Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TELECOMMUNICATIONS
DE L'UIT

H.551

(01/2022)

SERIE H: SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

Passerelles de véhicule et systèmes de transport intelligents – Architecture des passerelles de véhicule

Architecture des systèmes multimédias dans les véhicules

Recommandation UIT-T H.551

RECOMMANDATIONS UIT-T DE LA SÉRIE H

SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

CARACTÉRISTIQUES DES SYSTÈMES VISIOPHONIQUES	H.100–H.199
INFRASTRUCTURE DES SERVICES AUDIOVISUELS	
Généralités	H.200–H.219
Multiplexage et synchronisation en transmission	H.220–H.229
Aspects système	H.230–H.239
Procédures de communication	H.240–H.259
Codage des images vidéo animées	H.260–H.279
Aspects liés aux systèmes	H.280–H.299
Systèmes et équipements terminaux pour les services audiovisuels	H.300–H.349
Architecture des services d'annuaire pour les services audiovisuels et multimédias	H.350–H.359
Architecture de la qualité de service pour les services audiovisuels et multimédias	H.360–H.369
Téléprésence, environnements en immersion, réalité virtuelle et étendue	H.420-H.439
Services complémentaires en multimédia	H.450–H.499
PROCÉDURES DE MOBILITÉ ET DE COLLABORATION	
Aperçu général de la mobilité et de la collaboration, définitions, protocoles et procédures	H.500–H.509
Mobilité pour les systèmes et services multimédias de la série H	H.510–H.519
Applications et services de collaboration multimédia mobile	H.520–H.529
Sécurité pour les systèmes et services multimédias mobiles	H.530–H.539
Sécurité pour les applications et services de collaboration multimédia mobile	H.540–H.549
PASSERELLES DE VÉHICULE ET SYSTÈMES DE TRANSPORT INTELLIGENTS	
Architecture des passerelles de véhicule	**H.550–H.559**
Interfaces de passerelle de véhicule	H.560–H.569
SERVICES MULTIMEDIAS À LARGE BANDE, TRI-SERVICES MULTIMEDIAS ET SERVICES MULTIMEDIAS EVOLUÉS	
Services multimédias à large bande sur VDSL	H.610–H.619
Services et applications multimédias évolués	H.620–H.629
Applications des réseaux de capteurs ubiquitaires et de fourniture de contenus	H.640–H.649
SERVICES MULTIMÉDIAS ET APPLICATIONS DE TÉLÉVISION PAR RÉSEAU IP	
Aspects généraux	H.700–H.719
Terminaux pour la télévision par réseau IP	H.720–H.729
Intergiciels pour la télévision par réseau IP	H.730–H.739
Traitement d'évènements dans les applications de télévision par réseau IP	H.740–H.749
Métadonnées pour la télévision par réseau IP	H.750–H.759
Cadres généraux des applications multimédias pour la télévision par réseau IP	H.760–H.769
Exploration des services jusqu'au point de consommation dans la télévision par réseau IP	H.770–H.779
Affichage numérique	H.780–H.789
SYSTEMES, SERVICES ET APPLICATIONS MULTIMÉDIAS DE CYBERSANTÉ	
Systèmes de santé individuels	H.810-H.819
Tests de conformité des systèmes de santé individuels aux normes d'interopérabilité (HRN, PAN, LAN, TAN et WAN)	H.820–H.859
Services d'échange de données multimédias concernant la cybersanté	H.860–H.869
Écoute sans risque	H.870–H.879

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

Recommandation UIT-T H.551

Architecture des systèmes multimédias dans les véhicules

Résumé

La Recommandation UIT-T H.551 définit la configuration des systèmes multimédias dans les véhicules (VMS), le modèle de référence de l'architecture des systèmes VMS et la solution de référence pour les applications multimédias des systèmes VMS. Les questions liées à la sécurité des systèmes VMS ainsi qu'à la protection et à la confidentialité des informations d'identification personnelle sont également décrites.

Historique

Édition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T H.551	28-01-2022	16	11.1002/1000/14811

Mots clés

Architecture, systèmes multimédias dans les véhicules.

* 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-fr.

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 (TIC). 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.

À la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas des renseignements les plus récents, il est vivement recommandé aux développeurs de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T H.551

Architecture des systèmes multimédias dans les véhicules

1 Résumé

La présente Recommandation définit la configuration des systèmes multimédias dans les véhicules (VMS), le modèle de référence de l'architecture des systèmes VMS, et la solution de référence pour les applications multimédias des systèmes VMS. Les questions liées à la sécurité des systèmes VMS ainsi qu'à la protection et à la confidentialité des informations d'identification personnelle sont également décrites.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T F.749.3] Recommandation UIT-T F.749.3 (2020), *Cas d'utilisation et exigences pour les réseaux multimédias dans les véhicules*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 réseaux multimédias dans les véhicules (VMN) [UIT-T F.749.3]: les réseaux VMN se composent de la plate-forme de services multimédias dans les véhicules (VMSP), des réseaux de diffusion et de communication, et du système multimédia dans le véhicule (VMS), dans le véhicule.

3.1.2 plate-forme de services multimédias dans les véhicules (VMSP) [UIT-T F.749.3]: la plate-forme VMSP est une plate-forme dans le nuage qui permet de fournir le service multimédia pour le(s) utilisateur(s) final(s) dans le véhicule.

3.1.3 système multimédia dans le véhicule (VMS) [UIT-T F.749.3]: le système VMS se compose des entrées du système multimédia dans le véhicule (VM I/P), de l'unité multimédia dans le véhicule (VMU) et des sorties du système multimédia dans le véhicule (VM O/P).

3.2 Termes définis dans la présente Recommandation

Les termes suivants sont définis dans la présente Recommandation:

3.2.1 fonction principale du système VMS: fonction qui traite des données physiques, fonctionnelles et logiques du VMS.

3.2.2 fonction associée au VMS: fonction qui ne fait que recevoir et afficher les données fonctionnelles et logiques provenant d'autres systèmes ou sous-systèmes.

3.2.3 fonction partagée du système VMS: fonction qui est utilisée par d'autres systèmes ou sous-systèmes afin de partager les données physiques, fonctionnelles et logiques et les informations de commande.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et les acronymes suivants:

ADAS système avancé d'aide à la conduite (*advanced driver assistance system*)

ANC suppression active du bruit (*active noise cancellation*)

APP application (*application*)

AR réalité augmentée (*augmented reality*)

AVM surveillance du périmètre de vision (*around view monitoring*)

bCall appel de dépannage (*breakdown call*)

BGS balayage de fond (*background scan*)

CA accès conditionnel (*conditional access*)

CDR radio numérique convergente (*convergent digital radio*)

DAB radiodiffusion numérique (*digital audio broadcasting*)

DASH diffusion en flux adaptatif dynamique sur HTTP (*dynamic adaptive streaming over HTTP*)

DMS système de surveillance du conducteur (*driver monitoring system*)

DNT ne pas suivre (*do not track*)

DRM gestion des droits numériques (*digital rights management*)

eCall appel d'urgence (*emergency call*)

ECM message de commande d'habilitation (*entitlement control message*)

ECU unité de commande électronique (*electronic control unit*)

EMM message de gestion d'habilitation (*entitlement management message*)

FM modulation de fréquence (*frequency modulation*)

HEO orbite terrestre haute (*high earth orbit*)

HLS diffusion HTTP en direct (*HTTP live streaming*)

HTTP protocole de transfert hypertexte (*hypertext transfer protocol*)

HVAC chauffage, ventilation et climatisation (*heating, ventilation and air conditioning*)

IAM gestion des identités et des accès (*identity and access management*)

IBOC dans la même voie, dans la même bande (*in-band on-channel*)

iCall appel d'information (*information call*)

IHM interface homme-machine

IP protocole Internet (*Internet protocol*)

LCD affichage à cristaux liquides (*liquid crystal display*)

LED diode électroluminescente (*light emitting diode*)

LEO orbite terrestre basse (*low earth orbit*)

MA modulation d'amplitude

MR réalité mixte (*mixed reality*)

NAT traduction d'adresse réseau (*network address translation*)

OBD diagnostic embarqué (*on-board diagnostics*)

OEM fabricant d'équipements d'origine (*original equipment manufacturer*)

OLED diode électroluminescente organique (*organic light emitting diode*)

OS système d'exploitation (*operating system*)

OTA transmission sans fil (*over the air*)

PD diversité de phase (*phase diversity*)

PII informations d'identification personnelle (*personally identifiable information*)

PUF fonction physique non clonable (*physical unclonable function*)

RDS système de données radio (*radio data system*)

RF fréquence radio (*radio frequency*)

RGPD Règlement général sur la protection des données (*general data protection regulation*)

RVC caméra de recul (*rear view camera*)

TCP protocole de contrôle du transfert (*transfer control protocol*)

TCU unité de commande télématique (*telematic control unit*)

TMC canal de messages de trafic (*traffic message channel*)

UDP protocole de datagramme utilisateur (*user datagram protocol*)

V2I de véhicule à infrastructure (*vehicle-to-infrastructure*)

V2P de véhicule à personne (*vehicle-to-person*)

V2V de véhicule à véhicule (*vehicle-to-vehicle*)

V2X de véhicule à tout (*vehicle-to-everything*)

VM multimédia dans le véhicule (*vehicular multimedia*)

VM I/P entrées du système multimédia dans le véhicule (*vehicle multimedia system inputs*)

VM O/P sorties du système multimédia dans le véhicule (*vehicle multimedia system outputs*)

VMN réseau multimédia dans le véhicule (*vehicular multimedia network*)

VMS système multimédia dans le véhicule (*vehicle multimedia system*)

VMSP plate-forme de services multimédias dans le véhicule (*vehicular multimedia service platform*)

VMU unité multimédia dans le véhicule (*vehicle multimedia unit*)

VR réalité virtuelle (*virtual reality*)

5 Conventions

Dans la présente Recommandation:

– L'expression "il est obligatoire que" (*is required to*) indique une prescription qui doit être strictement suivie et par rapport à laquelle aucun écart n'est autorisé si la conformité à la présente Recommandation doit être déclarée.

– L'expression "il est interdit que" (*is prohibited from*) indique une prescription qui doit être strictement suivie et par rapport à laquelle aucun écart n'est autorisé si la conformité à la présente Recommandation doit être déclarée.

– L'expression "il est recommandé que" (*is recommended*) indique une prescription qui est recommandée mais qui n'est pas absolument obligatoire. Par conséquent, cette prescription ne doit pas être présente pour déclarer la conformité.

– L'expression "il n'est pas recommandé que" (*is not recommended*) indique une prescription qui n'est pas recommandée mais qui n'est pas expressément interdite. Par conséquent, la conformité à la présente Recommandation peut toujours être revendiquée même si cette prescription est présente.

6 Contexte

Dans la présente Recommandation, les caractéristiques et les configurations des systèmes multimédias dans les véhicules (VMS) et le modèle de référence de l'architecture des systèmes VMS sont définis conformément aux spécifications indiquées dans la Recommandation [UIT-T F.749.3]. Le modèle de référence de la plate-forme de services multimédias dans les véhicules (VMSP), la pile de protocoles de référence pour la transmission par convergence, et le modèle de récepteur de référence des dispositifs embarqués pour les applications multimédias des systèmes VMS sont également définis. Les questions de sécurité des systèmes VMS et de protection et de confidentialité des informations d'identification personnelle identifiables (PII) sont également définies.

