent aussi les logiciels des systèmes intégrés et les fonctions qui commandent les mécanismes comme le moteur ou les freins.

Un modèle de système est élaboré à partir de la nature des actifs et des diagrammes de flux de données qui spécifient les flux de données par rapport à ces actifs.

En ce qui concerne les effets indésirables (liés aux menaces), on étudie tout ce qui peut se produire à chaque point d'entrée, en particulier les pertes de confidentialité, d'intégrité ou de disponibilité qui peuvent se produire pour chaque type d'actif. Par exemple, il est important que les fonctions d'un système informatique pour automobile fonctionnent correctement, comme prévu, et toute perte d'intégrité ou de disponibilité doit être évitée. De même, il est important que les informations échangées entre les serveurs centraux et les dispositifs ITS (système de transport intelligent) à bord du véhicule soient protégées contre toute divulgation et modification, et toute perte de confidentialité ou d'intégrité doit aussi être évitée. Le Tableau I.1 donne des exemples d'informations et d'autres actifs à protéger dans les véhicules.

Tableau I.1 – Exemples d'informations et d'autres actifs qui doivent être protégés dans les véhicules (sécurité des informations dans les véhicules)

Objets à protéger	Description
Fonctionnement des "fonctions de commande de base"	Cohérence et disponibilité des "fonctions de commande de base", environnement d'exécution des "fonctions de commande de base", communications pour le fonctionnement.
Informations propres au véhicule	Informations qui sont propres au véhicule (identifiant de véhicule, identifiant de dispositif, etc.), code d'authentification, et informations accumulées, par exemple l'historique de circulation et l'historique de fonctionnement.
Informations sur l'état du véhicule	Données représentant l'état du véhicule, par exemple l'emplacement, la vitesse de circulation et la destination.
Informations sur l'utilisateur	Informations personnelles, informations d'authentification, informations de facturation, historique d'utilisation et historique de fonctionnement pour l'utilisateur (conducteur/passagers).
Logiciels	Logiciels associés aux "fonctions de commande de base" et aux "fonctions étendues" du véhicule, par exemple les logiciels pour les unités ECU.
Contenus	Données pour les applications vidéo, musicales, cartographiques, etc.
Informations de configuration	Données de réglage du comportement des matériels, logiciels, etc.

Etape 4: Définition des étapes du cycle de vie de la cible

On élabore un tableau du cycle de vie, dans lequel on indique toutes les étapes du cycle de vie du système cible.

Les agents de menaces sont les personnes qui interviennent à un moment ou à un autre tout au long du cycle de vie d'un véhicule, depuis sa construction jusqu'à son élimination, en passant par son utilisation par les propriétaires qui ont acheté le véhicule, neuf ou d'occasion. Cela s'explique par le fait que les informations confidentielles conservées par les systèmes intégrés pour automobiles sont stockées et consultées non seulement pendant la phase d'usage normal mais aussi pendant d'autres phases, notamment pendant la construction, la livraison ou l'entretien. Le cycle de vie de la cible TOE est décrit en détail dans le Tableau I.2.

Tableau I.2 – Cycle de vie de la cible TOE

Phase	Sous-phase	Description	Personnes concernées
Fonctionnement	Transport	Un membre du personnel du constructeur automobile doit transporter un véhicule neuf chez un concessionnaire. Il demande à un opérateur d'une entreprise de transport de s'en charger.	<ul style="list-style-type: none"> Personnel du constructeur automobile Opérateur de l'entreprise de transport Personnel du concessionnaire Tiers
	Livraison du véhicule	Un membre du personnel du concessionnaire livre le véhicule au propriétaire.	<ul style="list-style-type: none"> Personnel du concessionnaire Propriétaire Tiers
	Fonctionnement/usage normal	Le propriétaire ou un usager utilise le véhicule. Un administrateur système intervient en tant qu'administrateur du serveur de mise à jour qui fournit les logiciels. Un opérateur de télécommunication intervient pour la fourniture du réseau de communication.	<ul style="list-style-type: none"> Propriétaire ou usager Administrateur système Opérateur de télécommunication Tiers
	Fonctionnement/usage normal Téléchargement de logiciels	En vue de la mise à jour des logiciels via le serveur de mise à jour, le véhicule télécharge les logiciels à partir du serveur de mise à jour.	<ul style="list-style-type: none"> Personnel du constructeur automobile Personnel de l'équipementier Administrateur système Opérateur de télécommunication Tiers
	Entretien (mise à jour de logiciels via le serveur de mise à jour) Mise à jour de logiciels	Lorsque le véhicule est garé, une mise à jour des logiciels est effectuée. L'administrateur du serveur intervient en tant qu'administrateur système de mise à jour. L'opérateur de télécommunication intervient en tant que fournisseur du réseau de communication. Un membre du personnel d'un fournisseur intervient en	<ul style="list-style-type: none"> Personnel du constructeur automobile Personnel de l'équipementier Administrateur système Opérateur de télécommunication

Tableau I.2 – Cycle de vie de la cible TOE

Phase	Sous-phase	Description	Personnes concernées
		tant que fournisseur de services utilisant le réseau de communication.	<ul style="list-style-type: none"> • Tiers
	Entretien (mise à jour de logiciels via un connecteur OBD)	Un membre du personnel du concessionnaire ou de l'atelier d'entretien met à jour les logiciels via un connecteur OBD (diagnostic à bord) au moment de l'inspection du véhicule.	<ul style="list-style-type: none"> • Personnel du concessionnaire • Personnel de l'atelier d'entretien • Propriétaire ou usager • Tiers

I.1.2 Phase 2: Identification des menaces

On identifie les problèmes de sécurité concernant la cible TOE définie dans la phase 1.

La phase 2 comprend les trois étapes suivantes:

Etape 1: Formulation des hypothèses

Afin de préciser le cadre dans lequel les menaces sont identifiées, des hypothèses sont définies sur la base de la figure du modèle de la cible de l'évaluation, du descriptif des fonctions des modules et du tableau du cycle de vie. Le cadre dans lequel les menaces sont identifiées dans la phase 2 est limité. On définit les hypothèses sur l'environnement de la cible TOE et on attribue un identifiant avec le préfixe "A" à chaque hypothèse, ce qui permet d'élaborer un tableau des hypothèses.

Pour le fonctionnement de la cible TOE, les hypothèses sont les suivantes:

A.Reliability_OfficeStaff (fiabilité du personnel du constructeur automobile/de l'équipementier/du concessionnaire/de l'atelier d'entretien)

Le personnel du constructeur automobile or de l'équipementier n'accède pas physiquement au véhicule cible d'une attaque. En outre, le personnel du concessionnaire/de l'atelier d'entretien n'accède pas physiquement au véhicule en phase de fonctionnement/usage normal.

A.Reliability_ServiceProvider (fiabilité de l'administrateur système/de l'opérateur de télécommunication)

L'administrateur du serveur de mise à jour/l'opérateur de télécommunication n'accèdent pas physiquement au véhicule. En outre, l'administrateur du serveur de mise à jour/l'opérateur de télécommunication ne sont pas à l'origine de menaces intentionnelles.

A.Reliability_User (fiabilité du propriétaire/de l'usager)

En phase d'entretien, un propriétaire/usager n'accède pas physiquement au véhicule cible d'une attaque.

En phase d'entretien, un propriétaire/usager n'accède pas physiquement au véhicule. En outre, en phase de fonctionnement/usage normal, le propriétaire/usager verrouille toujours le véhicule et il ne permet pas aux personnes non autorisées concernées d'accéder à l'intérieur du véhicule.

A.Operation_Server (protection du serveur à l'extérieur de la cible de l'évaluation)

Le serveur de mise à jour est utilisé correctement, ce qui signifie que les personnes concernées n'accéderont pas aux informations stockées dans le serveur et ne les manipuleront pas.

A.Control_OBD-Tool (protection du dispositif de mesure, etc., à l'extérieur de la cible de l'évaluation)

Un dispositif de mesure est utilisé correctement, ce qui signifie que les personnes concernées n'accéderont pas aux informations stockées dans le dispositif de mesure et ne les manipuleront pas.

Etape 2: Identification des menaces

Sur la base de la figure du modèle de la cible de l'évaluation, du descriptif des fonctions des modules et du tableau du cycle de vie pour chaque composant du système, le Tableau I.3 présente l'identification des menaces selon différents points de vue: où (points d'entrée), qui (agents de menace), quand (phase du cycle de vie), pourquoi (motifs) et quoi (effets indésirables). On attribue un identifiant avec le préfixe "T" à chaque menace identifiée, ce qui permet d'élaborer un tableau des menaces.

En appliquant ces points de vue au modèle du système, au cycle de vie et aux effets indésirables, qui sont étudiés lors de la définition du système cible de l'évaluation décrit au § I.1, on peut identifier de manière exhaustive qui sont les agents de menace et quels sont les effets indésirables, sur quels actifs et dans quelles phases.

Tableau I.3 – Points de vue pour l'identification des menaces

Point de vue	Explication
Où	Identifier les points d'entrée des attaques.
Qui	Identifier les agents de menace.
Quand	Identifier les phases du cycle de vie visées par les attaques.
Pourquoi	Identifier les motifs des attaques.
Quoi	Identifier les effets indésirables.

Etape 3: Définition de la politique de sécurité de l'organisation

La politique de sécurité de l'organisation définit les dispositions nécessitant des mesures de sécurité pour des motifs autres que les menaces. On peut citer par exemple le cadre juridique et les lignes directrices à l'usage du secteur qu'il faut suivre lors de la définition de la cible TOE et dans l'environnement d'exploitation. On identifie les aspects du cadre juridique ou des règles de l'entreprise concernant la définition du système qui sont susceptibles de poser des problèmes de sécurité pour la cible TOE. On attribue un identifiant avec le préfixe "O" à chaque élément de la politique de sécurité, ce qui permet d'élaborer un tableau de la politique de sécurité de l'organisation.

Aucune politique de sécurité de l'organisation n'est appliquée à la cible TOE.

I.1.3 Phase 3: Analyse du risque

Cette étape définit le niveau de risque pour toutes les menaces qui ont été identifiées.

Pour chaque menace du tableau des menaces, on calcule son niveau de priorité.

La phase 3 comprend les deux étapes suivantes.

Etape 1: Evaluation du risque

En règle générale, le risque qu'une menace fait peser sur un système informatique est évalué à partir de l'importance des actifs et du coût d'une attaque, qui dépend de la manière dont la menace est mise en oeuvre. C'est une approche efficace lorsqu'on dispose de nombreux exemples d'attaques, et que l'on peut parvenir à un consensus sur le coût de la méthode d'attaque, y compris des facteurs comme la durée d'exécution nécessaire pour lancer l'attaque et les capacités de la personne qui lance l'attaque. Dans le cas de systèmes intégrés pour automobiles, un certain nombre d'exemples d'attaques ont été identifiés au niveau de la recherche, mais on ne dispose pas d'informations sur un large éventail de

variantes de méthode d'attaque, comme c'est le cas pour les systèmes informatiques. En conséquence, il est difficile d'estimer le coût des méthodes d'attaque.

I.1.3.1 Système CRSS

Le système de notation du risque (CRSS), basé sur le système CVSS, est une méthode d'évaluation du risque associé à une menace, qui est basée sur le système de notation des vulnérabilités courantes (CVSS), à savoir le système de notation du risque (RSS) de la Recommandation [UIT-T X.1521], utilisé pour noter la gravité des vulnérabilités des systèmes informatiques [b-JASO TP15002]. Le système CVSS se compose de trois groupes de métriques – de base, temporel et environnemental – constitués chacun d'un ensemble de métriques. Ces groupes sont décrits comme suit:

- de base: ce groupe représente les propriétés intrinsèques et fondamentales d'une vulnérabilité qui sont constantes dans le temps et d'un environnement d'utilisateur à l'autre.
- temporel: ce groupe représente les caractéristiques d'une vulnérabilité qui varient dans le temps mais pas d'un environnement d'utilisateur à l'autre.
- environnemental: ce groupe représente les caractéristiques d'une vulnérabilité qui concernent un environnement d'utilisateur particulier et qui sont propres à cet environnement.

Le système CRSS évalue les notes de risque au moyen du *groupe des métriques de base* du système CVSS. Le groupe des métriques de base représente les caractéristiques d'une vulnérabilité qui sont constantes dans le temps et d'un environnement d'utilisateur à l'autre. Le vecteur d'accès, la complexité de l'accès, et les métriques d'authentification indiquent comment accéder à la vulnérabilité et si des conditions supplémentaires sont nécessaires pour l'exploiter.

La méthode CRSS consiste à attribuer une valeur à chaque actif en termes de confidentialité, d'intégrité et de disponibilité puis à calculer une note de risque à partir de la facilité de lancement d'une attaque et du niveau d'impact.

La facilité de lancement d'une attaque est obtenue à partir de la métrique indiquant la proximité nécessaire des agents de menace par rapport aux actifs et à partir de l'existence d'obstacles à franchir pour y accéder. Un exemple de classement par rapport à la facilité de lancement d'une attaque est illustré dans le Tableau I.4.