La Recommandation est organisée de la manière suivante:

Le § 7 définit les caractéristiques et les configurations des systèmes VMS. Le § 8 définit le modèle de référence de l'architecture des systèmes VMS. Le § 9 définit le modèle de référence de la plate-forme VMSP, la pile de protocoles de référence pour la transmission par convergence de contenus multimédias sur des réseaux hétérogènes, et le modèle de récepteur de référence des dispositifs embarqués. Le § 10 traite des questions de sécurité des systèmes VMS. Le § 11 traite des questions de protection et de confidentialité des informations PII.

7 Caractéristiques et configurations du système VMS

7.1 Caractéristiques du système VMS

Les caractéristiques du système VMS sont fondées sur les principes suivants:

– Expérience utilisateur, fonctions et applications de divertissement et d'information pour le conducteur et le passager.

– Exigences spécifiques du marché, de la région et du pays.

– Exigences légales et obligatoires.

Toutefois, les caractéristiques du système VMS ne décrivent pas l'architecture globale du réseau des véhicules ni l'intégration de plusieurs domaines dans les véhicules.

7.2 Configurations du système VMS

Les configurations du système VMS sont fondées sur les principes suivants:

– Les configurations du système VMS définissent des spécifications autonomes en matière de divertissement et d'affichage d'informations pour le conducteur et le passager.

– Il est recommandé de définir les configurations du système VMS au niveau des caractéristiques et des fonctions.

– Il est recommandé d'inclure les composants matériels au sein des configurations du système VMS.

– Plusieurs configurations du système VMS sont possibles.

– Il est recommandé d'avoir des configurations de VMS très variables, et de prendre en considération les produits VMS d'origine et les produits d'extension (*plug-in*) après fabrication.

Toutefois, les configurations du système VMS ne décrivent pas l'architecture globale du réseau des véhicules ni l'intégration de plusieurs domaines dans le véhicule.

7.2.1 Facteurs décisifs

Les configurations du système VMS sont déterminées en fonction des facteurs décisifs suivants:

– Spécifications d'utilisation.
– Caractéristiques, spécifications fonctionnelles.
– Spécifications en matière d'interface.
– Spécifications en matière de coûts.
– Spécifications après analyse comparative.

7.3 Liste des fonctionnalités du système VMS

Les caractéristiques de référence du système VMS sont résumées dans le Tableau 1.

Tableau 1 – Caractéristiques de référence du système VMS

Caractéristiques	Sous-caractéristiques	Configuration
Interface homme-machine (IHM)	Technologie d'affichage	Diode électroluminescente (LED)/écran à cristaux liquides (LCD)/diode électroluminescente organique (OLED), etc.
	Nombre d'écrans	Multiples (avant, central, arrière, etc.)
	Commande	Commandes classiques: Boutons/molettes/commandes tactiles, etc.
		Commandes intelligentes: Commande vocale, reconnaissance faciale, biométrie vocale, gestuelle, personnalisation, commande des mouvements oculaires, commande tactile à rétroaction, etc.
	Interaction multi-écrans	Information à déplacer vers différents écrans
		Affichage synchrone ou asynchrone de fichiers vidéo
		Double écran de navigation
		Adaptation libre de l'interface d'affichage
	Langue du système	Interface utilisateur: Spécifications linguistiques différentes selon les règlementations
	Écran pour la caméra	Caméra de recul (RVC)/Surveillance du périmètre de vision (AVM)
	Commande et affichage	Affichage et commandes pour le chauffage, la ventilation et la climatisation (HVAC)
		Commandes et affichage de l'aide à la conduite
Radiodiffusion	Terrestre	Analogique: Diffusion en modulation d'amplitude (AM), diffusion en modulation de fréquence (FM), diffusion FM avec double tuner et diversité de phase (PD), diffusion FM avec balayage de fond (BGS), système de données radio (RDS), etc.
		Numérique: Radiodiffusion numérique (DAB), radiodiffusion télévisuelle numérique de Terre (DTTB), technologies dans la même bande et dans la même voie (IBOC), radio numérique convergente (CDR), etc.
	Satellite	Services audio/vidéo par satellite (par exemple, service de diffusion audio/vidéo en continu par satellite)

Tableau 1 – Caractéristiques de référence du système VMS

Caractéristiques	Sous-caractéristiques	Configuration
Connectivité réseau externe	Réseaux cellulaires	3G/4G/5G
	Satellites bidirectionnels	Réseaux de communication bidirectionnelle par satellite en orbite terrestre basse (LEO)
		Réseaux de communication bidirectionnelle par satellite en orbite terrestre haute (HEO)
	De véhicule à tout (V2X)	De véhicule à véhicule (V2V), de véhicule à infrastructure (V2I), de véhicule à personne (V2P)
	Réseaux locaux sans fil	Points d'accès IEEE 802.11
Connectivité mobile à bord du véhicule		Appels et écoute de musique en mains libres à l'aide de réseaux personnels
		Surf sur le web en utilisant les réseaux locaux IEEE 802.11
		Partage d'écran à l'aide de réseaux de communication à courte distance
		Applications tierces d'interface avec le véhicule
Configurations télématiques	À distance	Télésurveillance, commande, transfert des données du véhicule
	Appels	Appel d'urgence (eCall), appel de dépannage (bCall), appel d'information (iCall)
Magasins/suites d'APP en ligne	Boutique d'APP	Nouvelles fonctionnalités téléchargées
	Place de marché à thème	Remplacement du thème
Mise à jour sans fil (OTA)		Logiciels OTA
Médias	Audio	Normale et haute-fidélité
	Image	Dans différents formats
	Vidéo	Vidéo normale avec diverses résolutions, réalité augmentée (AR), réalité virtuelle (VR), réalité mixte (MR)
Navigation	Navigation locale	
	Navigation sur le nuage	Données du modem du boîtier télématique (3G/4G/5G)/données mobiles de l'utilisateur
	Trafic en temps réel	Canal de messages de trafic (TMC), Groupe d'experts du protocole de transport (TPEG), centre de trafic en temps réel, etc.
	Services	Services de navigation, services de prévisions météorologiques en temps réel, etc.
	Fonctions avancées	Applications de voyage intelligentes telles que calendrier, planificateurs, etc.
Synthèse et reconnaissance vocale (RV)	VR locale, VR en nuage et synthèse	Compréhension du langage naturel
		Reconnaissance vocale automatique
		De texte à parole

Tableau 1 – Caractéristiques de référence du système VMS

Caractéristiques	Sous-caractéristiques	Configuration
Audio	Qualité audio	Réglage du volume de la fonction de vitesse
		Algorithmes sonores
		Suppression active du bruit (ANC)
		Paramètres de personnalisation (modèles sonores et reconnaissance faciale)
		Meilleur réglage de la position d'écoute
		Technologie de réduction de la qualité du son
	Configurations des amplificateurs	Amplificateurs intégrés à canaux multiples
		Amplificateurs avec haut-parleurs
	Configuration du son	Configurations multiples des haut-parleurs: tweeter (haut-parleur des aigus)/woofer (haut-parleur des graves)/haut-parleurs à large bande
Sécurité		Gestion des identités et de l'accès, authentification, autorisation et audit des transactions
		Sécurité des réseaux
		Sécurité opérationnelle
		Sécurité des applications
		Sécurité des logiciels OTA
		Sécurité du matériel
		Sécurité cryptographique
Vie privée		Considérations générales sur la protection des données
		Protection des informations personnelles
		Protection de la visibilité des données
		Confidentialité, intégrité et disponibilité
Caractéristiques intelligentes	Système de surveillance du conducteur (DMS)	Reconnaissance de la fatigue, des expressions et des émotions
	Santé	Moniteur de rythme cardiaque, moniteur de pression sanguine
	Environnement de bureau	Courriel, appels en visioconférence, projection holographique, reconnaissance des gestes, commande des mouvements oculaires, mémo manuscrit
	Jeux	Jeux de quiz interactifs basés sur la voix, jeux avec interaction holographique, jeux d'aventure
	Social	Applications sociales dans le véhicule

NOTE – Les caractéristiques de sécurité et de vie privée sont essentielles pour les systèmes VMS dans les configurations M1 à M5, mais sont configurables au système VMS dans la configuration M0. Des exemples de systèmes VMS dans les configurations M0 à M5 sont donnés à l'Appendice I de [UIT-T F.749.3].

8 Architecture du système VMS

Ce paragraphe définit la classification des fonctions du système VMS, les facteurs décisifs et le modèle de référence de l'architecture du système VMS.

8.1 Fonctions du système VMS

En général, les fonctions du système VMS peuvent être classées en trois catégories, à savoir les fonctions centrales du système VMS, les fonctions associées du système VMS et les fonctions partagées du système VMS.

Les fonctions centrales du système VMS sont les fonctions du système VMS qui traitent des données physiques, fonctionnelles et logiques du système VMS. Parmi les exemples de fonctions centrales du système VMS, citons le tuner, le traitement des médias, les fonctions d'affichage, etc.

Les fonctions associées du système VMS sont les fonctions du système VMS qui ne font que recevoir et afficher des données fonctionnelles et logiques provenant d'autres systèmes ou sous-systèmes. Parmi les exemples de fonctions associées au système VMS, citons le flux de la caméra du véhicule arrière, l'affichage d'informations eCall déclenché par un accident, etc.

Les fonctions partagées du système VMS sont les fonctions du système VMS qui sont utilisées par d'autres systèmes ou sous-systèmes afin de partager les données physiques, fonctionnelles et logiques et les informations de commande. Parmi les exemples de fonctions partagées du système VMS, citons les commandes de chauffage, de ventilation et de climatisation par l'intermédiaire de l'unité multimédia du véhicule (VMU), etc.

8.2 Facteurs décisifs de l'architecture du système VMS

Les éléments suivants sont des facteurs déterminants de l'architecture du système VMS:

– Spécifications techniques.
– Spécifications du système d'exploitation, de la mémoire et matérielles.
– Caractéristiques, spécifications fonctionnelles, des sous-systèmes, logiques et physiques.
– Spécifications en matière d'interface.
– Spécifications en matière de coûts.
– Spécifications d'utilisation.
– Spécifications après analyse comparative.
– Spécifications en matière de conformité standard.

8.3 Modèle de référence de l'architecture du système VMS

L'architecture du système VMS est définie au niveau de l'interface, des sous-systèmes et des systèmes. La Figure 1 présente un modèle de référence de l'architecture du système VMS.