Le niveau d'impact indique dans quelle mesure une vulnérabilité, si elle est exploitée, affectera directement un actif, les impacts étant définis de manière indépendante en termes de perte de confidentialité, d'intégrité et de disponibilité. Par exemple, une vulnérabilité pourrait entraîner une perte partielle d'intégrité et de disponibilité, mais aucune perte de confidentialité. Un exemple de classement par rapport au niveau d'impact est illustré dans le Tableau I.5.

Tableau I.4 – Exemple de classement par rapport à la facilité de lancement d'une attaque (Tableau D.2 de [b-JASO TP15002])

Paramètre	Principe considéré	Classement	Exemples
Vecteur d'accès (AV): Classement de l'origine de l'attaque	Classement en termes d'origine (où) de l'attaque liée à la menace	Local (L)	Clé USB
		Réseau adjacent (A)	Dispositif de connexion WiFi
		Réseau (N)	Ligne mobile
Complexité de l'accès (AC): niveau de complexité des conditions de l'attaque	Classement en termes de compétences et de connaissances requises pour l'attaque	Elevé (H)	Des compétences et des connaissances sont nécessaires pour l'attaque
		Moyen (M)	Des connaissances sont nécessaires pour l'attaque

**Tableau I.4 – Exemple de classement par rapport à la facilité de lancement d'une attaque
(Tableau D.2 de [b-JASO TP15002])**

Paramètre	Principe considéré	Classement	Exemples
		Faible (L)	Pas (peu) de compétences et de connaissances nécessaires pour l'attaque
Authentification (Au): nombre d'authentifications nécessaires avant l'attaque	Classement en termes de nombre d'authentifications entre l'actif et l'agent de menace	Plusieurs (M)	Plusieurs
		Une seule (S)	Une seule
		Aucune (N)	Inutile

**Tableau I.5 – Exemple de classement par rapport au niveau d'impact
(Tableau D.3 de [b-JASO TP15002])**

Actif	Classement	C: impact sur la confidentialité			I: impact sur l'intégrité			A: impact sur la disponibilité		
		Aucun	Partiel	Total	Aucun	Partiel	Total	Aucun	Partiel	Total
Fonction de communication mobile	Service de mise à jour	Oui					Oui			Oui
Informations d'authentification sur mobile				Oui			Oui	Oui		
Fonction d'obtention de logiciel		Oui					Oui			Oui
Logiciel				Oui			Oui	Oui		
Fonction de mise à jour de logiciel à distance		Oui					Oui			Oui
Logiciel				Oui			Oui	Oui		
Fonction de réception GPS	Processus d'information	Oui				Oui			Oui	
Fonction de connexion WiFi		Oui				Oui			Oui	
Informations d'authentification WiFi			Oui			Oui		Oui		
Fonction de connexion USB		Oui				Oui			Oui	
Fonction de communication CAN	Commande du véhicule	Oui					Oui			Oui
Fonction de passerelle CAN		Oui					Oui			Oui
Table de routage				Oui			Oui	Oui		
Fonction de connexion OBD		Oui					Oui			Oui

Pour chacune des menaces décrites sous la forme "où, qui, quand, pourquoi, quoi", il est possible de calculer une note de risque.

Le Tableau I.6 fournit un exemple d'évaluation de notes de risque.

**Tableau I.6 – Exemple d'évaluation de notes de risque
(Tableau D.4 de [b-JASO TP15002])**

N°	Menaces	AV	AC	Au	Facilité de l'attaque	C	I	A	Niveau d'impact	Note de risque
1	T.control_fcn_Mobile_3rd_operation_on_purpose of interfere-fonction	Réseau	Moyen	Une seule		Inutile	Important	Important		
		1	0,61	0,56	6,83	0	0,66	0,66	9,20	7,95
2	T.vehicule_status_WiFi_dealer_main_purpose_forge	Réseau adjacent	Un seul ou plusieurs	Une seule		Faible	Faible	Aucun		
		0,646	0,71	0,56	5,14	0,275	0,275	0	4,94	4,14
3	T.info_transfer_USB_3rd_operation_pursuse_misop	Local	Faible	Aucune		Aucun	Faible	Aucun		
		0,395	0,71	0,704	3,95	0	0,275	0	2,86	2,11

Même dans les cas tels que celui des systèmes intégrés pour automobiles, dans lesquels les connaissances accumulées sur les menaces de sécurité sont insuffisantes, la méthode CRSS permet de calculer une note de risque analytiquement à partir des définitions des menaces et du système d'évaluation. Pour l'évaluation du risque, elle peut prendre en considération des facteurs tels que le risque de panne complète en considérant les fonctions comme des actifs et, pour l'estimation des valeurs, elle peut augmenter la valeur estimée des actifs dans le cas des fonctions pour lesquelles la perte d'intégrité ou de disponibilité a de graves conséquences.

Etape 2: Identifications des causes des menaces

Pour chaque menace pour laquelle la note de risque est supérieure à une certaine valeur, les causes sont analysées logiquement à l'aide d'un arbre de défaillance (FT).

I.2 Vérification des données au moyen d'algorithmes MAC

Les algorithmes MAC jouent un rôle important en matière de chiffrement et de sécurité en assurant l'intégrité des messages (authentification). En ce qui concerne les codes MAC, l'ISO/CEI a élaboré des normes importantes, notamment les normes [b-ISO/CEI 9797-1] (Mécanismes utilisant un chiffrement par blocs), [b-ISO/CEI 9797-2] (Mécanismes utilisant une fonction de hachage dédiée), et [b-ISO/CEI 9797-3] (Mécanismes utilisant une fonction de hachage universelle).

Etant donné qu'un véhicule dispose de ressources de mise en oeuvre limitées, il convient d'utiliser des normes de chiffrement pour environnements contraints. A cet égard, il existe deux types de codes MAC. Le premier type est un code MAC basé sur un chiffrement par blocs conformément à la norme [b-ISO/CEI 9797-1] et à la norme [b-ISO/CEI 29192-2] (chiffrement par blocs pour environnements contraints). Le second type est un code MAC basé sur une fonction de hachage conformément à la norme [b-ISO/CEI 9797-2] et à la norme [b-ISO/CEI 29192-5] (fonction de hachage pour environnements contraints).

Lorsqu'il s'agira de choisir des algorithmes MAC possibles pour la sécurité automobile, il faudra peut-être veiller à ce qu'ils offrent une sécurité ou une performance nettement meilleure que celles offertes par les algorithmes MAC normalisés existants. Le principal objectif du code MAC sera peut-être de parvenir à des mises en oeuvre logicielles compactes et rapides sur des microcontrôleurs ainsi que d'offrir la sécurité adéquate requise par les applications cibles. En particulier, il peut être souhaitable de disposer d'un algorithme MAC très efficace pour les microcontrôleurs.

Appendice II

Menaces, exigences de sécurité et contrôles de sécurité

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

Dans le domaine des systèmes informatiques, des exemples de diverses attaques/menaces contre la sécurité sont connus, et le savoir-faire pour évaluer un risque se développe au fur et à mesure de la conception de systèmes informatiques. Les concepts de sécurité de base nécessaires pour l'évaluation de produits informatiques sont donnés dans la norme [ISO/CEI 15408-1]. Dans le contexte de l'évaluation, la norme [ISO/CEI 15408-1] emploie l'expression "cible de l'évaluation (TOE)". Certains actifs sont des entités que le propriétaire de la cible TOE considère comme importantes. La norme [ISO/CEI 15408-1] vise à fixer des objectifs de sécurité pour une cible TOE, constituant une déclaration de l'intention de lutter contre les menaces identifiées et/ou de satisfaire aux politiques de sécurité de l'organisation identifiées. Les menaces entraînent des risques pour les actifs, qui sont fonction de la probabilité de mise en oeuvre d'une menace et de l'impact sur les actifs lorsque cette menace est mise en oeuvre. Toutefois, la norme [ISO/CEI 15408-1] ne spécifie pas comment identifier les menaces et analyser le risque, mais il existe plusieurs méthodes connues. Dans le présent appendice, après avoir défini la cible TOE relative à la passerelle VMG, qui est reconnue comme un composant essentiel pour la mise à jour sécurisée des logiciels, nous identifierons les principales menaces puis nous intéresserons aux exigences de sécurité relatives aux principales menaces. Enfin, nous présenterons des contrôles de sécurité de haut niveau afin de satisfaire aux exigences de sécurité.

II.1 Définition de la cible de l'évaluation

Le présent paragraphe définit la cible TOE relative à la passerelle VMG, qui est reconnue comme un composant essentiel pour la mise à jour sécurisée des logiciels dans la présente Recommandation.

L'interface avec l'extérieur comprend un connecteur OBD (diagnostic à bord), un module de communication mobile, un dispositif de réception de signaux GPS/GLONASS (système mondial de localisation /système mondial de navigation par satellite), une connexion WiFi (fidélité sans fil), une connexion de radio/télévision (TV), une connexion Bluetooth, une connexion CAN0/1, une interface utilisateur CD/DVD (disque compact/ disque numérique polyvalent), un connecteur USB (bus série universel) et un connecteur SD (numérique sécurisé). Dans le présent paragraphe, parmi les bus à l'intérieur du véhicule, on s'intéresse au connecteur CAN (réseau local de commande), mais des analyses identiques peuvent être effectuées pour les autres types de bus à l'intérieur du véhicule, par exemple MOST (transport dans des systèmes orientés média), LIN (réseau local d'interconnexion), FlexRay, etc.

Dans la Figure II.1, la cible TOE est définie par la zone entourée d'une ligne en pointillés, qui assure un contrôle sécurisé des communications en tant qu'interface de connexion avec l'extérieur du véhicule.

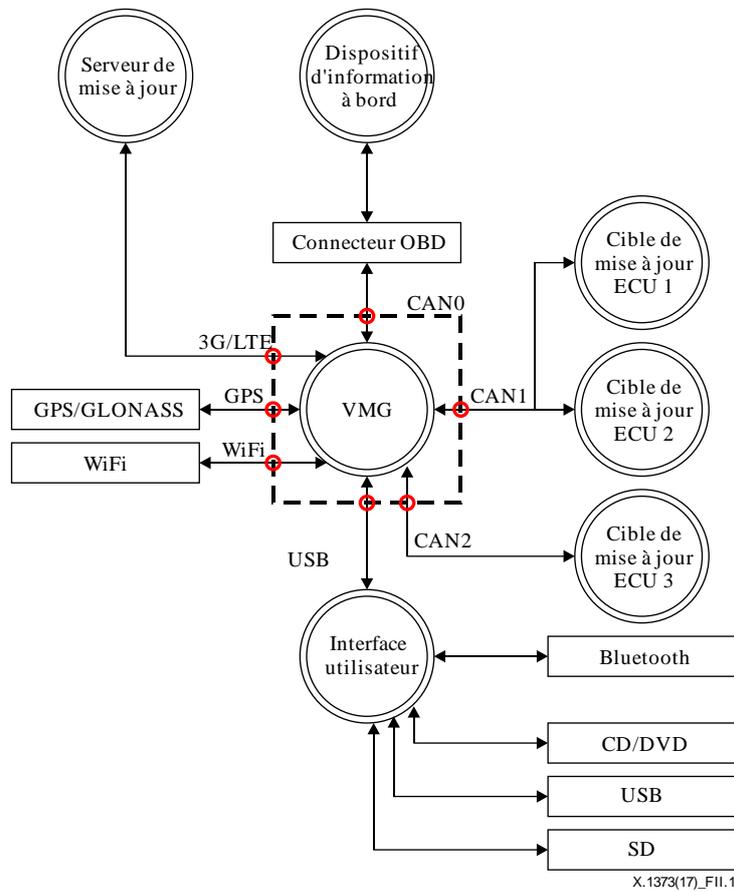


Figure II.1 – Modèle de la cible TOE

Un descriptif des fonctions des modules de la cible TOE est présenté dans le Tableau II.1. Ce tableau indique en outre la relation entre la fonction décrite dans la cible TOE et les principales fonctionnalités de sécurité que sont la confidentialité (C), l'intégrité (I) et la disponibilité (A) afin de définir les exigences de sécurité basées sur la cible TOE au paragraphe II.3.

Tableau II.1 – Descriptif des fonctions des modules de la cible TOE

#	Module	Fonction		Actif	C	I	A
1	Passerelle mobile de véhicule	Fonction de communication mobile	Elle communique avec le serveur via une connexion mobile.	Fonction de communication mobile		Oui	Oui
			Elle utilise des informations d'authentification pour authentifier le serveur.	Informations d'authentification	Oui	Oui	
		Fonction d'obtention de logiciel	Elle obtient un logiciel à distance via une connexion mobile ou via le connecteur OBD.	Fonction d'obtention de logiciel		Oui	Oui
				Informations des logiciels	Oui	Oui	
		Fonction de mise à jour de	Elle met à jour un logiciel à distance via une connexion	Fonction de mise à jour de logiciel à distance		Oui	Oui
				Fonction de mise à jour de logiciel à distance			