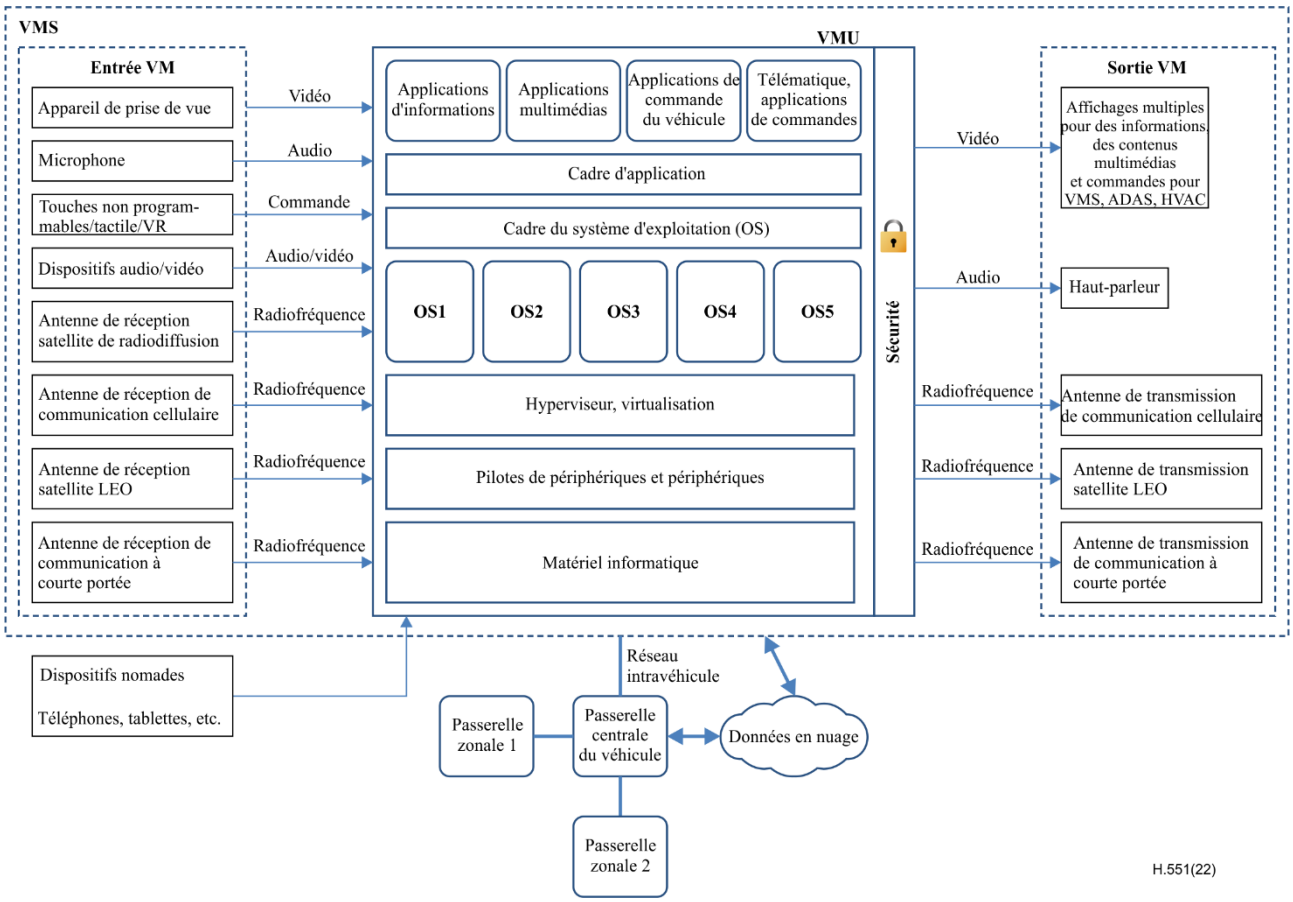

Figure 1 – Modèle de référence de l'architecture du système VMS

8.3.1 Applications

Les applications du système VMS comprennent:

– Les applications d'information, par exemple, groupe d'instrumentation, affichages tête haute, navigation et météo.

– Les applications multimédias, par exemple, médias, navigation, VR et IHM.

– Les applications de commande du véhicule, par exemple, chauffage, ventilation et climatisation et voitures connectées.

– Les applications télématiques, par exemple, commande à distance, diagnostics et accès aux données.

– Les applications d'affichage, par exemple, applications d'affichage avant et arrière.

8.3.2 Cadre d'application

Les caractéristiques et les fonctions du système VMS sont accessibles par le biais d'outils d'interface utilisateur conçus selon un cadre d'application.

8.3.3 Cadre du système d'exploitation (OS)

Le cadre du système d'exploitation gère les services du système. Il peut s'agir d'un cadre propriétaire de fabricants d'équipements d'origine (OEM) et de développeurs du système VMS.

8.3.4 OS

Divers noyaux et systèmes d'exploitation (OS) embarqués sont utilisés en fonction de la charge de traitement, de la vitesse et des exigences de précision.

8.3.5 Hyperviseur et virtualisation

Les techniques d'hyperviseur et de virtualisation sont utilisées pour prendre en charge plusieurs systèmes d'exploitation et tâches de traitement par un seul processeur de grande puissance grâce au partage des ressources informatiques.

8.3.6 Pilotes de périphériques et périphériques

Les pilotes de périphériques comprennent le pilote d'interface réseau du véhicule, les pilotes audio et vidéo, les pilotes d'affichage, les pilotes de protocole interprocesseurs et les pilotes de protocole intraprocesseurs.

8.3.7 Matériel informatique

Le matériel comprend les processeurs, la mémoire et d'autres composants.

8.3.8 Données en nuage

Les données en nuage comprennent:

– Les données pour les services multimédias.

– Les données pour les services télématiques, c'est-à-dire les services de diagnostic à distance, les services de mise à jour OTA des logiciels, les services bCall/iCall et les services de navigation.

9 Applications multimédias du système VMS

La Figure 2 décrit un système pour les applications multimédias du système VMS, qui se compose d'une plate-forme de services multimédias dans le véhicule (VMSP) dans le nuage, de réseaux hétérogènes et de dispositifs embarqués. Un schéma de transmission par convergence est utilisé pour améliorer l'efficacité de la transmission de contenus multimédias sur des réseaux hétérogènes, c'est-à-dire des réseaux de diffusion par satellite et des réseaux de communication mobile. Ce § décrit le modèle de référence de la plate-forme VMSP (§ 9.1), la pile de protocoles de référence pour la transmission par convergence de contenus multimédias sur des réseaux hétérogènes (§ 9.2), et le modèle de récepteur de référence des dispositifs embarqués (§ 9.3).

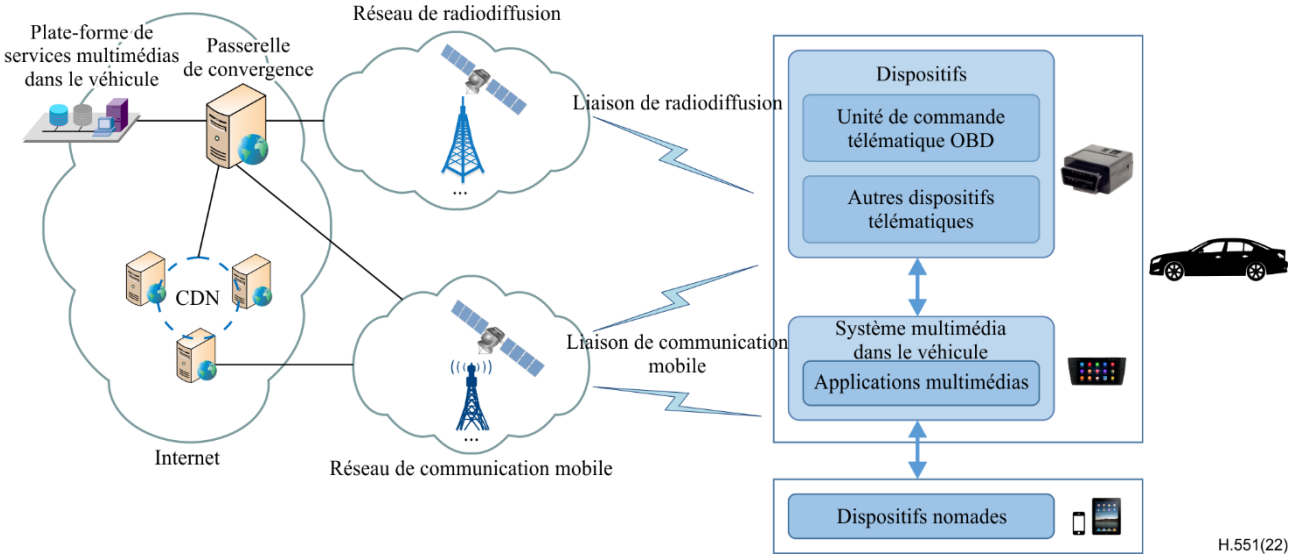

Figure 2 – Schéma d'un système d'applications multimédias du système VMS

9.1 Modèle de référence de la plate-forme VMSP

La plate-forme VMSP se compose d'un serveur de contenus, d'un serveur de licences (facultatif) et d'un serveur d'accès conditionnel (CA) (facultatif). Son modèle de référence est illustré sur la Figure 3.

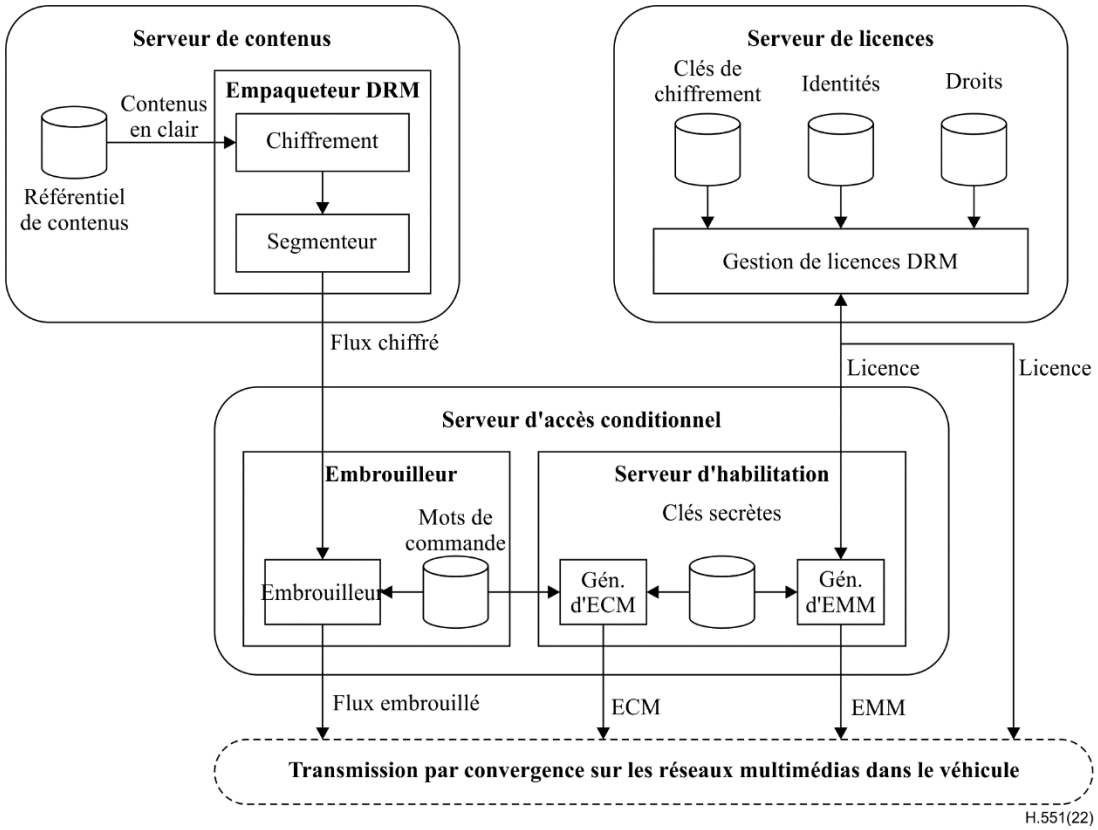

Figure 3 – Modèle de référence de la plate-forme VMSP

Le serveur de contenus se compose du référentiel de contenus et de l'empaqueteur de gestion des droits numériques (DRM). Le référentiel de contenus est utilisé pour stocker les contenus en clair que le fournisseur de contenus (CP) veut distribuer. Il convient de noter que le référentiel de contenus est souvent intégré à la solution DRM ou est parfois intégré à un système de gestion de contenus qui s'interface avec le serveur DRM. L'empaqueteur DRM crypte et met sous forme de paquets les contenus multimédias pour les diffuser en continu sur les réseaux VMN. Le serveur de licences est utilisé pour gérer la création, la modification et la révocation des licences DRM. La licence DRM contient les identités, la spécification des droits et les clés de chiffrement. En général, les clients DRM peuvent acquérir leurs licences DRM auprès du serveur de licences en utilisant des connexions de réseau de communication mobile. Les systèmes d'empaquetage candidats pour la diffusion en continu dans le réseau VMN comprennent MPEG-DASH [b-ISO/IEC 23009-1] et HLS [b-IETF RFC 8216].