Tableau II.1 – Descriptif des fonctions des modules de la cible TOE

#	Module	Fonction	Actif	C	I	A	
		logiciel à distance	mobile ou via le connecteur OBD. En cas de mise à jour de logiciel à distance, elle utilise des informations de sécurité pour la mise à jour afin d'authentifier le serveur.	Informations de sécurité pour la mise à jour	Oui	Oui	
				Informations des logiciels	Oui	Oui	
		Fonction de réception GPS	Elle reçoit des données provenant d'un satellite GPS.	Fonction de réception GPS		Oui	Oui
		Fonction de connexion WiFi	Elle établit une connexion Internet pour les dispositifs via une connexion WiFi. Elle utilise des informations d'authentification via une connexion WiFi.	Fonction de connexion WiFi		Oui	Oui
				Informations d'authentification	Oui	Oui	
		Fonction de connexion USB	Elle communique via un câble USB avec l'interface utilisateur.	Fonction de connexion USB		Oui	Oui
		Fonction de communication CAN	Elle envoie/reçoit des données par le bus CAN à destination/en provenance d'une unité ECU	Fonction de communication CAN		Oui	Oui
		Fonction de passerelle CAN	Elle route une communication par le bus CAN en s'appuyant sur une table de routage. Table de routage	Fonction de passerelle CAN		Oui	Oui
				Table de routage	Oui	Oui	
		Fonction de connexion OBD	Elle envoie des données par le bus CAN via le connecteur OBD.	Fonction de connexion OBD		Oui	Oui

II.2 Identification des principales menaces

Compte tenu de la définition de la cible TOE pour la mise à jour des logiciels, qui fait l'objet du paragraphe II.1, le présent paragraphe vise à identifier les principales menaces situées dans la cible TOE conformément au cadre défini dans la norme [ISO/CEI 15408-1].

En ce qui concerne la méthode utilisée pour identifier les principales menaces sur la base de ce modèle de cible TOE, la présente Recommandation emploie la méthode d'analyse du risque décrite dans l'Appendice I (donné à titre d'information).

Tableau II.2 – Principales menaces sur la base du modèle de la cible TOE

#	Etiquette	Qui	Quand (phase)	Pourquoi	Où/quoi
1	T.DoS- Functions- From-OBD- Device	Tiers Personnel de l'atelier d'entretien	Fonctionnement normal Entretien	Menace intentionnelle	Pour une fonction de la passerelle VMG, usurpe l'identité du connecteur OBD, envoie une grande quantité de données, et interfère avec cette fonction.
2	T.Malfunction- Functions- From-OBD- Device	Tiers Personnel de l'atelier d'entretien	Fonctionnement/usage normal/ entretien Entretien	Menace intentionnelle	Pour une fonction de la passerelle VMG, usurpe l'identité du connecteur OBD, envoie des données non autorisées, entraînant un dysfonctionnement de cette fonctionnalité.
3	T.MissDoS- Functions- From-OBD- Device	Personnel du concessionnaire Personnel de l'atelier d'entretien	Entretien	Menace involontaire	Pour une fonction de la passerelle VMG, envoie une grande quantité de données ou des données non autorisées à partir du connecteur OBD par erreur, entraînant un dysfonctionnement de cette fonctionnalité.
4	T.DoS- Functions- From-ECU	Tiers Personnel de l'atelier d'entretien	Fonctionnement/usage normal/ entretien Entretien	Menace intentionnelle	Pour une fonction de la passerelle VMG, utilise l'ingénierie inverse pour concevoir le même produit que les micrologiciels ECU connectés aux ports CAN0-2, met à jour lesdits micrologiciels en utilisant des micrologiciels non autorisés; envoie alors une grande quantité de données à partir des unités ECU connectées aux ports CAN1-5, et interfère avec cette fonctionnalité.
5	T.Malfunction- Functions- From-ECU	Tiers Personnel de l'atelier d'entretien	Fonctionnement/usage normal/ entretien Entretien	Menace intentionnelle	Pour une fonction de la passerelle VMG, utilise l'ingénierie inverse pour concevoir le même produit que les micrologiciels ECU connectés aux ports CAN1-5, met à jour lesdits micrologiciels en utilisant des micrologiciels non autorisés; envoie alors des données non autorisées à partir des unités ECU connectées aux ports CAN1-5, entraînant un dysfonctionnement de cette fonctionnalité.
6	T.DoS- Functions- From-Mobile- Device	Tiers	Fonctionnement/usage normal/ entretien	Menace intentionnelle	Pour une fonction de la passerelle VMG, usurpe l'identité d'un serveur, envoie une grande quantité de données à la passerelle VMG à partir d'un dispositif de connexion mobile, et interfère avec cette fonctionnalité.

Tableau II.2 – Principales menaces sur la base du modèle de la cible TOE

#	Etiquette	Qui	Quand (phase)	Pourquoi	Où/quoi
7	T.Spoofing-Server_ToGet-Data	Tiers	Fonctionnement/usage normal/entretien	Menace intentionnelle	Pour des informations de la passerelle VMG, envoie une commande pour obtenir ces informations à partir d'un dispositif de connexion mobile en interceptant un canal de communication ou en usurpant l'identité d'un dispositif de connexion mobile; reçoit alors les informations de la passerelle VMG.
8	T.MissDoS-Functions-From-mobile-Device	Administrateur système	Fonctionnement/usage normal/entretien	Menace involontaire	Pour une fonction de la passerelle VMG, le serveur envoie, à la suite d'un dysfonctionnement, une grande quantité de données ou des données non autorisées à partir d'un dispositif de connexion mobile, interfère avec cette fonctionnalité, entraînant un dysfonctionnement de cette fonctionnalité.
9	T.Leaking-Mobile-Information-From-Mobile-Device	Propriétaire/usager Administrateur système/ personnel du concessionnaire Administrateur système	Fonctionnement/usage normal/ livraison du véhicule Fonctionnement/usage normal/ entretien	Menace involontaire	Pour des informations de la passerelle VMG, à partir d'un dispositif de connexion mobile, envoie, à la suite d'un dysfonctionnement, une commande à la passerelle VMG pour obtenir un actif protégé (informations) de la passerelle VMG, entraînant une fuite de cet actif.
10	T.MissUpdate-Mobile-Information-From-Mobile-Device	Propriétaire/usager Administrateur système/ personnel du concessionnaire Administrateur système	Fonctionnement/usage normal Livraison du véhicule Fonctionnement/usage normal/ entretien	Menace involontaire	Pour des informations de la passerelle VMG, à partir d'un dispositif de connexion mobile, envoie, à la suite d'un dysfonctionnement, par erreur, une commande à la passerelle VMG pour mettre à jour un actif protégé (informations) de la passerelle VMG, entraînant une mise à jour de cet actif.
11	T.Malfunction-Functions-From-mobile-Device	Tiers	Fonctionnement/usage normal/entretien	Menace intentionnelle	Pour une fonction de la passerelle VMG, à partir d'un dispositif de connexion mobile, usurpe l'identité d'un serveur et envoie des données non autorisées, entraînant un dysfonctionnement de cette fonctionnalité.
12	T.Spoofing-Server_ToRewrite-Data	Tiers	Fonctionnement/usage normal	Menace intentionnelle	Pour un actif protégé (informations) de la passerelle VMG, à partir d'un dispositif de connexion mobile, usurpe l'identité de ce dispositif et envoie une commande de réécriture de l'actif, entraînant la réécriture de cet actif.

Tableau II.2 – Principales menaces sur la base du modèle de la cible TOE

#	Etiquette	Qui	Quand (phase)	Pourquoi	Où/quoi
13	T.DoS- Fonctions- From-Wi-Fi- Device	Tiers	Fonctionnement/usage normal/entretien	Menace intentionnelle	Pour la fonction de connexion WiFi, usurpe l'identité du dispositif de connexion WiFi, envoie une grande quantité de données, et interfère avec cette fonctionnalité.
14	T.Malfunction- Fonctions- From-Wi-Fi- Device	Tiers	Fonctionnement/usage normal/entretien	Menace intentionnelle	Pour la fonction de connexion WiFi, usurpe l'identité du dispositif de connexion WiFi et envoie des données non autorisées, entraînant un dysfonctionnement de cette fonctionnalité.
15	T.MissDoS- Fonctions- From-Wi-Fi- Device	Propriétaire/ usager	Fonctionnement/usage normal	Menace involontaire	Pour la fonction de connexion WiFi, à la suite d'un dysfonctionnement du dispositif de connexion WiFi ou de son infection par un logiciel malveillant, envoie une grande quantité de données ou des données non autorisées et interfère avec cette fonctionnalité, entraînant un dysfonctionnement de cette fonctionnalité
16	T.Spoofing-Wi-Fi- Device_ToGet- Wi-Fi- Information	Tiers	Fonctionnement/usage normal/entretien	Menace intentionnelle	Pour la fonction de connexion WiFi, usurpe l'identité du dispositif de connexion WiFi, envoie une commande pour obtenir les informations d'authentification de la connexion WiFi et exploite ces informations.
17	T.Spoofing-Wi-Fi- Device_ToRewrite- Wi-Fi- Information	Tiers	Fonctionnement/usage normal/entretien	Menace intentionnelle	Pour la fonction de connexion WiFi, usurpe l'identité du dispositif de connexion WiFi, envoie une commande de réécriture des informations d'authentification de la connexion WiFi, entraînant la réécriture de ces informations.
18	T.Leaking-Wi-Fi- Information- From-Wi-Fi- Device	Personnel du concessionnaire Propriétaire/ usager	Livraison du véhicule Fonctionnement/usage normal	Menace involontaire	Pour les informations d'authentification de la connexion WiFi, envoie une commande pour obtenir ces informations, entraînant une fuite de ces informations.
19	T.MissUpdate- Wi-Fi- Information- From-Wi-Fi- Device	Personnel du concessionnaire Propriétaire/ usager	Livraison du véhicule Fonctionnement/usage normal	Menace involontaire	Pour les informations d'authentification de la connexion WiFi, envoie une commande de réécriture de ces informations, entraînant leur réécriture.

II.3 Exigences de sécurité pour la cible TOE

A partir des menaces identifiées au § II.2, on définit trois groupes d'exigences de sécurité pour le modèle de la cible TOE dans les paragraphes qui suivent. Chaque exigence de sécurité est déduite des menaces définies au § II.2. Pour chacune des exigences de sécurité figurant au § II.3, on précise l'ensemble des menaces prises en compte, les numéros étant ceux indiqués dans le Tableau II.2.

II.3.1 Exigences de sécurité pour la cible TOE

II.3.1.1 SR.protection de l'intégrité/de la disponibilité des fonctions de la passerelle VMG via une connexion CAN

L'intégrité et la disponibilité des fonctions de la passerelle VMG doivent être garanties face aux attaques par déni de service (DoS) et aux attaques faisant suite à un dysfonctionnement, perpétrées à partir d'unités ECU via une connexion CAN0-CAN2 (voir les menaces 4 et 5).

Description

Concernant les communications CAN, seules les données CAN auxquelles un identifiant CAN spécifié est attribué sont routées. Si la passerelle VMG reçoit une grande quantité de paquets de données et/ou confirme la présence de séquences anormales en provenance des dispositifs de connexion CAN0-CAN2, elle ne doit pas fonctionner anormalement.

II.3.1.2 SR.protection de la confidentialité des données de la passerelle VMG

Il convient de protéger la confidentialité du contenu des communications entre la passerelle VMG et le serveur de manière à ce que ce contenu ne puisse pas être lu par des tiers (voir les menaces 7, 16 et 17).

II.3.1.3 SR.protection de l'intégrité/de la disponibilité des fonctions de la passerelle VMG via une connexion mobile

L'intégrité et la disponibilité des fonctions de la passerelle VMG doivent être garanties face aux attaques DoS et aux attaques faisant suite à un dysfonctionnement, perpétrées à partir de dispositifs mobiles via une connexion mobile (voir les menaces 6, 7, 8, 9, 10, 11 et 12).

Description

Concernant les communications avec un dispositif de connexion mobile, la passerelle VMG doit confirmer si l'entité communicante est un dispositif de connexion mobile autorisé. La passerelle VMG doit être protégée face à toute usurpation de l'identité du serveur lorsqu'elle reçoit des données non autorisées/anormales via des communications mobiles. Si la passerelle VMG reçoit un très grand nombre de paquets de données en provenance d'un dispositif de connexion mobile et/ou confirme la présence de séquences anormales en provenance d'un dispositif de connexion mobile, elle ne doit pas fonctionner anormalement. En outre, la passerelle VMG doit confirmer la cohérence et la fréquence de transmission entre les commandes envoyées par les dispositifs de connexion mobile.

II.3.1.4 SR.tolérance des fonctions de la passerelle VMG aux défaillances

Les fonctions de la passerelle VMG doivent continuer à fonctionner comme prévu, éventuellement à un niveau réduit en présence de quelque chose d'anormal en raison d'attaques (voir les menaces 1, 2, 3, 4, 5, 6, 8, 11 et 15).

II.3.1.5 SR.protection de l'intégrité/de la disponibilité des fonctions de la passerelle VMG via une connexion OBD

L'intégrité et la disponibilité des fonctions de la passerelle VMG doivent être garanties face aux attaques DoS et aux attaques faisant suite à un dysfonctionnement, perpétrées à partir de dispositifs de connexion OBD via un connecteur OBD (voir les menaces 1, 2 et 3).