Le serveur d'accès conditionnel (CA) se compose d'un embrouilleur et d'un serveur d'habilitation. L'embrouilleur est utilisé pour brouiller les flux entrants à l'aide de mots de commande. Le serveur d'habilitation est utilisé pour générer le message de commande d'habilitation (ECM) et le message de gestion d'habilitation (EMM). Habituellement, les flux embrouillés, ECM et EMM sortants sont acheminés par des réseaux de diffusion par satellite. Toutefois, les deux exceptions suivantes existent:

1) Lorsqu'un utilisateur se rend dans un endroit sans couverture de téléphonie mobile, il lui est impossible d'obtenir les licences DRM par un réseau de communication mobile. Dans ce cas, les licences DRM pourraient être intégrées dans les EMM et être délivrées à l'utilisateur via les réseaux satellitaires. Ainsi, la continuité du service pourrait être assurée.

2) Lorsqu'un opérateur de services démarre son activité, des milliers de nouveaux clients peuvent essayer d'activer leurs appareils en un court laps de temps. Cependant, la largeur de bande nécessaire à la diffusion des EMM pour ces dispositifs peut ne pas être disponible dans les réseaux de diffusion par satellite. Dans ce cas, les EMM pourraient être déchargés temporellement des réseaux de diffusion par satellite vers les réseaux de communication mobile. Ainsi, le succès du lancement de l'entreprise pourrait être garanti.

9.2 Pile de protocoles de référence pour la transmission par convergence

La radiodiffusion est généralement considérée comme le moyen le plus rentable de diffuser des programmes linéaires à une population importante sur de vastes zones géographiques. Malgré le succès de la diffusion DTV fixe en bandes Ka et Ku dans le monde, il est difficile de fournir ce service par diffusion aux véhicules. Par exemple, dans un environnement urbain, la fiabilité des communications de radiodiffusion reste tout de même problématique en raison du déplacement des récepteurs et du blocage fréquent du signal par les bâtiments de grande taille. Bien que le problème de la couverture urbaine par radiodiffusion puisse être résolu par des réseaux de répéteurs au sol qui pallient les pannes, la construction de ce type d'infrastructure est à la fois coûteuse et très longue. Une autre limitation à la communication par radiodiffusion réside tient au fait qu'elle fournit uniquement des services unidirectionnels et donc qu'elle est incapable d'offrir des services personnalisés ou de prendre en charge les interactions entre utilisateurs.

Pour relever ces défis, un schéma de transmission par convergence est proposé pour la transmission de contenus multimédias sur les réseaux VMN, où la plupart des contenus multimédias sont acheminés aux utilisateurs de manière massive par le biais des réseaux de radiodiffusion, et où les réseaux de communication mobile ne sont utilisés que pour récupérer les paquets qui ont été laissés de côté par les réseaux de radiodiffusion. Les flux embrouillés provenant de la plate-forme VMSP sont envoyés aux passerelles de convergence, où les segments de média sont ensuite mis sous forme de paquets séquencés et diffusés à tous les utilisateurs sur le réseau satellitaire. Au niveau du terminal, il est facile de détecter les paquets manquants ou erronés des flux de radiodiffusion. Ces paquets abandonnés sont récupérés par retransmission sur le réseau de communication mobile. Une fois les flux multimédias réassemblés sans discontinuité, le terminal peut non seulement les diffuser sur les écrans et les haut-parleurs du cockpit, mais peut aussi servir de centre d'infodivertissement local pour partager ces flux multimédias en WiFi avec tous les passagers à l'aide de leurs appareils personnels tels que les smartphones et les tablettes. Le schéma de transmission par convergence est illustré sur la Figure 4.

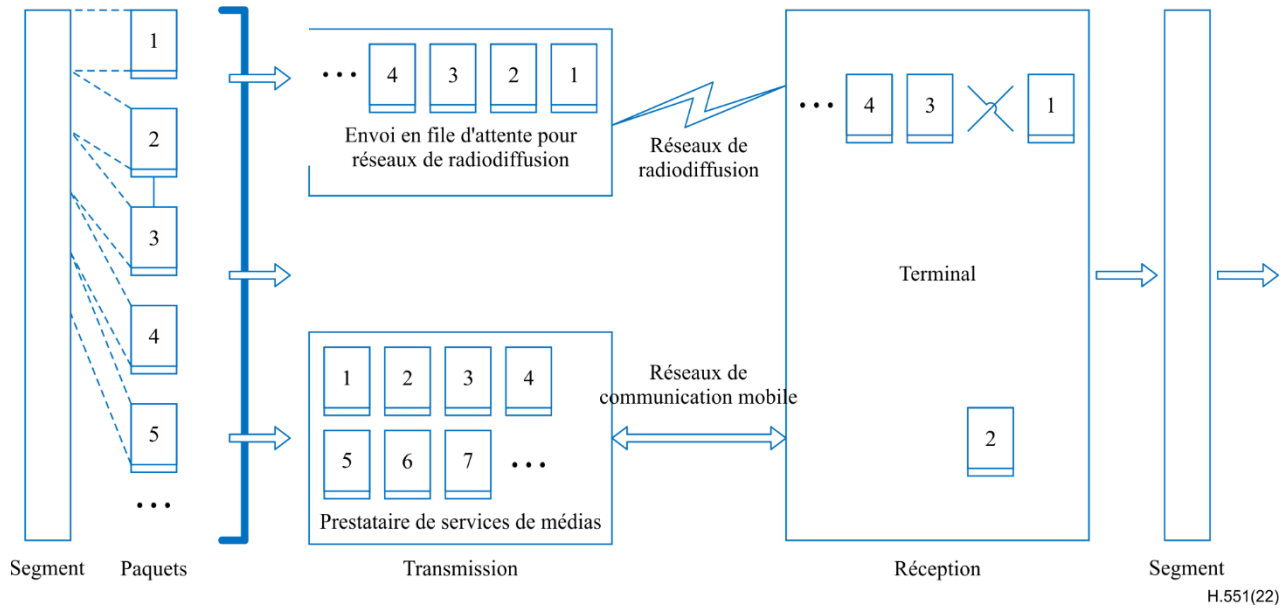

Figure 4 – Traitement de la transmission par convergence

Le schéma de transmission par convergence tire pleinement parti des atouts complémentaires des réseaux de radiodiffusion et des réseaux de communication mobile. Ainsi, l'efficacité du système de services de diffusion multimédia en continu sur le réseau VMN est optimisée.

La pile de protocoles de référence pour la transmission par convergence de contenus multimédias sur le réseau VMN est présentée sur la Figure 5. Il convient de noter que les protocoles de transmission par convergence sont agnostiques par rapport aux normes de la couche physique sous-jacente et sont transparents pour les normes de la couche supérieure. Ainsi, des modifications minimales aux infrastructures de diffusion ou de communication mobile existantes peuvent être garanties.

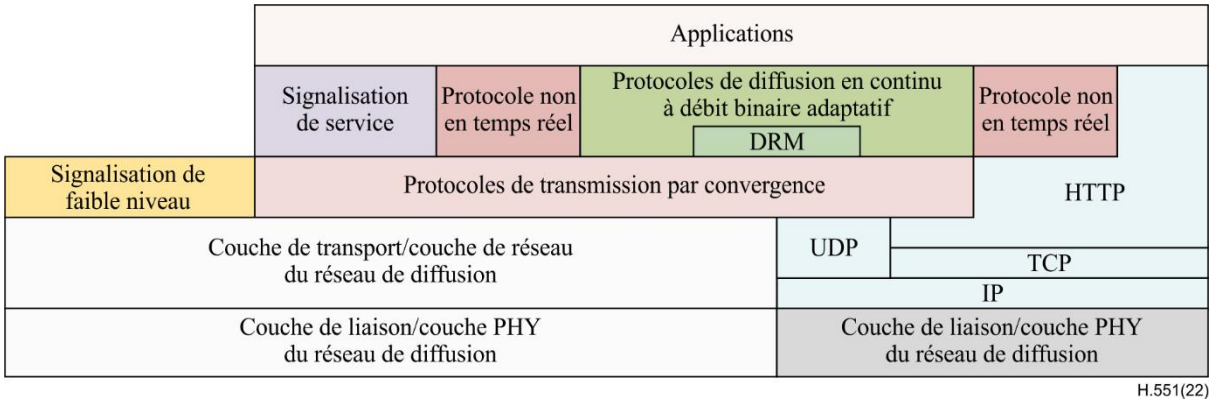

Figure 5 – Pile de protocoles de référence pour la transmission par convergence

L'hypothèse générale est que le protocole de la couche réseau peut être basé sur les deux versions du protocole IP (IPv4 et IPv6). Il est conseillé de choisir le protocole IPv6 [b-IETF RFC 8200] pour une connectivité directe et sécurisée entre le VMS et les plates-formes en nuage, pour les raisons suivantes:

– L'IETF préconise très clairement aux autres organismes de normalisation (SDO) de privilégier le protocole IPv6 [b-IAB]. En conséquence, il est recommandé de procéder à des travaux de normalisation pour prendre en charge le protocole IPv6.

– L'espace d'adresses IPv4 a été officiellement épuisé en janvier 2011, lorsque l'Internet Assigned Numbers Authority (IANA) a attribué son dernier espace d'adresses de premier niveau IPv4 (c'est-à-dire/8). Par conséquent, l'adoption du protocole IPv6 comme seul protocole de réseau représente la seule solution viable pour garantir l'évolution des services et des applications réseau.

– La transition vers le protocole IPv6 seul est considérée comme une initiative stratégique par plusieurs organismes gouvernementaux. Un exemple, parmi d'autres, est représenté par [b-USG OMB], où le gouvernement fédéral américain fixe des délais et des objectifs spécifiques pour la migration des réseaux des agences nationales vers le protocole IPv6.

– Les dispositifs des utilisateurs situés dans un véhicule peuvent avoir besoin d'une accessibilité de bout en bout, par exemple pour se connecter à des applications et des plates-formes. Il s'agit d'un cas où la traduction d'adresse réseau (NAT) [b-IETF RFC 2663] associée à l'adressage IPv4 privé ne peut être utilisée. À l'inverse, le protocole IPv6 prend pleinement en charge un schéma d'adressage global dans lequel les dispositifs des utilisateurs sont toujours joignables.

Bien que les utilisateurs connaissent mieux le protocole IPv4 et que le déploiement du protocole IPv6 présente certains nouveaux problèmes, la croissance des utilisateurs et du trafic du protocole IPv6 est beaucoup plus rapide que celle du protocole IPv4. Cela signifie que pour l'avenir, tout bien considéré, les professionnels du secteur ont opté collectivement et avec sagesse pour le protocole IPv6 [b-ETSI WP35].

9.3 Modèle de récepteur de référence

La Figure 6 présente le modèle de récepteur de référence des dispositifs embarqués, où les fonctions suivantes sont identifiées:

– Les connexions de radiodiffusion et les connexions à large bande qui fournissent la connectivité nécessaire pour que le récepteur reçoive la signalisation et les données.

– La pile de protocole de transmission par convergence/UDP/HTTP/TCP/IP et la pile HTTP/TCP/IP qui fournissent des protocoles de transport orientés objet pour que le récepteur reçoive des ressources de diffusion en continu à débit binaire adaptatif (par exemple, DASH ou HLS) pour des services de diffusion en continu de multimédias.

– Signalisation de niveau faible: Signalisation fournie sur les réseaux de radiodiffusion qui permet au récepteur de construire une liste de services de base et d'amorcer la découverte de la signalisation de service pour chaque service multimédia.

– Signalisation de service: Signalisation liée au service qui permet au récepteur de découvrir et d'accéder à des services de diffusion multimédia en continu et à leurs composants de contenus.

– Cache: Stockage et traitement temporaires des manifestes, des segments d'initialisation et des segments de média dont la réception est facilitée par la signalisation de service.

– Serveur de diffusion en continu à débit binaire adaptatif (c'est-à-dire DASH/HLS): serveur local de diffusion en continu à débit binaire adaptatif qui est utilisé pour abstraire les couches sous-jacentes du client de diffusion en continu à débit adaptatif. Pour le client de diffusion en continu à débit binaire adaptatif, les manifestes, les segments d'initialisation et les segments de média sont fournis par le serveur de diffusion en continu à débit binaire adaptatif.

– Client de diffusion en continu à débit binaire adaptatif: fonction qui consomme des manifestes et des segments, et communique avec d'autres composants du récepteur afin de personnaliser l'expérience média en fonction des capacités de la plate-forme, des préférences de l'utilisateur et de son interaction.

– Application: application native ou téléchargée qui utilise des données diffusées ou fournies en haut débit afin de fournir une présentation riche et interactive à l'utilisateur final.

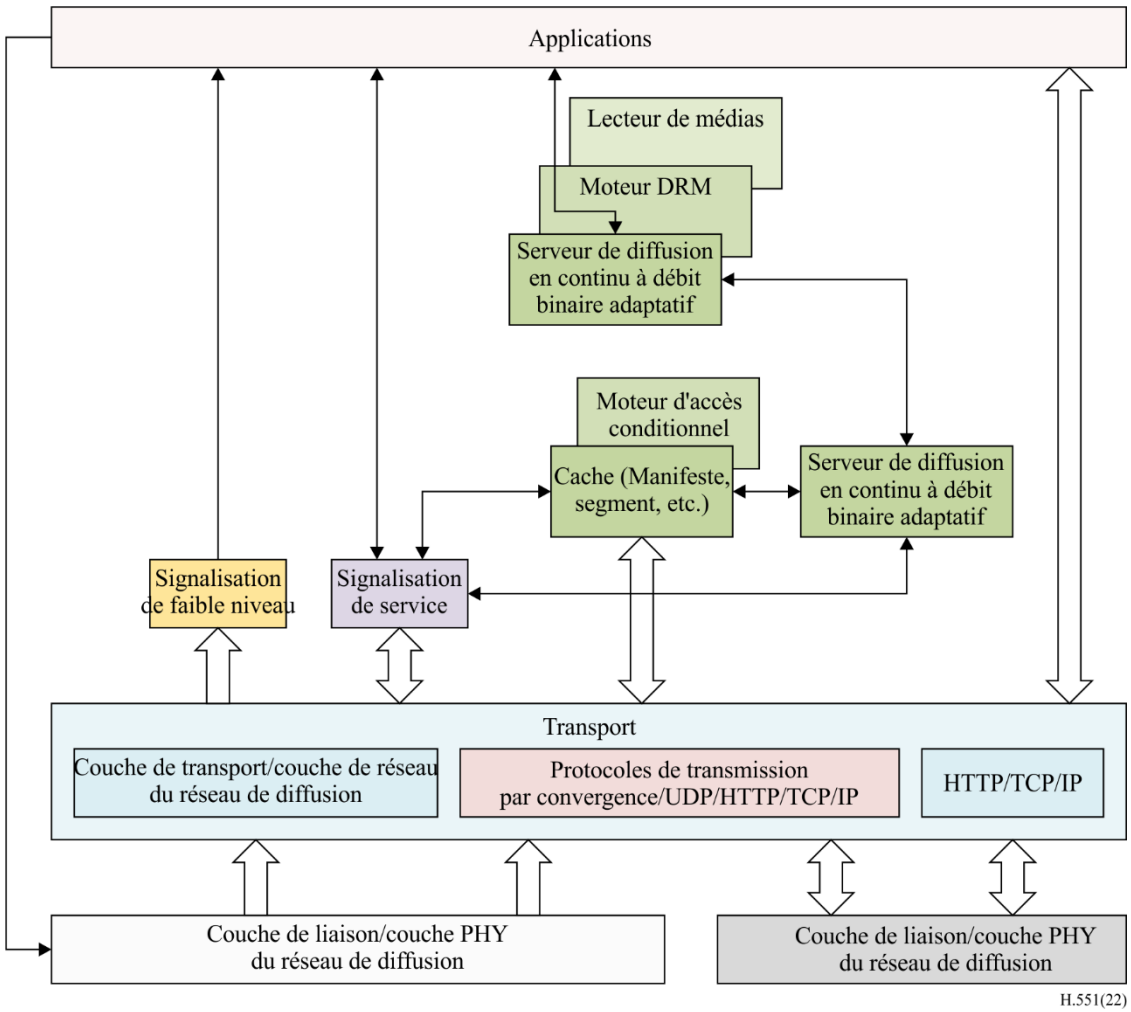

Figure 6 – Modèle de récepteur de référence des dispositifs embarqués

Une séquence type d'amorçage du récepteur de référence est présentée ci-après:

– L'application demande une liste de services préconfigurés dans une signalisation de niveau faible. La liste des services est transmise à l'application, qui fournit ensuite une interface utilisateur pour la sélection des services de diffusion multimédia en continu. L'utilisateur choisit un service de diffusion multimédia en continu à consommer.

– L'application utilise les informations du point d'entrée de la signalisation de service contenues dans la liste de services pour le service sélectionné afin de fournir des informations d'accès à la pile de protocole de transmission par convergence/UDP/HTTP/TCP/IP afin de récupérer la signalisation de service. La signalisation de service est fournie à l'application.

– En utilisant la signalisation de service, l'application fournit des informations d'accès à la pile de protocole de transmission par convergence/UDP/HTTP/TCP/IP pour télécharger les composants médias formatés pour la diffusion en continu à débit binaire adaptatif du service sélectionné, lesquels sont envoyés vers le cache pour y être stockés, désembrouillés puis transmis au serveur de diffusion en continu à débit binaire adaptatif.

– Lors de la sélection d'un service, l'application active le client de diffusion en continu à débit binaire adaptatif, amenant le client DASH/HLS à demander et à recevoir des segments de média du serveur de diffusion en continu à débit binaire adaptatif aux heures de début de disponibilité des segments de média ou après celles-ci.

– Lors de la réception des segments de média, la fonction composite comprenant le client de diffusion en continu à débit binaire adaptatif, le moteur DRM et le lecteur de médias décode les segments de média reçus, et le média décodé est renvoyé à l'application pour y être lu.

10 Sécurité du système VMS

Il est recommandé que les interactions entre le système VMS et les autres composants impliqués dans la sécurité d'une voiture (généralement l'unité de commande électronique (ECU)) soient limitées aux fonctions partagées mentionnées dans le § 8.1.

Les détails sont donnés à l'Annexe A.

11 Protection et confidentialité des informations d'identification personnelle (PII)

Il est recommandé que le système VMS assure une protection de bout en bout à mesure que les véhicules deviennent connectés et offrent des services plus interactifs. De plus en plus de données utilisateur et d'informations relatives à la vie privée doivent être protégées pour garantir la confidentialité et l'intégrité des données utilisateur stockées dans le VMS, dans le véhicule et dans le nuage ou les serveurs dorsaux du système VMS.

Les détails sont donnés dans l'Annexe B.

Annexe A

Sécurité du système VMS

(Cette Annexe fait partie intégrante de la présente Recommandation.)

A.1 Aperçu

Il est recommandé que les interactions entre le système VMS et les autres composants liés à la sécurité d'une voiture (généralement l'ECU) soient limitées aux fonctions partagées mentionnées dans le § 8.1. En effet, il est recommandé que le système VMS n'influence pas négativement les fonctions des autres composants qui assurent la sécurité nécessaire d'une voiture, notamment dans le cas des véhicules à conduite autonome.

En ce qui concerne la sécurité du système VMS, les menaces présumées pour le système VMS et son écosystème sont résumées dans le § A.2, et les capacités de sécurité contre les menaces sont fournies à titre de référence, pour information, dans le § A.3.

A.2 Menaces présumées pour le système VMS et son écosystème

A.2.1 Menaces liées à la plate-forme de services multimédias dans le véhicule (VMSP)

Ces dernières années, la connectivité des véhicules s'est considérablement diversifiée et la connectivité avec différents serveurs situés au niveau de la plate-forme VMSP, en particulier, est devenue absolument indispensable. Dans le contexte du système VMS, les serveurs dorsaux sont reconnus comme une plate-forme VMSP, y compris les serveurs fournis par le fabricant OEM, les serveurs fournis par le fournisseur et les serveurs fournis par les services TIC pour prendre en charge l'écosystème des véhicules depuis le système dorsal distant. Les menaces suivantes peuvent être identifiées concernant la plate-forme VMSP:

– Serveurs de la plate-forme VMSP utilisés pour attaquer un véhicule ou extraire des données.
– Perturbation des services fournis par la plate-forme VMSP.
– Perte ou compromission des données stockées sur des serveurs de la plate-forme VMSP.

A.2.2 Menaces pour les véhicules liées à leurs canaux de communication

Les communications du véhicule comprennent les communications externes par le biais de réseaux cellulaires, de satellites LEO, de réseaux de radiodiffusion et de réseaux à courte portée. Les canaux utilisés pour ces communications peuvent être la cible d'attaques telles que la simulation, l'interception, la manipulation de messages, etc. Les menaces suivantes peuvent être identifiées en relation avec les canaux de communication:

– Manipulations, suppressions ou autres modifications non autorisées du code/des données du véhicule.
– Utilisation des interfaces VM pour accéder à d'autres infrastructures (intelligentes) à l'intérieur du véhicule (par exemple, l'ECU sans rapport avec le VMS).
– Utilisation de messages non fiables/non sécurisés et attaques par détournement/répétition de session.
– Comme les applications du VM peuvent être mises à jour sans fil, ces attaques peuvent également s'appliquer au VM.
– Divulgation d'informations.
– Voir le § 9 de [UIT-T F.749.3].
– Attaques par déni de service.
– Le VM lui-même peut ne pas avoir accès à l'infrastructure critique du véhicule, mais peut servir de passerelle pour ces attaques.

– Accès privilégié par un utilisateur sans privilèges.
– Étant donné que des comptes d'utilisateurs personnalisés peuvent être associés aux applications du VM, un accès sans privilèges est possible. L'accès sans privilèges via le VM peut ne pas fournir d'accès direct à l'infrastructure critique (par exemple, accès root; accès au système de freinage), mais peut à nouveau servir de passerelle pour accéder à l'infrastructure du véhicule.
– Logiciels malveillants intégrés dans les moyens de communication.
– Les VM intelligents reposent sur le transfert de données entre le système VMS et une plate-forme VMSP dans le nuage. En pénétrant ce canal de communication, les attaquants peuvent utiliser les messages/transferts de données de la plate-forme VMSP au système VMS pour déployer des logiciels malveillants.
– Messages comportant des contenus malveillants.
– Les VM intelligents reposent sur le transfert de données entre le système VMS et, par exemple, une plate-forme VMSP dans le nuage. En pénétrant ce canal de communication, les attaquants peuvent modifier les messages/transferts de données entre la plate-forme VMSP et le système VMS afin d'accéder au système VMS et/ou aux ECU du véhicule intelligent ciblé.

A.2.3 Menaces pour les véhicules liées à leurs procédures de mise à jour

La mise à jour des systèmes du véhicule peut se faire de deux manières, à savoir par voie filaire sur un port de diagnostic embarqué (OBD), ou à l'aide de dispositifs portables, par exemple une carte numérique sécurisée (SD), ou d'un flash drive USB, et sans fil. Le logiciel à mettre à jour peut être un micrologiciel ou les données de configuration du véhicule. La plupart des problèmes électroniques et des défauts logiciels peuvent être mis à jour et résolus par voie électronique sans accès physique, par exemple au moyen d'un testeur OBD. En outre, les mises à jour sans fil permettent de raccourcir le cycle de mise à jour, de façon à limiter le plus possible l'exposition à des attaques en ce qui concerne les vulnérabilités connues du logiciel. Les menaces suivantes peuvent être identifiées en rapport avec les procédures de mise à jour:

– Utilisation abusive ou compromission des procédures de mise à jour.
– Quelle que soit la mise à jour utilisée – mise à jour sans fil ou mise à jour locale/physique –, la procédure de mise à jour peut s'accompagner de menaces qui consistent à créer de toutes pièces des programmes de mise à jour du système ou à utiliser des microgiciels compromis.
– Le logiciel peut être manipulé avant le processus de mise à jour, bien que ce processus soit intact. Le fournisseur de logiciel crée/prépare son logiciel aux fins de la mise à jour et celui-ci est fourni aux systèmes visés nécessitant la mise à jour. En conséquence, il existe un risque grave que le logiciel soit manipulé et corrompu avant d'être utilisé.
– En particulier pendant la procédure de mise à jour, les données de chiffrement, telles que les clés et les certificats de chiffrement utilisés dans la mise à jour logicielle, peuvent être compromises, ce qui peut entraîner une mise à jour invalide ou malveillante du logiciel.
– Déni de service et refus de mise à jour légitime.
– Une attaque par déni de service contre le serveur ou le réseau de mise à jour pour empêcher le déploiement de mises à jour critiques du logiciel et/ou le déverrouillage de fonctionnalités propres au client peut constituer une attaque possible dans la procédure de mise à jour du logiciel. Il est également possible de refuser des mises à jour légitimes.

A.2.4 Menaces pour les véhicules liées à leur connectivité et leurs connexions externes

Pour fournir divers services pratiques, les véhicules peuvent être équipés de composants permettant de communiquer avec les serveurs de la plate-forme VMSP et peuvent communiquer avec tout ce qui est rendu possible par les usagers de la route sur une connexion hertzienne. Outre les fonctionnalités

pratiques, il existe des avantages sur le plan de la sécurité tels que la fonctionnalité que constitue le système automatique d'appel d'urgence ainsi que les fonctionnalités assurées par les communications V2X. Toutefois, plus les véhicules assurant une connexion avec des entités externes pour améliorer la connectivité sont nombreux, plus il y a de risques de menaces et de vulnérabilités, étant donné que les interfaces additionnelles élargissent la surface vulnérable du système. Les menaces suivantes peuvent être identifiées en rapport avec la connectivité et les connexions externes:

– Manipulation de la connectivité des fonctions du véhicule.

  Le système VMS ne fournit pas d'accès direct aux fonctions critiques du véhicule, mais il peut être utilisé comme passerelle pour accéder à ces composants critiques, par exemple les ECU dédiés.

– Logiciels tiers embarqués.

  Les applications du système VMS peuvent être incluses dans la classe des "logiciels tiers embarqués".

– Dispositifs connectés à des interfaces externes.

  Comme le souligne [UIT-T F.749.3], la connectivité peut être basée sur des dispositifs intégrés tels que les smartphones.

A.3 Capacités de sécurité basées sur les menaces identifiées

A.3.1 Gestion des identités et de l'accès (IAM), authentification, autorisation et audit des transactions

Plusieurs administrateurs et utilisateurs interviennent dans les services du système VMS, et ces services sont accessibles et utilisés en interne et en externe. Il est donc nécessaire de gérer les identités, non seulement pour protéger ces identités, mais aussi pour faciliter les processus de gestion de l'accès, d'authentification, d'autorisation et d'audit des transactions dans une telle infrastructure du système VMS dynamique et ouverte.

La gestion IAM a besoin d'un ou plusieurs modèles de confiance communs pour authentifier les identités; les développeurs, les hyperviseurs et d'autres éléments du système ont eux aussi besoin de ces modèles de confiance pour authentifier les éléments du système comme les modules logiciels, les applications ou les ensembles de données téléchargés.

La gestion IAM contribue à la confidentialité, à l'intégrité et à la disponibilité des services et des ressources et devient à ce titre incontournable dans le système VMS. En outre, la gestion IAM peut permettre de mettre en œuvre l'authentification unique et la fédération d'identités pour le système VMS qui utilise des mécanismes d'authentification différents ou qui sont répartis dans des domaines de sécurité différents.

L'audit des transactions protège contre la répudiation, permet une analyse sur le plan légal après une atteinte à la sécurité et dissuade les attaques (qu'elles viennent de l'intérieur ou de l'extérieur). L'audit des transactions est plus qu'un simple enregistrement, puisqu'il comprend une surveillance active pour repérer les activités suspectes.

A.3.2 Sécurité des interfaces

Cette capacité sécurise, d'une part, les interfaces ouvertes aux développeurs du système VMS et/ou à d'autres fournisseurs de la plate-forme VMSP sous contrat, par l'intermédiaire desquels différents types de VMS sont fournis et, d'autre part, sécurise les communications fondées sur ces interfaces. Les mécanismes disponibles pour assurer la sécurité des interfaces sont notamment les suivants: authentification unilatérale/mutuelle, total de contrôle d'intégrité, chiffrement de bout en bout et signature numérique.

A.3.3 Sécurité du réseau

Dans un environnement VMS, la sécurité du réseau permet d'isoler à la fois le réseau physique et le réseau virtuel et de sécuriser les communications entre tous les participants. Elle permet de procéder à la partition des domaines de sécurité du réseau, de contrôler l'accès aux frontières du réseau (par exemple, avec un pare-feu), de détecter et d'empêcher les intrusions, d'assurer la séparation du trafic dans le réseau en fonction des politiques de sécurité et de protéger le réseau contre les attaques dans les environnements de réseaux virtuels ou physiques.

A.3.4 Sécurité opérationnelle

Cette capacité assure une protection de sécurité pour le fonctionnement et la maintenance au quotidien de l'infrastructure du système VMS et de la plate-forme VMSP.

Cette capacité de sécurité fonctionnelle:

– définit des ensembles de politiques de sécurité et des activités de sécurité telles que la gestion de la configuration, la mise à jour des correctifs, l'évaluation de la sécurité, la réaction aux incidents;

– surveille les mesures de sécurité de la plate-forme VMSP et leur efficacité et transmet les rapports pertinents aux VMS concernés.

Si les mesures de sécurité de la plate-forme VMSP ou leur efficacité évoluent, tous les systèmes VMS en aval en seront informés.

Ces rapports et alertes permettent aux systèmes VMS autorisés de consulter les incidents, les informations d'audit et les données de configuration se rapportant à leurs systèmes VMS.

A.3.5 Mises à jour des logiciels et micrologiciels

Les mises à jour OTA sécurisées doivent être conformes aux normes de sécurité de base. Il est recommandé que le processus de mise à jour tienne compte des facteurs opérationnels (par exemple, le calendrier des mises à jour et les processus de chiffrement/déchiffrement). La présence de plusieurs fabricants OEM et de vendeurs tiers contribue à l'existence de différentes interfaces de sous-systèmes au sein d'un même véhicule. Ainsi, toute vulnérabilité ou tout risque cybernétique visant ces fabricants OEM ou fournisseurs peut effectivement détourner une mise à jour logicielle OTA légitime, laquelle est ensuite envoyée sous forme de données en nuage pour être déployée dans d'autres véhicules.

Il est recommandé de concevoir, de mettre en œuvre et d'exploiter un mécanisme de mise à jour des logiciels et micrologiciels des systèmes VMS (ECU et systèmes connexes).

Dans le cadre du développement de service du système VMS, il est recommandé de concevoir et de mettre en œuvre un mécanisme de mise à jour des logiciels et micrologiciels des systèmes VMS en tant que fonction de base. Il est également recommandé de mettre en place, dès la conception, un mécanisme de retour en arrière des logiciels et micrologiciels, à utiliser en cas d'échec d'une mise à jour.

Dans le cadre de l'utilisation et de la prise en charge du service du système VMS, la signature numérique, les certificats de signature et la chaîne de certificats de signature du paquet de mise à jour du logiciel/micrologiciel sont vérifiés par le dispositif avant le début du processus de mise à jour.

Il est recommandé d'utiliser des clés de chiffrement pour mettre à jour la protection de l'intégrité et gérer la confidentialité de manière sécurisée pour l'utiliser de manière appropriée. Lorsque les mises à jour sont effectuées sans fil (OTA), il est recommandé d'utiliser des canaux de communication chiffrés.

Enfin, il est recommandé que les mises à jour par OTA réussissent complètement ou échouent de manière récupérable. En cas d'échec de la mise à jour, il est recommandé de revenir à la dernière bonne configuration connue et de ne pas pouvoir désactiver la connexion d'un appareil au serveur de mise à jour.

A.3.6 Sécurité des applications

Ces capacités de sécurité sont souvent utilisées pour améliorer la sécurité d'une "application VMS" le plus souvent en trouvant, en corrigeant et en prévenant les failles de sécurité dans le VMS et son écosystème. Différentes techniques sont utilisées pour faire apparaître ces vulnérabilités de sécurité à différentes étapes du cycle de vie d'une application, comme la conception, le développement, le déploiement, la mise à niveau et la maintenance.

A.3.7 Gestion des incidents

La gestion des incidents consiste à surveiller les incidents, à les prévoir, à déclencher une alerte et à intervenir. Afin de savoir si le VMS fonctionne comme prévu dans l'ensemble de l'infrastructure, une surveillance continue est nécessaire (par exemple, surveillance des performances en temps réel des serveurs utilisés dans la plate-forme VMSP). Les systèmes peuvent ainsi rendre compte de l'état de la sécurité des services, identifier les anomalies et avertir immédiatement en cas de surcharge du système de sécurité, d'atteinte à la sécurité, de discontinuité du service, etc. Lorsqu'un incident de sécurité se produit, le problème est identifié et l'incident est rapidement réglé, que ce soit de manière automatique ou grâce à l'intervention d'un administrateur humain. Les incidents résolus sont enregistrés et analysés afin de dégager d'éventuels schémas sous-jacents qui peuvent ensuite être traités préventivement.

A.3.8 Cryptographie

Cette capacité garantit la confidentialité et l'intégrité des données utilisées et échangées dans le VMS et ses écosystèmes. Il s'agit de la méthode de base pour stocker et transmettre des données sous une forme particulière afin que seuls ceux à qui elles sont destinées puissent les lire et les traiter. Cette capacité protège non seulement les données VMS contre le vol ou encore l'altération, mais elle peut également être utilisée pour l'authentification des utilisateurs, etc.

Comme bon exemple de mise en œuvre du chiffrement, les lignes directrices pour la sélection des primitives cryptographiques pour les systèmes IPTV sont données dans [b-UIT-T X.1197 Amd1] et peuvent être appliquées aux flux multimédias dans les systèmes présents dans les véhicules, dans la mesure où ceux-ci ont le même niveau d'importance/criticité que les flux multimédias dans les systèmes IPTV hors véhicules. De même, pour les véhicules dotés d'une connectivité 5G, [b-UIT-T X.1811] prodigue des conseils supplémentaires sur la manière de mettre en œuvre les niveaux de sécurité de base de [b-UIT-T X.1197 Amd1], notamment pour les flux multimédias.

En outre, avec une solution DRM fondée sur un chiffrement fort et authentifié, destiné à ne permettre qu'à un contenu légitime et protégé par des droits d'auteur d'être consommé par le système d'infodivertissement, seuls les flux multimédias externes légitimes en visibilité directe seraient pris en compte par le système d'infodivertissement et d'aide à la conduite, permettant ainsi au trafic de se poursuivre sans aucune perturbation.

A.3.9 Sécurité du matériel

Cette capacité vise à éliminer les vulnérabilités et les faiblesses de sécurité inhérentes au matériel informatique du système VMS, et assure un environnement sécurisé pour la mise en œuvre au niveau matériel. En particulier, il est devenu essentiel de mettre en œuvre de nombreuses fonctions de chiffrement fondamentales dans le matériel, telles que la gestion des clés de chiffrement, l'exécution du chiffrement/déchiffrement et la fourniture de signatures numériques et d'une authentification forte, qui sont très largement utilisées pour assurer la sécurité dans les systèmes VMS. À cette fin, il est

nécessaire de concevoir et de vérifier le fonctionnement du matériel connexe de manière sécurisée dès la phase de conception du matériel, en tenant compte des éventuelles menaces et attaques.

Par exemple, pour assurer la sécurité au niveau de l'ECU dans l'architecture du système VMS, il est recommandé que chaque ECU implémenté soit protégé par des HSM et des PUF, qui sont des composants classiques des modules de sécurité matériels.

A.3.10 Capacités générales de sécurité

NOTE – Les capacités de sécurité suivantes sont facultatives pour la présente Recommandation. Toutefois, ces capacités peuvent être utilisées efficacement pour améliorer la sécurité du système VMS.

– Évaluation et audit de la sécurité.

  Cette capacité permet d'évaluer la sécurité du système VMS. Grâce à elle, un tiers habilité vérifie qu'un système VMS respecte les exigences de sécurité applicables. L'évaluation de la sécurité ou l'audit de sécurité pourrait être réalisé par le système VMS, la plate-forme VMSP ou un tiers, tandis qu'un tiers habilité pourrait effectuer la certification de sécurité.

  Des critères de sécurité adaptés sont appliqués pour que le système VMS et la plate-forme VMSP aient la même compréhension du niveau de sécurité.

– Modèle de confiance.

  Tout système dans lequel plusieurs fournisseurs coopèrent pour fournir un service fiable nécessite un modèle de confiance commun.

  Étant donné qu'il fait intervenir par nature de multiples parties prenantes, l'environnement VMS devra comprendre un modèle de confiance général. Ce modèle de confiance permettra de créer des îlots et/ou des fédérations d'entités de confiance, de telle sorte que des éléments distincts du système pourront authentifier l'identité et les droits autorisés d'autres entités et éléments. Chaque îlot ou fédération de confiance reposera sur une ou plusieurs autorités de confiance (par exemple, une autorité délivrant des certificats d'infrastructure de clé publique (PKI)).

– Isolation et protection des données.

  a) Isolation des données

     L'isolation des données peut être logique ou physique, selon la granularité d'isolation requise et le modèle de déploiement des logiciels et des équipements d'informatique du système VMS utilisés.

  b) Protection des données

     La protection des données garantit que les données du système VMS et les données dérivées détenues dans une VMSP sont protégées comme il se doit afin que seules les personnes ou entités autorisées par le système VMS puissent avoir accès à ces données ou les modifier. Cette protection peut associer plusieurs méthodes: listes de contrôle d'accès, vérification de l'intégrité, correction des erreurs/récupération des données, chiffrement et autres mécanismes appropriés.

  Lorsqu'une plate-forme VMSP assure le chiffrement des mémoires pour les systèmes VMS, cette fonction peut correspondre à un chiffrement du côté du client (par exemple, dans une application CSP) ou du côté du serveur.

– Coordination de la sécurité

  Étant donné que différents systèmes VMS supposent différentes mises en œuvre de contrôle de sécurité, cette capacité de sécurité coordonne des mécanismes de sécurité hétérogènes pour éviter les conflits en matière de protection.

  Les parties jouant différents rôles dans l'écosystème du système VMS ont des niveaux différents de contrôle des ressources et des services physiques ou virtuels, notamment en ce qui concerne le contrôle de la sécurité.

Pour chaque partie, il y aura divers mécanismes de sécurité, comme l'isolation du superviseur, la gestion IAM, la protection des réseaux, etc.

La coordination de la sécurité dépend de l'interopérabilité et de l'harmonisation des divers mécanismes de sécurité.

– Sécurité de la chaîne d'approvisionnement

Une plate-forme VMSP fait appel à plusieurs fournisseurs pour mettre en place ses services. Certains d'entre eux appartiennent au secteur du système VMS, tandis que d'autres seront des équipementiers ou des fournisseurs de services de technologie de l'information traditionnels, par exemple des fabricants de matériel n'ayant pas de lien direct avec le VMS. Cette capacité permet d'établir une relation de confiance entre la plate-forme VMSP et tous les participants à la chaîne d'approvisionnement grâce à des activités de sécurité. Ces activités de sécurité consistent, d'une part, à recenser et à rassembler des informations sur les composants et les services achetés par la plate-forme VMSP et utilisés pour fournir des systèmes VMS et, d'autre part, à appliquer les politiques de sécurité dans la chaîne d'approvisionnement.

Les activités de sécurité types pour la chaîne d'approvisionnement d'une plate-forme VMSP peuvent par exemple être les suivantes:

a) Confirmation des informations générales sur les participants à la chaîne d'approvisionnement.

b) Validation du matériel, des logiciels et des services utilisés par la plate-forme VMSP.

c) Inspection du matériel et des logiciels achetés par la plate-forme VMSP en vue de s'assurer qu'ils n'ont pas été altérés pendant le transit.

d) Fourniture de mécanismes permettant de vérifier la provenance des logiciels utilisés par le système VMS, par exemple le code fourni par un vendeur de logiciels.

Cette capacité est mise en œuvre de manière ininterrompue afin de tenir compte des évolutions constantes et des mises à jour des systèmes.

– Environnement et procédures de développement sécurisés

Cette capacité permet d'éviter l'introduction de failles de sécurité dans le système VMS et ses écosystèmes pendant le développement. L'environnement de développement comprend les personnes, les processus, les technologies et les installations associés au développement du système. Il est recommandé au développeur du service VMS d'évaluer les risques dans les efforts de développement individuels du système VMS et d'établir des environnements de développement sécurisés en tenant compte des facteurs suivants:

a) Le personnel travaillant dans l'environnement.

b) L'application des méthodologies de développement et des processus de traitement des logiciels et des données.

c) L'utilisation de produits et services externalisés.

d) L'environnement physique et le réseau, et

e) La coexistence avec d'autres efforts de développement et d'exploitation.

Le développeur du service VMS doit également déterminer l'environnement de développement et les procédures associées pour atténuer les risques. Il est recommandé de diffuser les procédures auprès des personnes impliquées dans les efforts de développement.

Annexe B

Protection et confidentialité des informations d'identification personnelle (PII)

(Cette Annexe fait partie intégrante de la présente Recommandation.)

Il est recommandé que le système VMS assure une protection de bout en bout à mesure que les véhicules deviennent connectés et offrent des services plus interactifs. De plus en plus de données utilisateur et d'informations relatives à la vie privée doivent être protégées pour garantir la confidentialité et l'intégrité des données utilisateur stockées dans le système VMS, dans le véhicule et dans le nuage ou les serveurs dorsaux du système VMS.

Selon le National Institute of Standards and Technology (NIST) des États-Unis, les informations PII sont "toute représentation d'informations permettant de déduire raisonnablement, par des moyens directs ou indirects, l'identité d'une personne à laquelle les informations s'appliquent" [b-NIST SP 800-79-2].

Il n'existe pas de définition unique de l'expression "vie privée". La signification de la vie privée dépend des contextes juridique, politique, sociétal, culturel et sociotechnologique.

En général, la confidentialité des informations peut être définie de la manière suivante:

1) Un individu dispose d'informations relatives à sa vie privée s'il est protégé contre la pénétration, l'ingérence ou l'accès à ses propres données par des personnes non autorisées.

La protection des informations PII est l'un des aspects de la protection de la vie privée.

Le système VMS peut stocker des informations PII ou peut fonctionner comme une passerelle pour accéder aux PII du propriétaire du véhicule, du conducteur et/ou des autres occupants.

B.1 Sources d'information

Le système VMS comprend plusieurs sources d'entrée d'informations telles que:

– Des capteurs (détecteurs de mouvement, détecteurs de position, etc.)

– Un appareil de prise de vue (personnalisation, reconnaissance des fonctions, etc.)

– Un microphone – Un système audio (qui peut être utilisé pour les enregistrements vocaux et la reconnaissance vocale, la biométrie vocale, etc.)

– Des identifiants de protocoles de communication réseau tels que l'adresse IP, l'adresse MAC, etc.

– Des sources de médias telles qu'une clé USB, une carte Secure Digital, un disque dur externe, etc.

– Des applications tierces, des passerelles de paiement, des services, des dispositifs, des accessoires, etc.

Le système VMS stocke et partage les informations avec d'autres systèmes dans le véhicule ou dans le nuage en fonction de l'architecture du véhicule, des spécifications régionales, législatives et de certification.

B.2 Mise en œuvre de la protection des informations PII: Considérations générales

Les données personnelles (par exemple dans les données, les textes, l'audio, la vidéo ou les images) doivent être protégées, ainsi que tout contenu que peuvent demander des utilisateurs autres que le client prévu ou tout utilisateur final (comme le nuage, les magasins ou les processus à distance) utilisant le système VMS.

Un accord est nécessaire pour le partage des données en ce qui concerne les données personnelles liées à chaque client, aux utilisateurs finals et aux tiers. Tout accord de ce type avec le client, ou tout autre accord pertinent régissant l'utilisation de service du système VMS, doit être fondé sur les critères suivants:

– Accès personnalisé fondé sur la sélection par l'utilisateur des services et des intérêts.
– Système VMS conçu pour permettre son utilisation conformément aux exigences réglementaires en matière de protection de la vie privée.
– Conception du logiciel, du matériel et du réseau du système VMS de manière à n'autoriser que les accès authentifiés.
– La protection de la vie privée et des informations PII du système VMS doit être conçue pour les véhicules privés avec un seul utilisateur, ainsi que pour les véhicules partagés avec plusieurs utilisateurs.

B.3 Visibilité et transparence des données

Il est recommandé de mettre en œuvre des normes de sécurité bien connues et particulièrement contrôlées. Il est recommandé d'éviter les algorithmes de chiffrement propriétaires.

Il est recommandé d'adopter des processus bien connus.

Il est recommandé d'informer les utilisateurs des données stockées/accessibles par le système VMS. Comme la transparence améliore l'acceptation par les utilisateurs, il est recommandé que la notification aux utilisateurs comprenne des informations sur le type de données, l'objectif de la collecte, l'identité des entités traitant les données et la durée de leur stockage.

B.3.1 Protection de la vie privée par défaut

Il est recommandé que les utilisateurs puissent contrôler la limite de téléchargement des données, et qu'ils aient la possibilité d'accepter ou de refuser le téléchargement et le stockage des données. Les stratégies de refus ou de désinscription préservent davantage la vie privée et respectent mieux les principes de la protection de la vie privée par défaut. Par conséquent, les stratégies de refus ou de désinscription sont recommandées.

Il est recommandé que le système VMS puisse identifier la liste des cas d'utilisation qui répondent aux exigences et aux paramètres de confidentialité des données.

Les applications peuvent utiliser plusieurs ressources pour des cas d'utilisation spécifiques. Par exemple, dans le cas des services de localisation, le Bluetooth, le GPS, les points d'accès WiFi externalisés ou les emplacements des tours de téléphonie cellulaire peuvent être utilisés afin de déterminer les emplacements approximatifs de l'utilisateur. Il est recommandé que le système VMS puisse donner aux utilisateurs la possibilité de désactiver certaines possibilités de suivi. Le contrôle des paramètres globaux pourrait être utilisé à cette fin en définissant des politiques de confidentialité pour toutes les applications. Par ailleurs, les occupants pourraient être autorisés à contrôler l'accès aux données au niveau d'une seule application. Il est possible d'utiliser des contrôles de confidentialité tels que les approches avancées par PRICON, qui combinent les deux approches. Une autre option pour le système VMS serait un signal "Ne pas suivre" ("DNT" pour *Do Not Track*) qui est déjà utilisé par les navigateurs web. Un signal DNT est un champ d'en-tête HTTP indiquant la préférence de l'utilisateur pour le suivi de ses activités sur un service ou par le biais d'un suivi intersites de l'utilisateur.

Les applications ou les commandes peuvent par exemple demander à recevoir des données de localisation uniquement pendant l'utilisation de l'application ou à les autoriser à tout moment. Les occupants peuvent choisir de ne pas autoriser cet accès et il est recommandé de leur laisser la possibilité de modifier ce choix à tout moment dans les paramètres. Le Règlement général sur la protection des données (RGPD), appliqué à un service qui fonctionne également au sein de l'Union européenne, exige de permettre à l'utilisateur de prendre des décisions éclairées en matière de

confidentialité. Une décision éclairée en matière de protection de la vie privée est possible lorsque le décideur est conscient des conséquences de la divulgation des données (qui obtient quelles données, à quelle fin et dans quelles conditions) ou de leur refus (quelles fonctions spécifiques sont restreintes).

Si on autorise une application à accéder à certaines données et à les utiliser en arrière-plan, il est important de rappeler aux utilisateurs qu'ils ont donné leur accord et il faut leur permettre de modifier l'accès de l'application.

Il est recommandé que l'architecture du système VMS soit robuste pour empêcher les applications d'accéder à des informations auxquelles l'utilisateur n'a pas explicitement donné accès.

B.4 Exactitude des données et intégrité des données

Il est recommandé que le système VMS gère tous les aspects des données, tels que le téléchargement aval, le téléchargement amont, la communication et la suppression des données, et ce de manière spécifique.

Sécurité de bout en bout – Protection de l'ensemble du cycle de vie. Il est recommandé de procéder régulièrement à un examen du code et à des tests de sécurité rigoureux. En outre, il est recommandé de mettre en place des stratégies de protection au niveau de la radiodiffusion, de la base de données et du récepteur.

Il est recommandé d'assurer la sécurité des logiciels afin de prévenir la perte, l'inexactitude, l'altération, l'indisponibilité ou l'utilisation abusive des données et des ressources qui sont utilisées, contrôlées et protégées.

Il est recommandé de permettre aux utilisateurs de vérifier l'exactitude des informations PII et la légalité de leur traitement.

L'intégrité suppose le maintien dans le temps de la cohérence, de l'exactitude et de la fiabilité des données. Il est donc recommandé de mettre en place une protection contre la modification ou la destruction inappropriée des informations. Des mesures adaptées sont recommandées afin de garantir la non-répudiation et l'authenticité des informations.

Dans les paramètres, il est recommandé que les utilisateurs aient la possibilité de voir les applications auxquelles ils ont autorisé l'accès pour certaines informations. Ils devraient aussi pouvoir accorder ou révoquer tout accès futur.

En outre, il est recommandé que le système d'exploitation (OS) du système VMS impose des restrictions qui empêchent le mouvement des données entre les applications et les comptes installés par une solution de gestion des données fiable et celles et ceux installés par l'utilisateur.

Les utilisateurs peuvent demander la correction, la modification ou la suppression de leurs informations d'identification personnelle si elles sont inexactes ou s'ils pensent que le traitement de leurs informations d'identification personnelle constitue une violation de la loi applicable.

Des systèmes, des applications et des procédures doivent être mis en place pour sécuriser les informations d'identification personnelle des utilisateurs, afin de réduire autant que possible les risques de vol, de dommage, de perte d'informations, ou d'accès non autorisé aux informations ou de leur utilisation non autorisée.

Il est recommandé de détecter et de notifier à l'utilisateur toute modification non autorisée des informations PII dans le système VMS ou le nuage.

B.5 Confidentialité

La confidentialité consiste à préserver les restrictions autorisées en matière d'accès et de divulgation, y compris les moyens pour la protection de la vie privée et des informations confidentielles.

B.5.1 Niveaux d'impact de la confidentialité

Il est recommandé d'évaluer les PII afin de déterminer leur niveau d'impact sur la confidentialité, de sorte que des mesures de protection appropriées puissent être mises en place. Il est recommandé de ne pas traiter de la même manière toutes les données PII stockées ou créées.

Il est recommandé d'évaluer les niveaux d'impact sur la confidentialité selon qu'ils soient faibles, moyens ou élevés en fonction du caractère identifiable, de la sensibilité des données et de l'obligation de protection conformément aux réglementations.

B.5.2 Protection de la confidentialité

Il est recommandé de mettre en place une protection de la confidentialité par les mesures suivantes:

– Mise en œuvre d'un mécanisme de contrôle de l'accès à l'aide d'un mot de passe pour accéder aux données du système VMS.

– Accès multicouche aux informations PII confidentielles et à fort impact.

– Contrôle de l'accès à plusieurs niveaux à partir de téléphones mobiles, d'ordinateurs portables et de dispositifs numériques personnels.

– Chiffrement des informations PII avant leur transmission. Les mesures détaillées sont décrites dans le § A.3.8 (Cryptographie).

En outre, il est recommandé de procéder à des évaluations des risques avant le déploiement de nouvelles exigences. Il est également recommandé de mettre en place un mécanisme de surveillance continue des risques pour l'évaluation des changements dans le système VMS ou l'identification de nouveaux risques associés au système VMS.

B.6 Anonymisation des données

L'anonymisation des données est le processus qui consiste à modifier de manière irréversible des données classifiées afin de protéger les personnes concernées par les informations PII.

En rendant anonymes les données traitées dans l'environnement VMS, il est possible de réaliser un large éventail d'analyses et de partage de données.

B.7 Disponibilité des données

La disponibilité de données exige de garantir un accès rapide et fiable aux informations et leur utilisation.

Il est recommandé d'offrir aux occupants autorisés un contrôle détaillé de l'utilisation des informations de localisation par les services du système. Ils peuvent notamment désactiver l'inclusion des informations de localisation dans les informations recueillies par les applications internes, l'historique des recherches de navigation et les informations d'accès Bluetooth et WiFi. Si l'utilisateur se connecte au nuage OEM, les applications fonctionnellement nécessaires se voient accorder un accès par défaut au nuage OEM. Il est recommandé que les utilisateurs puissent contrôler l'accès de chaque application au nuage dans les paramètres.

Si la télématique permet d'accéder à distance aux informations PII, il est recommandé que les services connectés fonctionnent avec une authentification à plusieurs niveaux.

Puisque les données sont disponibles en effectuant divers traitements de données (calcul, traitement statistique, etc.) dans un format chiffré (par exemple, en utilisant un chiffrement homomorphe), des traitements de données similaires peuvent être effectués sur les données dans le système VMS.

Bibliographie

[b-UIT-T X.1197 Amd1] Recommandation UIT-T X.1197 Amd.1 (2019), *Lignes directrices relatives aux critères de sélection d'algorithmes cryptographiques pour la protection de services et de contenus de TVIP, Amendement 1*.

[b-UIT-T X.1811] Recommandation UIT-T X.1811 (2020), *Lignes directrices en matière de sécurité relatives à l'utilisation d'algorithmes à l'épreuve des attaques quantiques dans les systèmes 5G*.

[b-ETSI WP35] Livre blanc de l'ETSI 35 (2020), *Bonnes pratiques, avantages, défis de transition et voie à suivre en matière d'IPv6*. https://www.etsi.org/images/files/ETSIWhitePapers/etsi_WP35_IPv6_Best_Practices_Benefits_Transition_Challenges_and_the_Way_Forward.pdf

[b-IEEE 802.11] IEEE 802.11-2020, *Norme IEEE pour les technologies de l'information – Télécommunications et échange d'informations entre systèmes – Réseaux locaux et métropolitains – Exigences spécifiques – Partie 11: Spécifications de la couche de commande d'accès au support* (*MAC*) *et de la couche physique* (*PHY*) *des réseaux locaux hertziens*.

[b-IETF RFC 2663] IETF RFC 2663 (1999), *Terminologie et considérations du traducteur d'adresse réseau IP* (*NAT*).

[b-IETF RFC 8200] IETF RFC 8200 (Juillet 2017), *Spécification du Protocole Internet, Version 6* (*IPv6*).

[b-IETF RFC 8216] IETF RFC 8216 (2017), *Diffusion HTTP en continu et en direct*.

[b-ISO/IEC 23009-1] ISO/IEC 23009-1:2019, *Technologies de l'information – Diffusion en flux adaptatif dynamique sur HTTP* (*DASH*) *– Partie 1: Description de la présentation et formats de segments des médias*.

[b-IAB] Déclaration de l'Internet Architecture Board (IAB) sur l'épuisement des adresses IPv6 (Novembre 2016). https://www.iab.org/2016/11/07/iab-statement-on-ipv6/ [En ligne].

[b-NIST SP 800-79-2] Publication spéciale du NIST 800-79-2 (2015), *Lignes directrices relatives à l'autorisation des émetteurs de cartes de vérification d'identité personnelle* (*PCI*) *et des émetteurs de titres de compétences PIV dérivés* (*DPCI*).

[b-USG OMB] Bureau américain de la gestion et du budget (Novembre 2020), *Mémorandum à l'intention des chefs de départements exécutifs et d'agences*. https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf [En ligne].

SERIES 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	Équipements 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

Imprimé en Suisse
Genève, 2022