Description

Concernant une connexion CAN via le connecteur OBD, seuls les dispositifs spécifiés sont autorisés à accéder aux unités ECU. La passerelle VMG doit être protégée face à toute usurpation de l'identité de dispositifs de connexion OBD lorsqu'elle reçoit des données non autorisées/anormales via le connecteur OBD. Si la passerelle VMG reçoit une grande quantité de données ou des commandes non autorisées en provenance de dispositifs de connexion OBD, elle ne doit pas fonctionner anormalement.

II.3.1.6 SR.protection de la confidentialité/de l'intégrité/de la disponibilité de la passerelle VMG via une connexion WiFi

La passerelle VMG doit être protégée face à toute usurpation de l'identité de dispositifs WiFi, lorsqu'elle reçoit des données non autorisées/anormales via une connexion WiFi (voir les menaces 13, 14, 15, 16, 17, 18 et 19).

Description

Concernant les communications avec un dispositif WiFi, la passerelle VMG doit confirmer si le dispositif a été enregistré à l'avance. Si la passerelle VMG reçoit une grande quantité de paquets de données en provenance de dispositifs WiFi et/ou confirme la présence de séquences anormales en provenance d'un dispositif WiFi, elle ne doit pas fonctionner anormalement.

II.3.2 Exigences de sécurité pour l'environnement d'exploitation de la cible TOE du point de vue informatique

II.3.2.1 SRE.protection des unités ECU

Chaque module ECU doit être protégé contre toute analyse de ses micrologiciels basée sur une obfuscation du module. L'unité ECU doit être protégée contre les attaques utilisant des données de capteur non autorisées. L'unité ECU doit être protégée physiquement contre les attaques basées sur un remplacement non autorisé de l'unité ECU (voir les menaces 4 et 5).

II.3.2.2 SRE.protection des communications CAN

Les communications CAN doivent être protégées contre l'analyse du protocole de communication CAN au moyen d'opérations d'embrouillage (opérations simples comme le basculement de bits, etc.) sur les données utiles CAN. Le bus CAN doit être protégé physiquement contre les attaques dans lesquelles un tiers malveillant se rattache au câblage CAN (voir les menaces 4 et 5).

II.3.2.3 SRE.protection du réseau de communication mobile

Le réseau de communication mobile que la passerelle VMG utilise pour communiquer avec le serveur doit être protégé contre les attaques provenant de dispositifs non autorisés. Il est nécessaire de protéger la confidentialité des informations de configuration du réseau. Il est nécessaire de surveiller le réseau afin de détecter les attaques (voir les menaces 6, 7, 11 et 12).

II.3.2.4 SRE.protection des communications sans fil

Il est nécessaire de protéger les communications sans fil contre l'analyse du protocole de communication sans fil, en stockant uniquement le minimum de données nécessaires dans les données utiles du paquet de données, ou en embrouillant les données utiles au moyen d'opérations simples comme le basculement de bits, etc. (voir les menaces 7, 12, 16 et 17).

II.3.3 Exigences de sécurité pour l'environnement d'exploitation du point de vue de l'exploitation/gestion ne concernant pas les aspects informatiques

II.3.3.1 SREN.mise en garde

Il est à noter qu'une attaque visant un système à l'intérieur d'un véhicule constitue un acte criminel. En outre, il est nécessaire de restreindre la vente de produits favorisant la criminalité (voir les menaces 1, 2, 4, 5, 6, 7, 11, 12, 13, 14, 16 et 17).

II.3.3.2 SREN.serveur de réseau

L'administrateur système doit empêcher toute fuite ou altération des données stockées due à une gestion inappropriée du serveur (voir les menaces 7 et 8).

II.3.3.3 SREN.protection des outils OBD

Il est nécessaire de protéger les outils OBD se connectant à un véhicule contre toute utilisation non autorisée grâce à une gestion sécurisée. En outre, les méthodes d'utilisation des outils connectés à un véhicule doivent être confirmées avant l'utilisation (voir la menace 3).

II.3.3.4 SREN.usager

Lorsqu'un usager utilise un véhicule, il doit être informé des précautions à prendre.

Description

Si l'usager s'éloigne du véhicule, il doit le verrouiller pour éviter toute intrusion par un tiers. Lorsque le véhicule n'est pas utilisé, il doit être garé à un endroit difficile d'accès pour les tiers. L'usager doit confirmer l'absence de dispositif non identifié avant d'utiliser un véhicule. L'usager doit être prudent lorsqu'il connecte des produits du commerce au connecteur OBD qui sert d'interface pour l'entretien (voir les menaces 1, 2, 4, 5, 13, 14, 16 et 17).

II.3.3.5 SREN.recherche des virus

Les dispositifs connectés au système via une connexion mobile/WiFi doivent être analysés régulièrement (voir les menaces 9, 10, 15, 18 et 19).

II.3.3.6 SREN.protection des dispositifs sans fil

La personne concernée doit confirmer comment utiliser un dispositif connecté via une connexion mobile/WiFi avant l'utilisation. En outre, elle doit veiller à éviter toute fuite du mot de passe des dispositifs connectés par WiFi et des commandes (voir les menaces 9, 10, 12, 13, 14, 16, 17, 18 et 19).

II.3.3.7 SREN.écran de dispositif sans fil

Un usager utilisant un dispositif de connexion WiFi/mobile doit confirmer l'envoi ou non de commandes "get/write" (obtenir/écrire) concernant les informations de la passerelle VMG en sélectionnant l'option correspondante sur l'écran du dispositif (voir les menaces 9, 10, 18 et 19).

II.4 Contrôles de sécurité

Compte tenu des exigences de sécurité définies au § II.3, le présent paragraphe définit des contrôles de sécurité qui satisfont à ces exigences, notamment du point de vue informatique.

II.4.1 SC.démarrage sécurisé

Comme mesure contre l'analyse (par exemple l'altération) du module du programme d'origine d'une unité ECU, il est recommandé de mettre en oeuvre dans l'unité ECU des mécanismes de contrôle automatique de ses logiciels en utilisant le mécanisme de protection de la sécurité du démarrage du module matériel de sécurité (HSM) à chaque séquence de démarrage de l'unité ECU.

Exigence de sécurité correspondante

- SRE.protection des unités ECU (§ II.3.2.1)

II.4.2 SC.vérification des messages

Contre les attaques d'altération, d'écoute clandestine et de répétition, la vérification des messages est efficace pour parvenir à conserver l'authenticité des entités et l'intégrité des messages.

Deux méthodes peuvent être utilisées à cette fin: la première repose sur une signature numérique (méthode de la signature numérique) et la seconde sur un code d'authentification de message (MAC).

Cependant, en ce qui concerne les mises en oeuvre pratiques des unités ECU dans un véhicule, les capacités de chiffrement des dispositifs varient en fonction des véhicules. Par exemple, un véhicule de luxe pourrait avoir des modules HSM pour toutes ses unités ECU, tandis qu'un véhicule courant pourrait n'avoir des modules HSM que pour certaines unités ECU. En outre, les capacités de chiffrement diffèrent en fonction des types de module HSM utilisés.

Il faut donc tenir compte, dans l'architecture de sécurité, des différences entre les capacités de sécurité d'un véhicule à l'autre. Ainsi, pour les véhicules utilisant un algorithme de chiffrement asymétrique (par exemple un module de plate-forme fiable (TPM)), la présente Recommandation recommande d'utiliser la méthode de la signature numérique basée sur la Recommandation [UIT-T X.509] pour la vérification des messages, tandis que pour les véhicules n'utilisant pas d'algorithme de chiffrement asymétrique (par exemple module HSM et carte à puce), elle recommande d'utiliser un code MAC pour la vérification des messages. Pour plus de détails concernant le protocole de communication y compris la vérification des messages, voir le § 7. Ce contrôle de sécurité est essentiel pour la mise à jour à distance des logiciels afin de vérifier les messages définis dans la présente Recommandation.

Exigences de sécurité correspondantes

- SR.protection de la confidentialité des données de la passerelle VMG (§ II.3.1.2);
- SR.protection de la confidentialité/de l'intégrité/de la disponibilité de la passerelle VMG via une connexion WiFi (§ II.3.1.6);
- SRE.protection du réseau de communication mobile (§ II.3.2.3);
- SRE.protection des communications sans fil (§ II.3.2.4).

II.4.3 SC.authentification de l'entité de communication

Afin d'éviter toute usurpation de l'identité des entités en communication (par exemple des unités ECU, de la passerelle VMG et du serveur de mise à jour), il est recommandé que ces entités s'authentifient mutuellement au début de chaque communication. Ce contrôle de sécurité devrait être mis en oeuvre dans la couche transport, et les procédures de mise à jour sécurisée des logiciels définies dans la présente Recommandation devraient être sécurisées au moyen d'une fonction de couche inférieure. Pour l'authentification des entités en communication, une mesure efficace consiste à effectuer une authentification à la fois du client et du serveur basée sur les protocoles SSL/TLS (couche de connecteurs sécurisés/sécurité de la couche transport) au moyen d'une autorité de certification (CA) tierce.

Exigences de sécurité correspondantes

- SR.protection de la confidentialité/de l'intégrité/de la disponibilité de la passerelle VMG via une connexion WiFi (§ II.3.1.6);
- SRE.protection du réseau de communication mobile (§ II.3.2.3);
- SRE.protection des communications sans fil (§ II.3.2.4).

II.4.4 SC.filtrage des messages

Dans une attaque DoS contre une passerelle VMG, il se peut par exemple que l'attaquant compromette une unité ECU de manière à ce qu'elle envoie une très grande quantité de messages falsifiés à la passerelle VMG pour lui faire utiliser, à mauvais escient, sa puissance de calcul. Afin de réduire l'impact de ce type d'attaques DoS sur la sécurité, une méthode efficace consiste à utiliser une technique de filtrage des messages. Il est recommandé que la passerelle VMG élimine les messages inappropriés en fonction de l'identifiant de l'expéditeur, du type de message, de sa taille, de sa fréquence, etc., ou d'une combinaison de tous ces critères.

Exigences de sécurité correspondantes

- SR.protection de l'intégrité/de la disponibilité des fonctions de la passerelle VMG via une connexion CAN (§ II.3.1.1);
- SR.protection de l'intégrité/de la disponibilité des fonctions de la passerelle VMG via une connexion mobile (§ II.3.1.3);
- SR.protection de l'intégrité/de la disponibilité des fonctions de la passerelle VMG via une connexion OBD (§ II.3.1.5).

II.4.5 SC.tolérance des fonctions de la passerelle VMG aux défaillances

Il est fortement recommandé aux fournisseurs de passerelles VMG de mettre en oeuvre des logiciels à sûreté intégrée dans les passerelles VMG afin qu'elles puissent continuer à fonctionner comme prévu en présence de quelque chose d'anormal en raison d'attaques. En particulier, une passerelle VMG surveille l'état de fonctionnement et si elle détecte quelque chose d'anormal, elle prend une mesure (par exemple redémarre) afin de revenir à un état normal. Si tout rétablissement est impossible, le conducteur est informé du problème et le fonctionnement de la passerelle VMG est suspendu en toute sécurité.

Exigence de sécurité correspondante

- SR.tolérance des fonctions de la passerelle VMG aux défaillances (§ II.3.1.4).

Bibliographie

- [b-UIT-T F.749.1] Recommandation UIT-T F.749.1 (2015), *Exigences fonctionnelles pour les passerelles de véhicule*.
- [b-ISO/CEI 9797-1] ISO/CEI 9797-1:2011, *Technologies de l'information – Techniques de sécurité – Codes d'authentification de message (MAC) – Partie 1: Mécanismes utilisant un chiffrement par blocs*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50375>
- [b-ISO/CEI 9797-2] ISO/CEI 9797-2:2011, *Technologies de l'information – Techniques de sécurité – Codes d'authentification de message (MAC) – Partie 2: Mécanismes utilisant une fonction de hachage dédiée*.
<http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51618>
- [b-ISO/CEI 9797-3] ISO/CEI 9797-3:2011, *Technologies de l'information – Techniques de sécurité – Codes d'authentification de message (MAC) – Partie 3: Mécanismes utilisant une fonction de hachage universelle*.
<http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51619>
- [b-ISO/CEI 29192-2] ISO/CEI 29192-2:2012, *Technologies de l'information – Techniques de sécurité – Cryptographie pour environnements contraints – Partie 2: Chiffrements par blocs*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56552>
- [b-ISO/CEI 29192-5] ISO/CEI 29192-5:2016, *Technologies de l'information – Techniques de sécurité – Cryptographie pour environnements contraints – Partie 5: Fonctions de hachage*.
<http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67173>
- [b-JASO TP15002] JASO TP15002:2015, *Guideline for automotive information security analysis*.
- [b-FIPS-202] Federal Information Processing Standards Publication-202 (2015), *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*.
National Institute of Standards and Technology,
<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf>
- [b-ISO 14229] ISO 14229-1:2013, *Véhicules routiers – Services de diagnostic unifiés (SDU) – Partie 1: Spécification et exigences*.
- [b-ISO 13400] ISO 13400, *Véhicules routiers – Communication de diagnostic au travers du protocole internet (DoIP) – Partie 1: Informations générales et définition de cas d'usage*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication