ITUPublications
Recommandations

Union internationale des télécommunications
Secteur de la normalisation

Recommandation

# UIT-T X.1381 (03/2023)

SÉRIE X: Réseaux de données, communication entre systèmes ouverts et sécurité

Applications et services sécurisés (2) – Sécurité des systèmes de transport intelligents

# Lignes directrices relatives à la sécurité des réseaux embarqués basés sur l'Ethernet

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 | X.1000-X.1099 |
| APPLICATIONS ET SERVICES SÉCURISÉS (1) | X.1100-X.1199 |
| SÉCURITÉ DU CYBERESPACE | X.1200-X.1299 |
| APPLICATIONS ET SERVICES SÉCURISÉS (2) | X.1300-X.1499 |
| Communications d'urgence | X.1300-X.1309 |
| Sécurité des réseaux de capteurs ubiquitaires | X.1310-X.1319 |
| Sécurité des réseaux électriques intelligents | X.1330-X.1339 |
| Courrier certifié | X.1340-X.1349 |
| Sécurité de l'Internet des objets (IoT) | X.1350-X.1369 |
| **Sécurité des systèmes de transport intelligents** | **X.1370-X.1399** |
| Sécurité de la technologie des registres distribués (DLT) | X.1400-X.1429 |
| Sécurité des applications (2) | X.1450-X.1459 |
| Sécurité de la toile (2) | X.1470-X.1489 |
| ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ | X.1500-X.1599 |
| SÉCURITÉ DE L'INFORMATIQUE EN NUAGE | X.1600-X.1699 |
| COMMUNICATIONS QUANTIQUES | X.1700-X.1729 |
| SÉCURITÉ DES DONNÉES | X.1750-X.1799 |
| SÉCURITÉ DES IMT-2020 | X.1800-X.1819 |

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

# Recommandation UIT-T X.1381

## Lignes directrices relatives à la sécurité des réseaux embarqués basés sur l'Ethernet


### Résumé

La Recommandation UIT-T X.1381 définit des lignes directrices relatives à la sécurité des réseaux embarqués (IVN) basés sur l'Ethernet. La tendance actuelle observée dans l'architecture électrique et électronique (E/E) consiste à intégrer l'Ethernet à des réseaux IVN d'ancienne génération, comme le gestionnaire de réseau de communication (CAN), le réseau local d'interconnexion (LIN), le transport dans des systèmes orientés média (MOST) et FlexRay. Autrefois, l'Ethernet n'était considéré que comme un moyen de connexion entre des véhicules et des environnements extérieurs. Des protocoles types permettant des connexions selon le protocole Internet sur l'Ethernet (communication de diagnostic au travers du protocole Internet ou protocole universel de mesure et de calibration, par exemple) ont été utilisés pour permettre des communications entre l'environnement extérieur et les véhicules. En général, il n'est pas nécessaire que ces cas d'utilisation répondent à des contraintes de temps réel rigoureuses. Cependant, les applications embarquées utilisant la communication Ethernet doivent présenter certaines caractéristiques, notamment une sensibilité temporelle et une fiabilité élevées.

Les évolutions actuelles concernant les technologies de communication embarquées nécessitent une largeur de bande accrue dans le réseau. En comparaison avec l'Ethernet, les réseaux IVN d'ancienne génération sont insuffisants pour offrir la largeur de bande nécessaire aux applications embarquées actuelles. Par conséquent, aujourd'hui et demain, les réseaux IVN basés sur l'Ethernet constituent et constitueront un élément majeur de l'architecture E/E.

Cependant, les contre-mesures connues des réseaux informatiques ordinaires ne peuvent pas convenir à une application automobile, car elles n'ont pas été élaborées en tenant compte des besoins et des capacités des automobiles.

Pour répondre à ce besoin, la présente Recommandation définit des lignes directrices relatives à la sécurité de la technologie Ethernet automobile. Elle contient un modèle de référence de l'Ethernet automobile ainsi qu'une analyse des menaces et des vulnérabilités concernant les réseaux IVN basés sur l'Ethernet. En outre, la présente Recommandation présente des exigences de sécurité et des cas d'utilisation des réseaux IVN basés sur l'Ethernet.



### Historique*

| Édition | Recommandation | Approbation | Commission d'études | ID unique |
|---|---|---|---|---|
| 1.0 | UIT-T X.1381 | 03-03-2023 | 17 | 11.1002/1000/15107 |

### Mots clés

Sécurité de l'Ethernet automobile, sécurité des systèmes ITS.


* Pour accéder à la Recommandation, reporter cet URL https://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique.

## 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 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 de 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/.

© UIT 2023

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

# Recommandation UIT-T X.1381

## Lignes directrices relatives à la sécurité des réseaux embarqués basés sur l'Ethernet

### 1 Domaine d'application

La présente Recommandation définit des lignes directrices relatives à la sécurité des réseaux embarqués (IVN) basés sur l'Ethernet. Elle contient:

1) une analyse des menaces concernant la sécurité;

2) des exigences de sécurité; et

3) des cas d'utilisation;

présentés sous l'angle de la cybersécurité. Selon les principes de cybersécurité, l'architecture de communication technique concernée fait ou peut faire partie intégrante de systèmes cyberphysiques (piles de protocole de communication Ethernet faisant partie de systèmes intégrés, par exemple).

### 1.1 Déclarations d'applicabilité

Les réseaux en général, et les réseaux basés sur l'Ethernet en particulier, sont utilisés pour assurer des services de communication. Par conséquent, la présente Recommandation est axée sur la sécurité des communications, mais pas nécessairement sur la sécurité de l'information à proprement parler pour les nœuds de calcul fonctionnant avec la connectivité Ethernet.

Les lignes directrices relatives à la sécurité figurant dans la présente Recommandation portent donc sur l'ingénierie des réseaux basés sur l'Ethernet utilisés dans les applications automobiles et sont présentées sous l'angle de l'ingénierie sécurité. Ainsi, les architectures de communication en couches associées et leurs piles de protocoles en couches constituent un élément fondamental de ces considérations liées à la sécurité.

### 1.2 Validité des lignes directrices relatives à la sécurité au fil du temps

La sécurité des architectures de communication nécessaires pour les réseaux Ethernet embarqués change profondément, principalement en raison:

1) des évolutions possibles des topologies de réseau (induites par les architectures informatiques distribuées en mutation utilisant ces réseaux de communication, par exemple dans le sens de l'automatisation des véhicules);

2) des architectures de protocoles en couches: les piles de protocoles Ethernet et non-Ethernet actuellement utilisées peuvent changer, obtenir des extensions, etc.;

3) de l'évolution des protocoles: les protocoles actuels des technologies de l'information et de la communication (TIC) utilisés (dont sont propriétaires les organismes de normalisation comme l'IEEE, l'IETF, l'UIT-T, l'ETSI ou le Partenariat 3GPP) font toujours l'objet d'activités de maintenance et d'extensions en continu, comme en témoignent les activités consistant à établir un profil de protocole (normes de l'IEEE relative à la mise en réseau sensible au temps (TSN) pour les applications automobiles, par exemple) [b-IEEE 1722-2016] ou à gérer des versions d'un protocole;

NOTE – Par ailleurs, les considérations de sécurité liées à la spécification des protocoles peuvent également faire l'objet de mises à jour.

4) de l'évolution des moyens et des solutions de sécurité dans le contexte de la sécurité des communications.

De futures révisions de la présente Recommandation sont donc attendues.

La présente Recommandation est axée en particulier sur les lignes directrices initiales relatives à la sécurité, qui résultent d'une première série de cas d'utilisation. L'accent est mis avant tout sur les réseaux IVN basés sur l'Ethernet de(s) première(s) génération(s), pour lesquels des bonnes pratiques en matière de sécurité et des lignes directrices relatives à la sécurité étaient en vigueur au moment de la publication de la présente Recommandation.

## 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 se reporter, si possible, aux versions les plus récentes des Recommandations et autres références énumérées ci-dessous. 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 X.1371] Recommandation UIT-T X.1371 (2020), *Menaces pour la sécurité des véhicules connectés*.

## 3 Définitions

### 3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

**3.1.1 imputabilité** [b-UIT-T X.800]: propriété qui garantit que les actions d'une entité ne peuvent être imputées qu'à cette entité.

**3.1.2 authentification** [b-UIT-T X.1252]: processus formalisé de vérification qui, s'il est concluant, aboutit à une identité authentifiée pour une entité.

NOTE – Dans un contexte de gestion d'identité, le terme "authentification" désigne l'authentification de l'entité.

**3.1.3 authenticité** [b-UIT-T X.641]: protection par authentification mutuelle et authentification de l'origine des données.

**3.1.4 autorisation** [b-UIT-T X.800]: attribution de droits, comprenant la permission d'accès sur la base de droits d'accès.

**3.1.5 disponibilité** [b-UIT-T X.800]: propriété d'être accessible et utilisable sur demande par une entité autorisée.

**3.1.6 confidentialité** [b-UIT-T X.800]: propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.

**3.1.7 intégrité des données** [b-UIT-T X.800]: propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée.

**3.1.8 pare-feu** [b-UIT-T X.1039]: type de barrière de sécurité placée entre des environnements de réseau, qui se présente sous la forme d'un dispositif dédié ou d'un ensemble de plusieurs composants et techniques, à travers laquelle passe tout le trafic d'un environnement de réseau à un autre et vice versa. Seul le trafic autorisé défini dans le cadre d'une politique de sécurité locale est autorisé à passer.

**3.1.9 passerelle de sécurité** [b-UIT-T X.1039]: point de connexion entre des réseaux, ou entre des sous-groupes à l'intérieur de réseaux, ou entre des applications logicielles à l'intérieur de domaines de sécurité différents dont le rôle est de protéger un réseau conformément à une politique de sécurité donnée.

**3.1.10 passerelle de véhicule (VG)** [b-UIT-T F.749.1]: une passerelle de véhicule est un dispositif dans un véhicule qui rend possibles les communications entre un dispositif dans le véhicule et un autre dispositif qui peut se trouver physiquement soit à l'intérieur du véhicule soit à l'extérieur (exemples: station en bordure de route, serveur dans le nuage, etc.). Une passerelle de véhicule fournit des interfaces et protocoles normalisés, permet les communications entre des réseaux hétérogènes, sélectionne les réseaux de manière optimale en tenant compte des besoins des applications et de la qualité de service des réseaux, arbitre et intègre les communications de réseau, assure la sécurité et la connexion aux réseaux de commutation pour garantir la continuité des services.

NOTE 1 – Le terme "passerelle centrale" (tel que décrit dans la présente Recommandation) est généralement synonyme de "passerelle de véhicule" dans les réseaux embarqués (IVN) abstraits, ou de "passerelles périphériques de véhicule" dans les architectures de réseaux IVN plus détaillées.

NOTE 2 – Le terme "passerelle de véhicule pour les systèmes de transport intelligents (ITS)" est généralement synonyme de "passerelle de véhicule".

## 3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

**3.2.1 architecture électrique et électronique (architecture E/E)**: architecture de véhicule couplée en deux plans, composée: 1) d'un plan de réseau de distribution d'électricité ou d'énergie; et 2) d'un plan architectural de réseau de communication et de traitement de l'information.

NOTE – Un exposant trois est parfois ajouté à "architecture E/E" pour indiquer la technologie de propulsion du véhicule ($E^3$), le troisième E indiquant que le véhicule en question est électrique.

**3.2.2 passerelle périphérique de véhicule**: passerelle de véhicule située à la périphérie et à l'intérieur du ou des domaine(s) de réseau(x) interne(s) et externe(s) d'un véhicule. Par conséquent, tout le trafic des communications de véhicule à tout autre élément (V2X) est acheminé via ce type de passerelle de véhicule.

NOTE 1 – Le terme "passerelle de véhicule" correspond aussi à cette définition et pourrait donc suffire pour les architectures des réseaux embarqués (IVN) avec une seule passerelle de véhicule déployée. Cependant, les réseaux IVN peuvent également utiliser les passerelles de véhicule, uniquement à des fins d'interconnexion interne et d'interfonctionnement. Ces contextes de réseau peuvent conduire à la nécessité de distinguer les types de passerelle de façon plus détaillée.

NOTE 2 – Les fonctions d'interfonctionnement spécifiques prises en charge par un type de passerelle particulier sont souvent présentées sous la forme d'un nom de passerelle étendu indiquant, par exemple, l'emplacement dans une hiérarchie de réseau (comme le niveau de l'accès ou du réseau central), le type de périphérie ou d'interconnexion de réseaux (comme les domaines de sécurité), les interfaces réseau spécifiques ou les technologies de la communication.

NOTE 3 – Une unité de contrôle des communications est comprise comme étant un composant technique appartenant à la catégorie "passerelle périphérique de véhicule" (fonctions).

NOTE 4 – La communication V2X englobe tous les types de trafic, par exemple le trafic des services télématiques, ITS ou de diagnostic.

**3.2.3 architecture électrique et électronique orientée zone**: architecture électrique et électronique (E/E) regroupant des éléments embarqués (Note 1), comme des capteurs, des actionneurs et des nœuds de calcul, selon leur emplacement (Note 2) dans les sous-domaines de réseau. Chaque sous-domaine, appelé zone (Note 3), possède son propre nœud de calcul de véhicule associé à une zone (connu comme étant un contrôleur de zone dans les applications automobiles) connecté à tous les intrasous-domaines des éléments embarqués. Les contrôleurs de zone de chaque zone sont interconnectés à l'aide d'un nœud de calcul embarqué à haute performance supérieur. Par conséquent, il en résulte une hiérarchie de traitement entre les zones et le domaine de réseau IVN global dans le cas des architectures de calcul réparties.

NOTE 1 – Accent mis sur les éléments de calcul et de mise en réseau dans le contexte des réseaux IVN.

NOTE 2 – Par "emplacement", on entend l'emplacement du réseau au niveau topologique du réseau IVN physique ou virtuel.

NOTE 3 – Ici, la notion de zone se réfère principalement au concept de domaines de réseau dans le contexte des architectures E/E. Une telle zone n'englobe pas nécessairement le concept de zone de sécurité, de zone de confiance ou de zone démilitarisée utilisé dans d'autres recommandations UIT-T portant sur la sécurité (par exemple la Recommandation [b-UIT-T Y.2770]).

## 4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

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

ARP protocole de résolution d'adresse (*address resolution protocol*)

AUTOSAR architecture de systèmes ouverts pour automobiles (*automotive open system architecture*)

AVB pontage audiovisuel (*audio video bridging*)

CAN gestionnaire de réseau de communication (*controller area network*)

CGW passerelle centrale (*central gateway*)

CPU unité centrale de traitement (*central processing unit*)

CRC contrôle de redondance cyclique (*cyclic redundancy check*)

DHCP protocole de configuration dynamique du serveur (*dynamic host configuration protocol*)

DoIP communication de diagnostic au travers du protocole internet (*diagnostic communication over Internet protocol*)

DoS déni de service (*denial of service*)

DTLS sécurité de la couche transport en mode datagramme (*datagram transport layer security*)

E/E électrique et électronique (*electrical and electronic*)

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

FDB base de données de transmission (*forwarding database*)

FIB base d'informations de transmission (*forwarding information base*)

HSM module de sécurité matériel (*hardware security module*)

ICMP protocole des messages de commande Internet (*Internet control message protocol*)

ID identificateur (*identifier*)

IDS système de détection des intrusions (*intrusion detection system*)

IP protocole Internet (*Internet protocol*)

IPsec sécurité du protocole Internet (*Internet protocol security*)

IPv4 protocole Internet version 4 (*Internet protocol version 4*)

IPv6 protocole Internet version 6 (*Internet protocol version 6*)

ITS système de transport intelligent (*intelligent transport system*)

IVN réseau embarqué (*in-vehicle network*)

LIN réseau local d'interconnexion (*local interconnect network*)

| | |
|---|---|
| MAC | commande d'accès au support (*media access control*) |
| MACsec | sécurité de la commande d'accès au support (*media access control security*) |
| MCU | microcontrôleur (*microcontroller unit*) |
| MOST | transport dans des systèmes orientés média (*media oriented systems transport*) |
| MPU | unité de commande multipoint (*multipoint control unit*) |
| OBD | diagnostic embarqué (*on-board diagnostic*) |
| OEM | fabricant d'équipements d'origine (*original equipment manufacturer*) |
| PDU | unité de données de protocole (*protocol data unit*) |
| PVID | identificateur de port VLAN (*port VLAN ID*) |
| QoS | qualité de service (*quality of service*) |
| SecOC | communication de bord sécurisée (*secure onboard communication*) |
| SR | recommandation sur la sécurité (*security recommendation*) |
| TARA | analyse des menaces et évaluation des risques (*threat analysis and risk assessment*) |
| TCP | protocole de commande de transmission (*transmission control protocol*) |
| TIC | technologie de l'information et de la communication |
| TLS | sécurité de la couche transport (*transport layer security*) |
| TP | protocole de transport (*transport protocol*) |
| TSN | mise en réseau sensible au temps (*time-sensitive networking*) |
| UDP | protocole de datagramme utilisateur (*user datagram protocol*) |
| UDS | service de diagnostic unifié (*unified diagnostic service*) |
| V2X | de véhicule à tout (*vehicle to everything*) |
| VG | passerelle de véhicule (*vehicle gateway*) |
| VID | identificateur de VLAN (*VLAN identifier*) |
| VLAN | réseau local virtuel (*virtual local area network*) |

## 5 Conventions

La présente Recommandation fournit une liste d'exigences de sécurité, intitulées [SR-*x*], *x* étant un nombre. Ces exigences emploient les expressions suivantes avec les significations qui suivent:

L'expression "**il est recommandé**" ou "**devrait**" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

L'expression "**peut, à titre d'option**" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée comme l'obligation pour le fabricant de mettre en œuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de services de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité à la présente Recommandation.

## 6 Aperçu des architectures automobiles fondées sur Ethernet et des architectures embarquées en évolution

L'Ethernet automobile est un réseau physique qui est utilisé pour connecter les composants à l'intérieur d'un véhicule à l'aide d'un réseau câblé. C'est également le nom utilisé pour l'ensemble du réseau Ethernet embarqué en tant que tel, comprenant toutes les couches de protocole et tous les protocoles utilisés dans ce domaine du réseau. Il est conçu pour répondre aux besoins du marché automobile, notamment pour satisfaire aux caractéristiques électriques (émissions et sensibilité en matière d'interférences électromagnétiques ou de brouillages radioélectriques), aux besoins de largeur de bande, aux exigences en matière de temps de latence et aux exigences en matière de synchronisation et de gestion de réseau. Les véhicules autonomes et les systèmes d'aide évoluée à la conduite (ADAS) faisant l'objet d'une grande attention, les véhicules modernes sont généralement équipés de plusieurs caméras, de systèmes de diagnostic à bord (OBD) et de systèmes d'infoloisirs qui nécessitent une grande largeur de bande. En outre, à mesure que le nombre de fonctions augmente, le nombre de nœuds de calcul interconnectés (tels que les unités de commande électroniques (ECU)) dans un véhicule le fait aussi. Cela entraîne une augmentation du faisceau de câblage et de la masse du véhicule, ce qui dégrade ses performances et son rendement énergétique. L'architecture électrique/électronique (E/E) orientée en fonction des zones est un exemple parlant d'architecture de réseau et d'informatique embarquée spécifique, dans le cadre de laquelle l'Ethernet est également utilisé au niveau supérieur de la hiérarchie réseau, pour l'interconnexion de toutes les zones (un réseau dit dorsal) dans l'ensemble de l'architecture. Lorsqu'un réseau embarqué (IVN) traditionnel, notamment un gestionnaire de réseau de communication (CAN), un réseau local d'interconnexion (LIN), le transport dans des systèmes orientés média (MOST) ou FlexRay, est intégré à l'Ethernet, des câbles Ethernet normalisés peuvent être utilisés pour réduire considérablement la masse et les coûts. En outre, grâce à la grande largeur de bande, le nombre de systèmes de contrôle peut être réduit, de même que leur complexité.

Cependant, les domaines de l'IVN ne passeront pas tous à l'Ethernet automobile. C'est par exemple le cas du groupe motopropulseur, de la carrosserie et du châssis. Cela signifie que certains domaines, par exemple une carrosserie qui a besoin d'une faible quantité de données et de largeur de bande, n'ont pas besoin de changer de protocole de réseau avec des ressources et des efforts supplémentaires.

La Figure 1 montre un réseau IVN mixte comprenant des anciens protocoles IVN, tels que le protocole CAN et l'Ethernet automobile. Les communications nécessitant une faible largeur de bande peuvent toujours utiliser les anciens protocoles IVN, tandis que les communications nécessitant une largeur de bande élevée, telles que les fonctions autonomes ou ADAS, peuvent passer à un IVN fondé sur l'Ethernet.

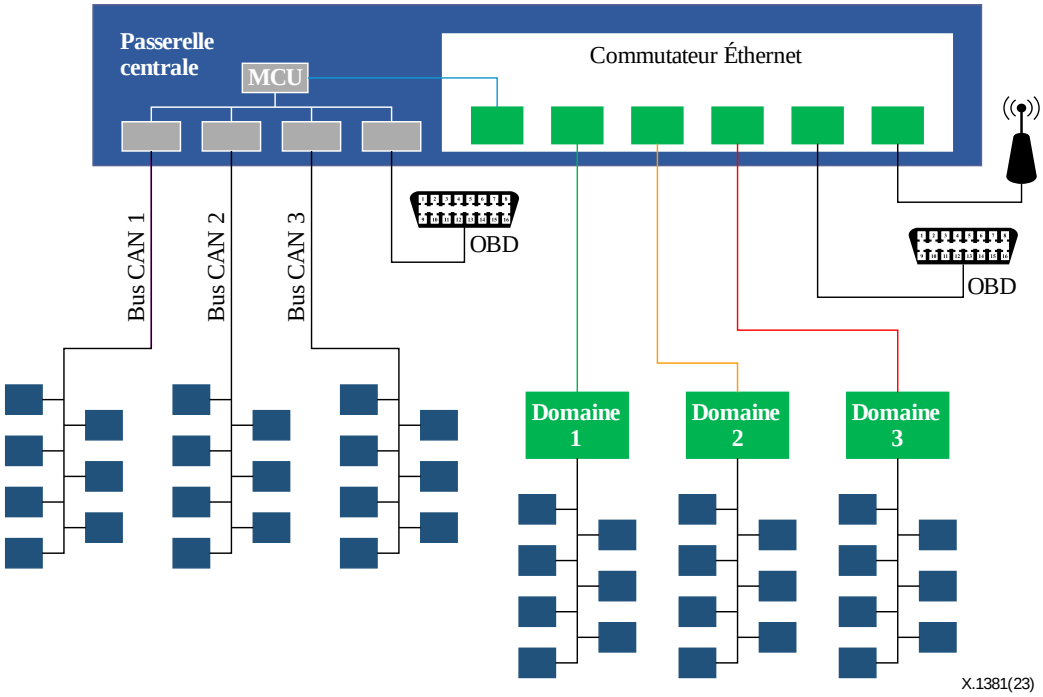


**Figure 1 – Hétérogénéité actuelle d'un réseau embarqué typique, fondé sur les anciens protocoles et l'Ethernet automobile**

L'évolution attendue des IVN fondés sur l'Ethernet au fil du temps est reconnue. Ces évolutions de réseau s'accompagnent généralement de changements dans l'architecture de communication (topologies de communication, piles de protocoles structurées en couches, etc.), qui auront très probablement une incidence sur les architectures de sécurité pour les communications correspondantes.

Les concepts de sécurité pour les architectures E/E classiques, c'est-à-dire fondées sur les protocoles CAN/FlexRay/LIN et parfois MOST, ont déjà été examinés auparavant et certains mécanismes proposés sont déjà en voie de normalisation. L'Ethernet et les protocoles de couche supérieure y relatifs seront une solution de remplacement des anciens systèmes de bus automobiles non seulement simple mais aussi plus rapide, et modifieront probablement les concepts fondamentaux des architectures E/E actuelles.

La mise en place de l'Ethernet offre la possibilité conséquente d'améliorer la sécurité à bord des véhicules car de nombreux problèmes de sécurité exigeant une attention particulière dans les applications automobiles ont déjà été résolus pour l'Ethernet, par exemple dans les activités des TIC dites de qualité opérateur (par exemple, les réseaux métropolitains fondés sur l'Ethernet, les réseaux d'accès hertziens de Terre fondés sur l'Ethernet), mais aussi dans les activités classiques des technologies de l'information (par exemple, l'Ethernet comme connectivité de base dans les réseaux locaux d'entreprise privés). Cependant, elle pose également d'énormes difficultés, notamment dues aux contraintes des systèmes automobiles ou intégrés, pour ce qui est de garantir au moins le même niveau de sécurité que celui actuellement attendu pour les architectures E/E existantes à sécurité renforcée.

## 6.1 Architecture d'informatique et de réseau électrique et électronique dans un véhicule

Les anciennes architectures E/E utilisent une passerelle centrale (CGW; également appelée passerelle de véhicule (VG) ou passerelles de véhicule pour les systèmes de transport intelligents (ITS) dans ce type d'IVN) pour la communication et l'interconnexion à bord du véhicule entre les différents sous-domaines. Il existe donc des connexions de bout en bout, qui sont acheminées à travers ces VG.

NOTE 1 – Dans ce contexte, le terme "acheminé" désigne la fonction générique d'acheminement du trafic, et non un autre acheminement tel que celui de l'IP. Les IVN actuels fondés sur l'Ethernet n'utilisent pas d'entités de routage IP, mais uniquement des passerelles de type IP. Une telle utilisation de l'IP et de l'Ethernet engendre une sorte de réseau IP commuté (pour les services de communication fondés sur l'IP). Cet aspect est essentiel du point de vue de la sécurité des communications car il réduit les objectifs de sécurité liés à l'IP (par exemple, il ne peut pas y avoir de menaces de sécurité dues aux protocoles de routage IP).

La communication ciblée fondée sur l'Ethernet devrait répondre à l'exigence de performances en temps réel élevées et de communication fiable, et bénéficier d'une technologie et d'une technique de communication mûre, largement utilisée et éprouvée.

NOTE 2 – La norme [b-IEEE 802.1], et notamment [b-IEEE 802.1CB], permet une communication fiable, qui comprend une architecture à anneau incluant un dispositif de redondance de couche 2 (R-Tag).

Les protocoles CAN, FlexRay, LIN et MOST sont en particulier utilisés de façon native pour la communication embarquée et le protocole CAN est le plus populaire. Une CGW, les VG en général et une passerelle frontalière de véhicule en particulier sont en tant que tels des éléments de réseau et de sécurité essentiels dans les réseaux et les architectures de communication embarqués. Les Appendices II et III fournissent des renseignements complémentaires qui pourraient être utiles du point de vue de la sécurité des communications.

Par le passé, il n'était pas possible d'accéder à un véhicule à distance (par exemple, en utilisant la connectivité d'un atelier à des fins de diagnostic ou les différents types d'options de communication V2X). Les ECU embarquées étaient connectées les unes aux autres par l'intermédiaire d'un ou plusieurs bus de terrain automobiles natifs optimisés.

L'accès légal après la production n'était possible que par une connectivité physique directe et câblée. Ainsi, la connexion point à point sur une courte distance est utilisée exclusivement pour les services de diagnostic qui nécessitent une connexion au port OBD via le protocole CAN. Les fabricants d'équipements d'origine (OEM) étaient conscients du risque de sécurité accru de la fonctionnalité de diagnostic et du protocole CAN natif qui ne fournissait aucune fonctionnalité de sécurité. [b-Autosar 654] s'est concentré sur l'authenticité et l'intégrité des messages CAN et les concepts de sécurité appropriés utilisent principalement des codes d'authentification des messages.

En raison de l'évolution actuelle, une communication fondée sur l'Ethernet entre des dispositifs externes et le véhicule est possible. En général, Une ECU dédiée dans le véhicule sert de point d'accès à un certain type de communication externe. Si nécessaire, l'ECU achemine les renseignements pertinents vers d'autres ECU via des réseaux automobiles communs ou fait passer le trafic par une connexion Ethernet jusqu'à un CGW pour l'acheminer vers d'autres ECU normalement connectées.

## 6.2 Comparaison de la sécurité des architectures électriques et électroniques actuelles et futures

En raison d'un certain nombre de cas d'utilisation abusive mettant en jeu des composants embarqués, des mécanismes de sécurité ont été établis pour les architectures E/E actuelles. En ce qui concerne les systèmes de communication, des mécanismes d'authentification pour le réseau CAN prédominant ont été publiés et normalisés et seront partiellement appliqués aux futures générations de véhicules. Le partenariat AUTOSAR (architecture des systèmes ouverts pour automobiles) définit un module de communication à bord sécurisé axé sur l'authenticité et l'intégrité de la communication embarquée. On notera qu'un mécanisme d'authentification ne se limite pas à vérifier l'authenticité des messages transmis, mais garantit également l'authenticité des partenaires de communication.

En outre, le réseau CAN, en tant que technologie de bus sur la couche physique, transmet uniquement des messages radiodiffusés.

NOTE 1 – La nature des communications sur support physique partagé, comme la topologie de bus, diffère donc fondamentalement de l'approche suivie pour la conception de réseaux Ethernet commutés.

Par conséquent, chaque participant est en mesure de lire la totalité du trafic transmis via le bus CAN. Différents domaines de réseau fondés sur des bus ainsi que d'autres sous-domaines séparent le trafic lié à la sécurité des autres types (par exemple, les infoloisirs ou le confort). La communication entre les domaines du réseau peut se faire uniquement via une passerelle centrale, qui met généralement en œuvre des mécanismes d'application de règles de politique (par exemple, des règles associées aux filtres) pour prévenir les attaques par inondation et garantir la disponibilité du réseau.

NOTE 2 – Les passerelles de véhicule (comme les passerelles centrales) prennent en charge un ensemble de fonctions de réseau, dont un sous-ensemble particulier concerne la sécurité des communications. Par conséquent, des règles de politique spécifiques sont appliquées non seulement dans le domaine de la sécurité, mais aussi en dehors de celui-ci (par exemple, pour l'interfonctionnement de réseaux VLAN, l'acheminement IP ou la mise en place d'actions pour une qualité de service fondée sur les réseaux TSN).

L'Ethernet est une norme établie pour les communications de réseau, qui comprend une large gamme d'applications. Elle est utilisée pour la mise en œuvre de réseaux communs de communication de type machine (par exemple des ordinateurs), y compris des réseaux de différentes échelles (de petite taille, locaux ou métropolitains) et des réseaux d'accès radioélectrique de Terre pour les communications mobiles. Compte tenu de ces considérations et du contexte du réseau, certains schémas relatifs à la sécurité du réseau pourraient être réutilisés.

Les communications basées sur l'Ethernet étant largement utilisées, elles font l'objet d'un certain nombre d'attaques (y compris dans les protocoles de couche supérieure). Néanmoins, des contre-mesures peuvent être appliquées dans différents cas d'utilisation. Par exemple, sur l'Internet, pour les services de transport fondés (uniquement) sur le protocole de commande de transmission (TCP), il est vivement recommandé d'utiliser le protocole de sécurité de couche transport (TLS), afin de garantir l'authenticité, l'intégrité et la confidentialité des communications. Il est également recommandé d'utiliser le protocole complémentaire de sécurité pour les transports pour assurer la sécurité de la couche transport en mode datagramme (DTLS) des services de transport basés sur le protocole de datagramme d'utilisateur (UDP). L'Ethernet étant la norme établie la plus répandue pour les communications embarquées, son utilisation peut permettre de réutiliser les mécanismes de sécurité associés aux piles IP. Toutefois, les contre-mesures connues des réseaux informatiques courants peuvent ne pas convenir à une application automobile, car elles n'ont pas été spécialement conçues pour répondre à ses besoins et à ses capacités. Par exemple, elles peuvent ne pas être en mesure de fournir des assurances en temps réel et ou nécessiter une performance améliorée qui ne peut pas être prise en charge par des dispositifs intégrés à ressources limitées. Par conséquent, l'intégration des mécanismes de sécurité pour les protocoles de communication fondés sur l'Ethernet qui sont sensibles au temps n'est donc pas examinée au moment de la publication.

La séparation des communications embarquées est essentielle aux fins de sécurité. À l'heure actuelle, les fabricants d'équipements d'origine étudient l'isolation logique du trafic Ethernet au moyen de la virtualisation de réseau, qui consiste en un réseau local virtuel (VLAN) établi en tant que réseau privé virtuel de couche 2 dans le cas de l'Ethernet. Il est à noter que la séparation du trafic embarqué peut également être effectuée par d'autres moyens, en utilisant par exemple des réseaux VPN de couche 1 (avec des réseaux Ethernet physiquement séparés) ou de couche 3 (en utilisant une solution VPN connue pour assurer des services de communication IP sur Ethernet).

Un réseau VLAN est une pratique bien établie permettant d'assurer une isolation logique sur la couche liaison de données dans les réseaux informatiques courants. Les réseaux VLAN sont couramment utilisés pour diviser des réseaux physiques en différents réseaux logiques. L'application embarquée d'un réseau VLAN est principalement basée sur le fait que ce type de réseau permet de hiérarchiser le trafic (par exemple, en mappant les codes de priorité VLAN directement avec les classes de trafic TSN).

NOTE 3 – Les considérations relatives à la sécurité des réseaux VLAN hiérarchisés, qui pourraient relever des futurs réseaux IVN pour des modèles d'interconnexion V2X spécifiques, n'entrent pas dans le cadre de cette édition de la présente Recommandation. Le présent texte porte donc uniquement sur les réseaux VLAN à étiquette unique ou à accès.

Si l'application de la norme Ethernet très répandue dans les communications embarquées offre des possibilités non négligeables, il convient néanmoins d'être particulièrement attentif. En effet, en plus de l'absence de mécanismes de sécurité, aucun équipement spécial n'est recommandé pour connecter un dispositif externe au véhicule via l'Ethernet.

Même les utilisateurs peuvent vouloir brancher leurs ordinateurs portables ou utiliser leurs téléphones intelligents pour améliorer l'accès aux réseaux IVN. L'utilisation d'un commutateur Ethernet comme composant additionnel peut constituer un vecteur d'attaque intéressant pour une personne non autorisée spécialement formée. Les auteurs d'attaques peuvent lancer des attaques connues sur l'Internet ou des attaques exploitant des failles de sécurité ("exploits") publiées pour des commutateurs Ethernet couramment utilisés. Comme pour la sécurité des communications, il existe des contre-mesures pour protéger les commutateurs Ethernet courants. Toutefois, des études plus approfondies sont nécessaires concernant les environnements automobiles.

Le Tableau 1 montre les différences entre les protocoles IVN existants, axés sur les bus de terrain, et ceux basés sur l'Ethernet à un niveau très abstrait. La première colonne de chaque élément de comparaison est le niveau de mise en œuvre des critères correspondants, qui est représenté par les symboles suivants: (−) pour mauvais, (0) pour neutre, (+) pour bon, (++) pour optimal. Veuillez noter que le Tableau 1 est délibérément simplifié; une évaluation plus exhaustive du protocole passerait par une comparaison de l'Ethernet avec chaque bus de terrain ou technologie de communication par bus embarquée.

**Tableau 1 – Comparaison des architectures de communication embarquées existantes et basées sur l'Ethernet**

| **Critères** | **Protocoles IVN axés sur les bus de terrain (Note 1)** | | **Réseaux IVN basés sur l'Ethernet** | |
|---|---|---|---|---|
| Simplicité | − | Passerelle complexe, hétérogène, multiprotocole | ++ | Très homogène dotée (essentiellement) de commutateurs de couche 2 |
| Flexibilité | − | Difficile d'étendre/adapter un nouveau sous-réseau (au sein de sous-réseaux facilement) | ++ | Facile d'étendre/adapter un nouveau sous-réseau ou au sein d'un sous-réseau |
| Qualité de fonctionnement | + | Dépend du type de bus | ++ | Jusqu'à plusieurs gigabits par seconde |
| Temps réel | ++ | Reconnu depuis des dizaines d'années | − | Capable mais non conçu pour |
| Quantité de matériel physique lié au réseau | − | Câblage par bus | + | Une paire torsadée pour tous |
| Coûts (investissements, autres qu'opérationnels) | − | Production en petite série destinée aux automobiles | + | Production en masse à l'échelle mondiale également destinée à des secteurs autres qu'automobile |
| Degré de normalisation | − | Norme à application très diverse | + | Norme à application restreinte |
| Modèles de connectivité dans les couches physique et liaison de données (NOTE 2) | − | Seulement les modèles de communication point à multipoint en raison de l'utilisation de supports physiques partagés ("bus") | + | L'Ethernet prend en charge les modèles de communication point à point et point à multipoint (NOTE 3). |

**Tableau 1 – Comparaison des architectures de communication embarquées existantes et basées sur l'Ethernet**

| Critères | Protocoles IVN axés sur les bus de terrain (Note 1) | | Réseaux IVN basés sur l'Ethernet | |
|---|---|---|---|---|
| Intégrité des messages (NOTE 4) | + | Contrôle de redondance cyclique (CRC) + mesures relatives aux bus | + | CRC, codes de blocs |
| Mesures de sécurité (NOTE 5) | − | Quasiment aucune | 0 | Modules complémentaires (protocole Internet version 4 (IPv4)), sécurité du protocole Internet (IPsec) (Protocole Internet version 6 (IPv6)) |

NOTE 1 – Les évaluations relatives aux critères énumérés correspondent au modèle de protocole type, mais ne sont pas valables pour toutes les technologies de communication axée sur les bus de terrain. Par exemple, le réseau CAN ne dispose pas de protocole inhérent pour la prise en charge des communications en temps réel.

NOTE 2 – Hypothèse: les applications embarquées requièrent généralement des services de communication de type point à point ou point à multipoint. Ces types de topologies doivent être desservies par une topologie de connexion logique, ce qui suppose que les topologies de connexion de couche liaison soient considérées comme une "couche protocole" commune aux technologies de communication examinées.

NOTE 3 – Les réseaux Ethernet embarqués seront déployés et exploités uniquement en "mode commutation" (en suivant principalement les objectifs définis en matière de qualité de service), ce qui suppose la prise en charge de modèles de connexion point à point uniquement au niveau de la couche support physique Ethernet. Les supports physiques ne sont pas partagés, mais chaque point d'extrémité Ethernet de couche 1 a un accès exclusif aux ressources de la couche physique. Toutefois, les topologies de communication point à multipoint sont aussi prises en charge, soit directement, par une capacité Ethernet native de diffusion et multidiffusion intégrée moyennant les fonctions de transmission de la couche liaison de données, soit indirectement, par les protocoles de couche supérieure (tels que le protocole IP et les types d'adresses réseau associées: multidiffusion, unidiffusion ou diffusion).

NOTE 4 – L'intégrité relative à la sécurité vise à la fois: a) l'intégrité des bits; et b) l'intégrité des données, à savoir l'intégrité des données binaires d'une unité de données de protocole (*protocol data unit*, PDU) ou de la totalité de l'unité PDU (au niveau de certaines couches de protocole).

NOTE 5 – Les mesures de sécurité sont évaluées, que la spécification du protocole correspondant comporte ou non des fonctionnalités de sécurité inhérentes.

Les critères de comparaison décrits ci-dessus portent sur l'ingénierie de base des réseaux et l'ingénierie des services de communication ainsi que sur des aspects propres à la sécurité.

### 6.3 Services de communication utilisant l'Ethernet dans les applications automobiles

À l'heure actuelle, l'Ethernet automobile est principalement utilisé pour l'établissement de diagnostics et la transmission de flux multimédias, par exemple les données vidéo provenant de capteurs de caméras utilisées par les systèmes évolués d'aide à la conduite (ADAS). En outre, depuis le milieu des années 2010, cette technologie permet aux nœuds de calcul (comme les unités de contrôle électronique ou ECU) des véhicules de communiquer via l'Ethernet.

### 6.3.1 Diagnostics

La méthode de diagnostic classique utilisée pour un véhicule consiste à connecter un outil de diagnostic à un port OBD-II et à communiquer avec l'unité ECU cible au moyen d'un protocole de service de diagnostic unifié (SDU). Le protocole SDU est un protocole au niveau de l'application élaboré par le secteur automobile, qui permet aux systèmes de diagnostic de communiquer avec les unités ECU pour diagnostiquer les dérangements et reprogrammer les unités ECU en conséquence (voir la norme [b-ISO 14229-5]).

La communication de diagnostic par protocole Internet (DoIP) est basée sur le protocole IP (voir la norme [b-ISO 13400-2]). Le protocole DoIP permet la transmission de messages SDU entre un véhicule et des équipements de test externes via l'Ethernet et il devient possible d'extraire les données de diagnostic d'un véhicule à distance, sans avoir à se connecter physiquement au véhicule. Le protocole DoIP assure l'encapsulation des messages SDU dans les paquets TCP ou dans les datagrammes UDP, comme indiqué dans la Figure 2.

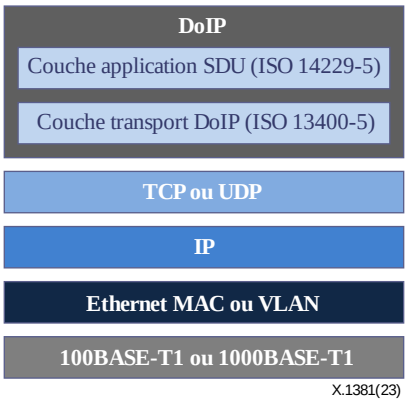


**Figure 2 – Pile de protocoles pour la communication de diagnostic via l'application du protocole Internet**

Le protocole DoIP lui-même ne prévoit aucun mécanisme pour la sécurité des communications. En général, les messages ne sont ni authentifiés ni chiffrés, de quelque manière que ce soit. Le protocole DoIP prévoit une authentification dans la ou les couches supérieures, mais elle n'est pas obligatoire.

### 6.3.2 Flux de médias dans le contexte des services multimédias

En ce qui concerne les systèmes ADAS, les véhicules hautement automatisés et totalement autonomes doivent déployer un grand nombre de capteurs, par exemple des caméras haute définition et des fonctions de connectivité, afin d'obtenir suffisamment d'informations relatives à l'environnement du véhicule. En outre, nombre de véhicules sont équipés de dispositifs qui utilisent ou transmettent des flux de médias au niveau des applications (à ne pas mélanger avec des (sous-)couches de support physique dans le cas de l'Ethernet). Ces dispositifs sont utilisés par des systèmes d'infoloisirs, de surveillance du périmètre de vision, d'aide au stationnement, d'aide au maintien dans la file de circulation ou encore de vision nocturne. Dans le cas des caméras, des flux de médias relativement importants (en termes de volume de trafic) sont générés conformément à des objectifs de qualité de service définis par les applications, à savoir une transmission haute qualité à faible temps de latence. Si le protocole est celui du réseau CAN, les prescriptions précédentes sont impossibles à satisfaire en raison des limitations propres à la conception du protocole, telles que l'intervalle de taille des données utiles.

L'Ethernet automobile peut satisfaire à ces prescriptions en utilisant le cadre défini par l'IEEE pour le pontage audio/vidéo (AVB).

NOTE – Le terme AVB désigne un ensemble de normes [b-IEEE 802.1], qui comprend les normes [b-IEEE 802.1Qav], [b-IEEE 802.1AS] et [b-IEEE 802.1Qat]. En 2012, le groupe de travail IEEE AVB a donc changé de nom pour s'appeler Groupe de travail TSN, et ses travaux porteront désormais également sur les normes AVB.

Les normes AVB peuvent satisfaire aux prescriptions plus générales concernant la mise en réseau sensible au temps (TSN), ce qui permet aux fonctions d'infoloisirs, de commande de carrosserie et d'assistance au conducteur, voire les fonctions cruciales de sécurité, d'être prises en charge par un seul et même réseau.

Dans le cas d'un système de surveillance du périmètre de vision, un réseau de caméras offre une vue d'ensemble synchronisée à 360° de l'environnement du véhicule. Ce flux de média vidéo peut être envoyé au système d'alerte du conducteur, par un système d'affichage tête haute ou un système de navigation vidéo, par exemple. Il peut aussi être synchronisé avec des données de capteur supplémentaires et les unités ECU associées via le réseau AVB.

### 6.3.3 Réseau dorsal du réseau embarqué

Les véhicules modernes peuvent être dotés de plus de 100 unités ECU. Un nœud ECU ou de calcul de véhicule renvoie à un nœud de réseau dans la topologie de réseau IVN Ethernet, doté d'un ou plusieurs nœuds d'extrémité (selon le nombre d'interfaces de connexion Ethernet physiques, logiques ou virtuelles par nœud de calcul). En outre, le nombre d'unités ECU peut encore augmenter. Par ailleurs, les systèmes ADAS et les véhicules autonomes exigent aux réseaux IVN une capacité de transport dans le réseau (désignée couramment par le terme "largeur de bande") de plus en plus importante.

En outre, les anciens protocoles IVN utilisent un système de faisceau de câblage, qui est lourd et coûteux. En utilisant l'Ethernet comme réseau dorsal du réseau IVN, il est possible de réduire jusqu'à 80% des coûts de connexion à l'intérieur du véhicule et jusqu'à 30% de la masse du câblage à l'intérieur du véhicule.

Comme le montre la Figure 1, le réseau IVN basé sur l'Ethernet comporte plusieurs domaines. Les anciens protocoles IVN sont utilisés dans chacun des domaines et l'Ethernet est employé pour les communications entre domaines, c'est-à-dire au niveau du réseau central (par comparaison avec les réseaux TIC), que l'on désigne aussi couramment par le terme réseau dorsal.

L'Ethernet automobile a une topologie différente de celle d'un système de bus. Aucun conducteur de bus n'est connecté à plusieurs unités ECU, capteurs et actionneurs. En revanche, ils sont connectés à un commutateur Ethernet en mode point à point. Les messages envoyés d'un domaine à un autre peuvent être traités facilement par les fonctions d'interfonctionnement de réseau, telles que les fonctions des commutateurs Ethernet, des passerelles VLAN, éventuellement aussi les routeurs IP et les passerelles IP du réseau IVN basé sur l'Ethernet. À l'inverse, les anciens protocoles de bus de terrain embarqués doivent être pris en charge par le réseau et, éventuellement, dans le cadre de l'interfonctionnement des services, et sont généralement situés dans les passerelles, lorsqu'ils communiquent avec les points d'extrémité situés dans le réseau Ethernet.

## 7 Analyse des menaces

### 7.1 Méthode pour l'analyse des menaces

Le présent paragraphe analyse les scénarios de menace pour la sécurité dans le contexte des réseaux Ethernet embarqués. Les menaces générales identifiées pour les véhicules connectés sont décrites dans la Recommandation [UIT-T X.1371].

Il convient de fixer des objectifs de sécurité afin de définir le concept de sécurité. Une analyse des menaces et une évaluation des risques (TARA) sont effectuées afin de déterminer la méthode de traitement des risques en fonction de l'objectif de sécurité. Pour effectuer une analyse des menaces et

une évaluation des risques, il convient d'identifier les ressources de sécurité et les objectifs de sécurité, ainsi que les menaces connexes. Le concept de sécurité peut être déterminé si la méthode de traitement des risques respectifs est choisie au moyen d'une évaluation des incidences et d'une évaluation de la faisabilité des attaques prenant en compte les ressources de sécurité, les objectifs de sécurité et les menaces identifiés (voir [b-ISO/SAE 21434] pour de plus amples informations). Conformément à la méthode d'analyse des menaces décrite dans la norme [b-ISO/SAE 21434], on identifiera dans ce qui suit les ressources de sécurité et les objectifs de sécurité associés, ainsi que les menaces de sécurité.

Les processus d'évaluation des incidences, d'évaluation de la faisabilité des attaques et de prise de décision concernant les risques n'entrent pas dans le cadre de la présente Recommandation et feront l'objet d'un complément d'étude.

## 7.2 Ressources de sécurité

On entend par ressource de sécurité tout objet de données, fonction ou ressource qui doit être protégé. En ce qui concerne les réseaux IVN fondés sur Ethernet, les ressources de sécurité retenues sont énumérées dans le Tableau 2.

**Tableau 2 – Ressources de sécurité**

| Ressource | Description |
|---|---|
| Données de gestion | Les données de gestion couvrent les deux catégories (Note 1) suivantes:<br>1) Les données de configuration, qui caractérisent le comportement fonctionnel des éléments de réseau ou des fonctions de réseau ayant une connectivité Ethernet, par exemple une passerelle, un commutateur Ethernet, un système de détection des intrusions (IDS) ou un pare-feu.<br>2) Les données d'état opérationnel, qui décrivent non seulement le comportement réel de ces entités de réseau, mais aussi celui de tous les services de gestion utilisant des notifications [b-UIT-T M.3702] telles que la signalisation des alarmes [b-UIT-T M.3703] dans le cadre de la gestion des défaillances.<br>Les flux de données de gestion pour les deux catégories entre l'entité de gestion et l'entité gérée font en principe l'objet d'une protection de la sécurité. Toutefois, les incidences sur la sécurité engendrées notamment par la manipulation des données de configuration sont en général beaucoup plus importantes que celles portant sur les données d'état opérationnel. D'autre part, la suppression intentionnelle d'une alarme émise par un élément de réseau Ethernet risque par exemple d'aggraver la situation de défaillance existante. |
| Unités de données de protocole de la couche 2 relatives aux communications Ethernet | Le trafic Ethernet est constitué du trafic de la couche liaison de données, c'est-à-dire des trames Ethernet de commande d'accès au support (MAC) (en tant qu'unités PDU de la couche 2) qui sont transférées au réseau IVN automobile fondé sur Ethernet. |
| Données de gestion générées par la journalisation (Note 2) | La détection réussie des événements de sécurité ainsi que les informations associées peuvent faire l'objet d'une vérification. |
| Données de chiffrement | Clés et certificats pour les systèmes symétriques et asymétriques, y compris les autres justificatifs d'identité, tels que les mots de passe. |

**Tableau 2 – Ressources de sécurité**

| Ressource | Description |
|---|---|
| Image de micrologiciel ou de logiciel | Code compilé à exécuter au niveau des nœuds informatiques embarqués tels que les unités ECU. |
| NOTE 1 – Voir le cadre de gestion de réseau applicable à l'Ethernet, par exemple tel qu'il est décrit dans [b-UIT-T M.3010, b-UIT-T X.703, b-UIT-T G.8013, b-UIT-T Y.1730]. Les données de gestion des entités de réseau Ethernet sont fondées sur la norme YANG [b-IETF RFC 6020], qui est le texte de référence en ce qui concerne la spécification et le langage de modélisation des données de gestion. La norme IEEE 802 (propriétaire technique de l'Ethernet) définit des modèles de données de gestion fondés sur le langage YANG pour toutes les entités Ethernet, constituant ainsi la principale référence en ce qui concerne les données de gestion pour la présente Recommandation.<br>NOTE 2 – La gestion des fonctions de journalisation [b-UIT-T M.3705] n'est pas couverte par ce tableau. La journalisation désigne ici les événements du système engendrés par les flux d'informations de gestion qui sont enregistrés par les fonctions de journalisation (voir [b-UIT-T G.7710] sur les flux de données de gestion internes des équipements de réseau).<br>NOTE 3 – Ce type de fonction de détection appartient à la catégorie des fonctions de vérification des hypothèses statistiques, principalement en raison des incertitudes relatives à la description des événements ou à la description des conditions de la règle de politique pour l'identification non ambiguë des événements considérés. Par conséquent, une détection réussie ne donne que des résultats intrinsèquement probabilistes, y compris des faux positifs, qui viennent s'ajouter aux vrais positifs. La qualité de la détection doit donc être qualifiée et quantifiée, par exemple par une estimation du taux de résultats qui ne sont pas des faux positifs attendu. | |

## 7.3 Objectifs de sécurité

Les ressources de sécurité (voir le § 7.1) sont analysées en fonction d'une liste d'objectifs de sécurité, comme indiqué dans le Tableau 3.

**Tableau 3 – Objectifs de sécurité**

| Ressource de sécurité | Objectif de sécurité | Explication |
|---|---|---|
| Données de gestion | Intégrité, confidentialité | Les données qui déterminent le comportement fonctionnel d'éléments de réseau Ethernet tels que la passerelle de véhicule, le commutateur Ethernet, le système IDS et le pare-feu ne devraient pas être manipulées. |
| Unités de données de protocole de la couche 2 relatives aux communications Ethernet | Confidentialité | Il s'agit d'empêcher la divulgation des unités de données de protocole propres à une couche ((Lx)-PDU) transférées vers un réseau IVN automobile fondé sur Ethernet. |
| | Disponibilité | Les services de communication utilisant le réseau IVN automobile fondé sur Ethernet devraient pouvoir fonctionner chaque fois que cela est nécessaire, dès lors que les contraintes bien définies qui leur sont imposées sont respectées. |
| | Authenticité | Les communications sur le réseau IVN automobile fondé sur Ethernet devraient détecter et rejeter les usurpateurs d'autres composants. |
| | Intégrité | Il s'agit d'empêcher la manipulation des données de communication échangées sur le réseau IVN automobile fondé sur Ethernet. |

**Tableau 3 – Objectifs de sécurité**

| Ressource de sécurité | Objectif de sécurité | Explication |
|---|---|---|
| Données de gestion générées par la journalisation | Intégrité | Il s'agit d'empêcher la manipulation des preuves relatives aux événements de sécurité journalisés et des informations associées pouvant faire l'objet d'une vérification sans que cela soit détecté. L'intégrité désigne l'intégrité des bits et des données dans le cadre des informations journalisées. |
| Données de chiffrement | Confidentialité | Il s'agit d'empêcher la divulgation des clés secrètes et des clés privées, ainsi que des justificatifs d'identité de l'utilisateur tels que les mots de passe. |
| | Intégrité | Il s'agit d'empêcher la manipulation des clés et des certificats sans que cela soit détecté. |
| Image de micrologiciel ou de logiciel | Confidentialité | Il s'agit d'empêcher la divulgation, à des entités non autorisées, du contenu des micrologiciels et des logiciels tel que les codes compilés et les données d'étalonnage concernant la propriété intellectuelle. |
| | Intégrité | Il s'agit d'empêcher la manipulation des images de micrologiciels et de logiciels, notamment dans le cadre de procédures de modification des capacités (par exemple au moyen d'un micrologiciel par voie hertzienne, d'un logiciel par voie hertzienne ou d'un système de gestion des logiciels de façon générale). |

## 7.4 Menaces identifiées

### 7.4.1 Menaces pour la confidentialité

– Exposition non autorisée du trafic de communication Ethernet (constitué d'unités PDU de la couche physique (L1) ou de la couche liaison de données (L2) du réseau Ethernet).

L'auteur d'une attaque peut renifler le trafic de communication Ethernet en se connectant au composant chargé de la communication externe grâce au commutateur Ethernet. Il analyse ensuite les informations du trafic de communication en reniflant les unités PDU relatives au réseau Ethernet.

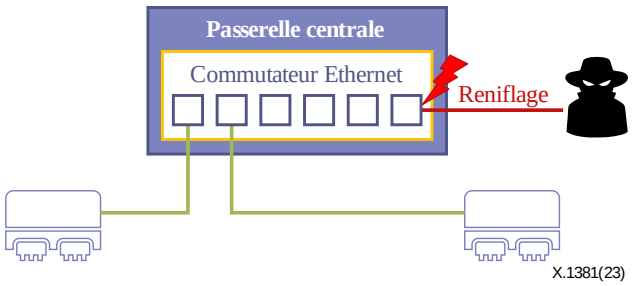


**Figure 3 – Menaces pour la confidentialité liées au reniflage**

– Exposition non autorisée de données de chiffrement.

L'auteur d'une attaque peut renifler des données de chiffrement:

- en récupérant des données de chiffrement en ouvrant physiquement le boîtier où elles sont stockées;
- en lisant des données de chiffrement à partir de la mémoire de chaque composant au niveau duquel elles sont utilisées;

- en modifiant le micrologiciel et en altérant le flux de commande afin d'exposer des données de chiffrement.

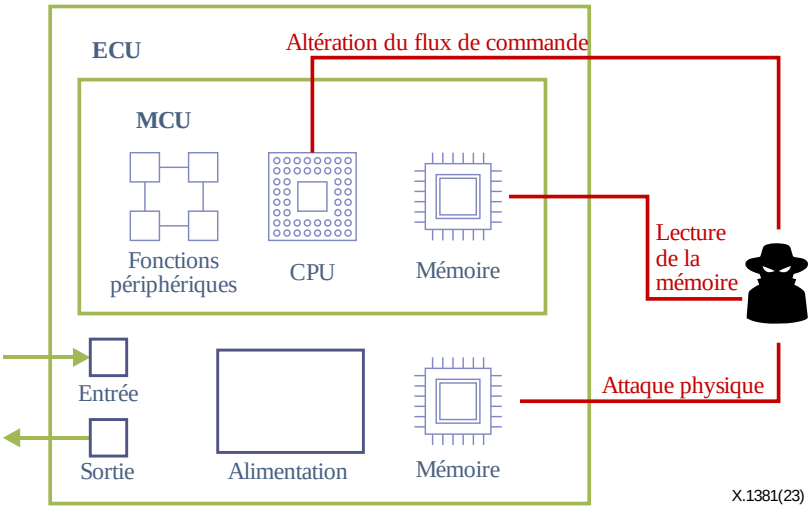


**Figure 4 – Menaces pour la confidentialité des données de chiffrement**

### 7.4.2 Menaces pour l'intégrité

Le concept de l'intégrité est limité aux objets de données en général, correspondant ici à des cas d'utilisation particuliers de la sécurité.

– Manipulation de données de configuration.

L'auteur d'une attaque peut manipuler les données de configuration du commutateur Ethernet.

– Manipulation de données de journaux.

L'auteur d'une attaque peut supprimer ou modifier des données de journaux et, en particulier, de journaux d'audit en ce qui concerne des événements de sécurité relatifs au système IDS, au pare-feu et au système de communication par voie hertzienne.

– Manipulation de données de chiffrement.

L'auteur d'une attaque peut modifier par lui-même des données de chiffrement valides.

– Manipulation d'un micrologiciel.

L'auteur d'une attaque peut transformer un micrologiciel en micrologiciel malveillant.

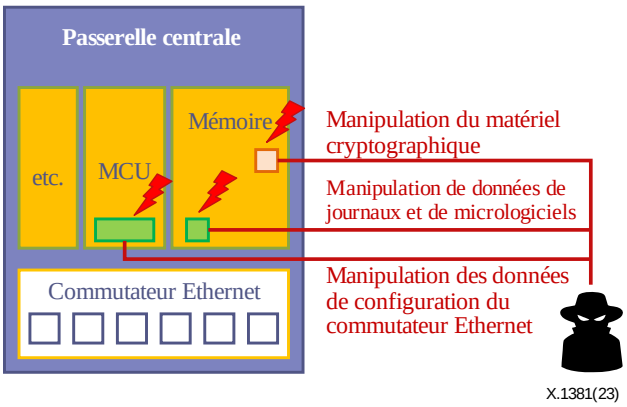


**Figure 5 – Menaces pour l'intégrité des unités de données pendant les communications**

### 7.4.3 Menaces pour la disponibilité

La disponibilité des attributs de qualité du système renvoie ici à la disponibilité des services de communication assurant les communications fondées sur Ethernet, ce qui est généralement traduit par les exigences relatives à la disponibilité des connexions de réseau et des connexions propres à une couche, ce qui, là encore, peut mener par exemple à la disponibilité des conduits Ethernet dans le cas d'un réseau IVN Ethernet à conduits redondants.

– Menaces propres à la disponibilité: Attaque par déni de service (DoS) sur un réseau IVN Ethernet.

L'auteur d'une attaque peut lancer une attaque DoS pour entraver le fonctionnement d'une unité ECU donnée, par exemple une passerelle CGW, une passerelle périphérique de véhicule ou une unité de commande de la connectivité.

Comme indiqué dans la Figure 6, l'auteur d'une attaque peut rendre une unité ECU ou une passerelle CGW spécifique indisponible pour les unités ECU ciblées par l'attaque en utilisant des techniques d'attaque DoS bien connues, telles que les attaques propres au protocole de transport IP comme les attaques par inondation SYN du protocole TCP ou les attaques *Teardrop* visant le protocole TCP. En outre, l'auteur d'une attaque peut entraîner l'épuisement des ressources du réseau IVN au moyen d'attaques telles que des tempêtes de diffusion visant la couche 2, de sorte que les trames MAC Ethernet normales (comme les unités PDU de la couche 2) ne puissent plus être échangées.

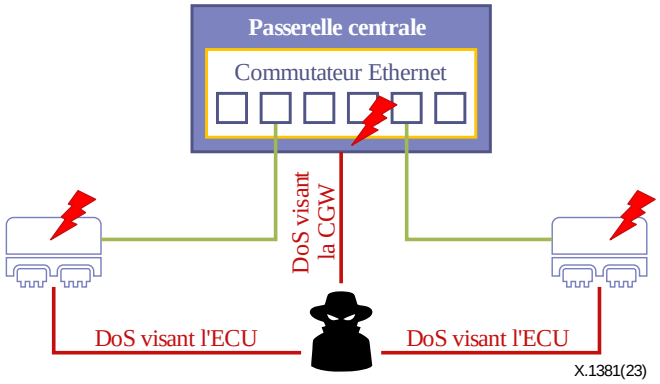


**Figure 6 – Menaces pour la disponibilité**

### 7.4.4 Menaces pour l'authenticité

– Usurpation de l'identité des nœuds de calcul des véhicules (par exemple les unités ECU).

L'auteur d'une attaque peut usurper l'identité d'un composant valide tel qu'une unité ECU et envoyer des messages malveillants à d'autres composants. Il peut se faire passer pour un point d'extrémité de communication valide (par exemple hébergé par une unité ECU) et envoyer des messages malveillants ou recevoir le trafic de communication transmis. Dans l'exemple de la Figure 7, la situation normale est représentée par les connexions de couche supérieure entre les unités ECU A et B (par exemple les connexions de transport IP point à point): l'unité ECU-A envoie le trafic Ethernet à l'unité ECU-B (l'inverse étant aussi possible). L'auteur d'une attaque prétend être l'unité ECU-A en utilisant des méthodes d'attaque telles que l'usurpation d'adresse ARP ou l'usurpation d'adresse IP (voir par exemple [b-IETF RFC 2827][b-IETF RFC 4953] [b-IETF RFC 6575][b-IETF RFC 6959]), puis envoie un message malveillant à l'unité ECU-B.

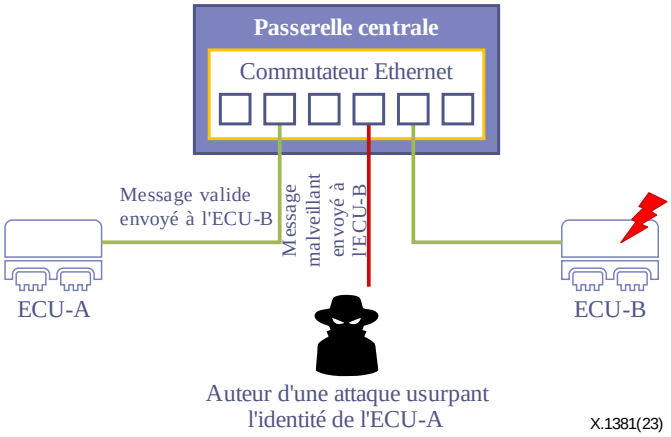


**Figure 7 – Menaces pour l'authenticité**

## 8 Exigences de sécurité

Le présent paragraphe décrit les exigences de sécurité permettant de faire face aux menaces identifiées dans les environnements IVN fondés sur Ethernet.

### 8.1 Confidentialité

– [SR-01] Il est recommandé qu'une unité ECU qui stocke et utilise des données de chiffrement utilise un stockage sécurisé tel qu'un module matériel de sécurité (HSM) pour stocker ces données en toute sécurité.

– [SR-02] Il est recommandé de déployer les algorithmes et protocoles bien connus spécifiés, par exemple, par des organisations internationales de normalisation.

– [SR-03] Il est recommandé d'utiliser des mécanismes de sécurité permettant d'empêcher l'écoute illicite dans les messages de communication Ethernet.

  Différents protocoles de sécurité propres à une couche peuvent être appliqués, à titre d'option, à la couche de protocole correspondante afin de chiffrer cette couche ainsi que les unités PDU propres au protocole (entièrement ou en partie) en tant que composantes du trafic de communication Ethernet dans un véhicule. Comme exemples de tels protocoles de sécurité relatifs aux communications, on peut citer la sécurité des commandes d'accès au support (MACsec), la sécurité IPsec, la sécurité TLS et la sécurité DTLS.

– [SR-04] Une entité non autorisée ne peut pas divulguer des données de chiffrement sensibles.

  Le mécanisme de sécurité d'un véhicule n'est plus sécurisé si des données de chiffrement sont exposées à des entités non autorisées.

– [SR-05] Il est recommandé que seuls le personnel et les équipements autorisés puissent manipuler les données de chiffrement pendant la phase de production, conformément à une politique de contrôle d'accès relative au réseau embarqué.

– [SR-06] Il est recommandé que la table d'adresses MAC du commutateur Ethernet soit configurée de manière statique.

  Les unités ECU qui peuvent accéder au réseau Ethernet embarqué sont prédéfinies en configurant la table d'adresses MAC du commutateur Ethernet de manière statique.

  Les adresses MAC dynamiques peuvent engendrer des problèmes de sécurité tels que l'usurpation d'identité et l'inondation MAC. Le commutateur peut diffuser la trame de données à tous les ports réseau lorsqu'un grand nombre d'adresses MAC sont stockées dans la table. Dans le cas d'un véhicule, la table d'adresses MAC peut être configurée de manière statique pour éviter ces problèmes de sécurité, car dans ce cas, l'unité ECU qui communique avec le commutateur est déjà spécifiée.

– [SR-07] Il est recommandé de désactiver la fonction d'apprentissage dynamique de la table d'adresses MAC du commutateur Ethernet.

  La désactivation de la fonction d'apprentissage dynamique de la table d'adresses MAC permet d'empêcher les inondation MAC, qui consistent en la transmission de messages Ethernet à des destinations indues.

  Néanmoins, si cette fonction est essentielle pour le fonctionnement ou la maintenance du véhicule, le commutateur ne devrait mémoriser les adresses MAC apprises que pour une durée limitée.

– [SR-08] Il est recommandé que des adresses IP fixes soient attribuées par la fonction de gestion de réseau pertinente aux interfaces de réseau IP des fonctions de l'hôte IP (par exemple celles hébergées par des unités ECU) qui utilisent Ethernet.

NOTE – Les fonctions de gestion de réseau spécifiques assurent ici la gestion des identités ainsi que la gestion des adresses réseau. Ces fonctions de gestion peuvent être exécutées au cours de différentes phases du cycle de vie et de l'exploitation du réseau IVN fondé sur l'Ethernet. La gestion de la configuration peut notamment être à priori entièrement statique ou consister en une combinaison de fonctions statiques et dynamiques, ce qui dépend également de l'utilisation ou non de protocoles opérationnels de réseau relatifs aux couches Ethernet et Internet.

Cette exigence de sécurité s'applique non seulement aux différentes unités ECU dans leur ensemble, mais également à chaque partition ou nœud d'un réseau Ethernet (par exemple chaque machine virtuelle).

### 8.2 Intégrité

– [SR-09] Il est recommandé que les données de journaux et de configuration d'un commutateur Ethernet soient protégées contre les modifications et suppressions non autorisées.

– [SR-10] Il est recommandé que les mises à jour des données de configuration ne soient effectuées que par des entités autorisées.

– [SR-11] Il est recommandé qu'une unité ECU utilise des fonctionnalités de démarrage sécurisé comprenant une vérification de l'intégrité de son micrologiciel.

L'intégrité du micrologiciel d'une unité ECU ainsi que celle des données d'un commutateur Ethernet stockées dans la mémoire d'une unité ECU devraient être vérifiées avant ou pendant l'exécution. Une vérification de l'intégrité de la configuration et des paramètres d'entrée du micrologiciel peut être utilisée pour garantir un démarrage sécurisé.

### 8.3 Disponibilité

Dans ce contexte, la disponibilité fait référence à la disponibilité dans le réseau des domaines Ethernet, autrement dit au service de communication disponible. Les attaques de sécurité peuvent avoir des incidences sur les objectifs en matière de disponibilité définis, mais c'est également le cas d'événements relatifs à des aspects autres que la sécurité (par exemple la panne de composant ou l'échec d'une communication).

Par conséquent, les exigences relatives à la disponibilité (définies dans le présent paragraphe) sont en fait des exigences de sécurité qui peuvent avoir une incidence sur les objectifs en matière de disponibilité.

– [SR-12] Il est recommandé que les attaques DoS contre les réseaux IVN fondés sur Ethernet soient prises en compte lors de la phase de conception d'un véhicule.

– [SR-13] Il est recommandé qu'un commutateur assure la détection des attaques DoS utilisant des messages de communication Ethernet ainsi que la protection contre ces attaques.

– La surveillance et le contrôle des flux de trafic entre les unités ECU sont essentiels afin de réduire au minimum les risques liés aux attaques DoS visant le réseau IVN.

– [SR-14] Il est recommandé d'utiliser des fonctions de sécurité essentielles afin d'assurer l'isolation vis-à-vis des autres réseaux à bord d'un véhicule.

### 8.4 Authenticité

L'authenticité désigne la capacité permettant de garantir que l'information donnée n'a été ni modifiée ni falsifiée et qu'elle a bien été produite par l'entité qui déclare l'avoir fournie.

– [SR-15] Il est recommandé que des contre-mesures soient fournies pour protéger les messages de communication Ethernet contre les attaques par usurpation d'identité.

– [SR-16] Il est recommandé que l'état de fonctionnement temporel des interfaces physiques de réseau Ethernet des éléments de réseau IVN (activer, désactiver), qui ne sont pas destinées à être utilisées dans des véhicules en production, puisse être modifié et que ces interfaces soient désactivées dans la configuration par défaut.

NOTE – Une telle exigence liée à la gestion du réseau implique évidemment la prise en charge d'un modèle de données de gestion à granularité fine adapté pour le réseau Ethernet.

Cette exigence limite la surface d'exposition aux attaques en réduisant le nombre de points d'entrée disponibles.

– [SR-17] Il est recommandé que l'accès à l'interface de communication, qu'il soit effectué dans le domaine matériel ou logiciel, soit limité conformément au principe du moindre privilège.

– [SR-18] Il est recommandé de configurer une interface de débogage dans une unité ECU afin d'assurer une protection contre les entités non autorisées. Cette exigence vise les interfaces de débogage des nœuds de calcul de véhicule tant locales que distantes qui bénéficient d'un accès fondé sur le réseau IVN à ces nœuds de réseau.

Le Tableau 4 indique les correspondances entre les menaces identifiées au paragraphe 7 et les exigences de sécurité définies au paragraphe 8.

**Tableau 4 – Correspondances entre les exigences de sécurité et les menaces**

| Menaces | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Exposition non autorisée d'un message de communication Ethernet | – | X | X | – | – | – | – | – | – | – | – | – | – | – | – | – | – | X |
| Exposition non autorisée de données de chiffrement | X | X | – | X | X | – | – | – | – | – | – | – | – | – | – | – | – | X |
| Manipulation de données de configuration | X | X | – | – | – | X | X | – | X | X | X | – | – | – | – | – | – | X |
| Manipulation de données de journaux | X | X | – | – | – | – | – | – | X | – | X | – | – | – | – | – | – | X |
| Manipulation de données de chiffrement | X | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | X |
| Attaque DoS contre un réseau IVN fondé sur Ethernet | – | – | – | – | – | – | – | – | – | – | – | X | X | X | – | – | – | – |
| Attaque par usurpation de l'identité d'une unité ECU | – | X | – | – | – | X | X | X | – | – | – | – | – | X | X | X | X | X |

Chaque menace identifiée peut être traitée en répondant aux exigences de sécurité correspondantes indiquées par un X. Par exemple, les exigences de sécurité pour la première menace, l'exposition non autorisée d'un message de communication Ethernet, sont les suivantes: [SR-2], [SR-3] et [SR-18].

# 9 Mise en œuvre de réseaux embarqués fondés sur Ethernet sécurisés

## 9.1 Considérations préalables relatives à la mise en œuvre

La présente Recommandation contient des considérations relatives à la mise en œuvre afin:

- de décrire les aspects de la sécurité qui sont régis par des contraintes techniques;
- d'illustrer les problèmes de sécurité propres à la mise en œuvre dans le cas d'une architecture technique IVN type.

La valeur de ces informations de sécurité est intrinsèquement liée uniquement au point de vue technique spécifique adopté, de sorte que ces informations peuvent devenir obsolètes dans l'avenir, par exemple en cas de modification des architectures techniques des systèmes IVN.

Toutefois, il n'existe pas encore de modèles de référence ou d'architectures de référence non techniques applicables aux réseaux IVN qui pourraient servir de base pour l'analyse des aspects de sécurité propres à la mise en œuvre. Par conséquent, la présente Recommandation contient au moins certaines considérations relatives à la sécurité fondées sur l'examen d'exemples de systèmes techniques IVN (tels que décrits au paragraphe 6).

## 9.2 Fonctions de passerelle de sécurité associées à l'Ethernet automobile

La surveillance et le contrôle du flux de communication entre les différents domaines d'un réseau logique (par exemple un réseau VLAN, un sous-réseau IPv4, un sous-réseau défini par un préfixe IPv6; chaque domaine de réseau logique représente un domaine de sécurité spécifique selon ses attributs de sécurité) sont importants pour réduire le plus possible les risques liés aux accès non autorisés et aux attaques DoS dans les réseaux IVN fondés sur Ethernet. Les pare-feu en particulier ou les passerelles de sécurité en général sont utilisés pour autoriser ou refuser des données de communication conformément à des règles prédéterminées au niveau du réseau IVN ou au niveau de la jonction du réseau embarqué et du réseau externe, afin d'accroître le niveau de sécurité du véhicule.

Les composants techniques suivants, qui permettent de surveiller les messages de communication provenant de l'extérieur du véhicule ou du réseau IVN, sont recommandés pour la mise en œuvre de ces fonctions de passerelle de sécurité (comme les pare-feu) selon leur état actuel dans l'architecture technique E/E de véhicule type.

– Commutateur Ethernet.

NOTE 1 – Le composant logique constitué par le commutateur Ethernet représente un type de nœud de réseau et non un nœud d'extrémité. Il existe deux possibilités de mise en œuvre: un commutateur Ethernet en tant que composant technique autonome ou intégré de manière monolithique en tant que nœud d'entrée ou d'extrémité dans un nœud de calcul du véhicule.

– Passerelle périphérique de véhicule.

NOTE 2 – Le choix d'origine car ce composant technique représente le seul point d'observation pour le trafic normal de communication V2X.

– Unité ECU: lorsque l'unité ECU reçoit des communications directes externes.

NOTE 3 – Un nœud de calcul de véhicule peut fournir des interfaces de communication supplémentaires pour les communications directes externes au véhicule (c'est-à-dire en contournant la passerelle périphérique de véhicule), par exemple à des fins de diagnostic.

Le pare-feu utilise plusieurs mécanismes pour le filtrage des paquets, y compris le filtrage statique des paquets, l'inspection des paquets sans état ou avec état, l'inspection des paquets peu approfondie, moyennement approfondie ou même approfondie.

NOTE 4 – Les termes imagés "peu approfondie", "approfondie", etc. doivent être mis en correspondance et associés avec: a) la couche protocole; et b) le type de contexte PDU des informations (voir par exemple les Recommandations [b-UIT-T Y.2770][b-UIT-T Y.2771]) afin d'être non ambigus; par exemple, "inspection peu approfondie" correspondrait en général à un contrôle d'en-tête au niveau des couches L3,4 dans le cas du trafic Internet.

En particulier, le mécanisme statique de filtrage des paquets est fondé sur des règles de politique prédéfinies. Il est donc recommandé de définir des règles de politique particulières en fonction de l'architecture E/E du véhicule et du protocole de communication appliqué. Par ailleurs, la politique de pare-feu suit par défaut la méthode de la liste blanche, ce qui, fondamentalement, bloque toutes les communications qui ne sont pas explicitement autorisées.

L'une des principales caractéristiques d'un pare-feu est la défense contre les attaques DoS. Les pare-feu peuvent protéger les réseaux contre les attaques DoS en fixant des seuils au moyen de valeurs préenregistrées, telles que des compteurs, ou en appliquant des filtres en matière de fréquence.

Une autre caractéristique complémentaire du pare-feu est la fonction de journalisation (c'est-à-dire que l'élément de réseau constitué par le pare-feu en tant qu'entité gérée fournit une fonction intégrée de gestion de registre de consignation conformément à la Recommandation [b-UIT-T M.3705]). Les événements liés à la sécurité devraient en général faire l'objet de services de journalisation. Ainsi, les pare-feu, les systèmes IDS ou les passerelles de sécurité doivent figurer dans les informations générales de journalisation lorsqu'un événement de sécurité se produit, ce qui permet non seulement aux spécialistes d'analyser la situation relative à l'événement, mais aussi d'améliorer la précision de la politique de pare-feu grâce à des études portant par exemple sur les enregistrements relatifs à des blocages. Par conséquent, il est nécessaire d'utiliser le mécanisme de chiffrement pour le stockage du registre de consignation afin d'en garantir l'intégrité.

### 9.3 Configuration des réseaux VLAN sécurisés

La configuration d'un réseau VLAN sécurisé est très importante pour que la sécurité des communications du réseau IVN réponde aux exigences [SR-14] et [SR-17]. Les constructeurs OEM devraient constituer l'autorité chargée des spécifications de ce type de réseau VLAN car leur configuration dépend de l'architecture E/E choisie pour le véhicule.

Chaque réseau VLAN a une valeur unique appelée identificateur VLAN (ID). Conformément à la spécification relative aux réseaux VLAN, les identificateurs VLAN (VID) peuvent être compris entre 0 et 4 094, mais les identificateurs VLAN prédéfinis décrits dans le Tableau 5 ne doivent pas être utilisés. L'identificateur VLAN 1 peut aussi être utilisé pour les attaques par double encapsulation. Le commutateur devrait donc changer l'identificateur VLAN 1 en un autre identificateur VLAN.

**Tableau 5 – Identificateurs VLAN réservés**

| Valeur de l'identificateur VLAN (hexadécimale) | Signification/utilisation |
|---|---|
| 0 | L'identificateur VLAN nul correspond au cas où l'en-tête d'étiquette ne contient que des informations de priorité; aucun identificateur VLAN n'est présent dans la trame. Cette valeur d'identificateur VLAN ne devrait pas être configurée comme l'identificateur d'un port de réseau VLAN (PVID) ou comme un élément d'un ensemble d'identificateurs VLAN, ni être configurée dans une quelconque entrée d'une base de données de transfert (FDB) ou être utilisée dans une quelconque opération de gestion. |
| 1 | Valeur par défaut de l'identificateur PVID utilisée pour classer les trames à leur arrivée au niveau d'un port de pont. La valeur de l'identificateur PVID d'un port peut être modifiée par une opération de gestion. |

**Tableau 5 – Identificateurs VLAN réservés**

| Valeur de l'identificateur VLAN (hexadécimale) | Signification/utilisation |
|---|---|
| FFF | Réservé pour une utilisation lors de la mise en œuvre. Cette valeur d'identificateur VLAN ne doit pas être configurée comme un identificateur PVID ou comme un élément d'un groupe d'identificateurs VLAN, ni être transmise dans un en-tête d'étiquette. Cette valeur d'identificateur VLAN peut servir à indiquer une correspondance avec un caractère générique pour l'identificateur VLAN dans les opérations de gestion ou les entrées d'une base de données FDB. |

L'auteur d'une attaque peut surveiller le trafic Ethernet au moyen d'un accès non autorisé à partir d'un autre réseau VLAN grâce à une attaque par "saut de VLAN". Pour contrer cette attaque, la configuration doit être telle que les trames qui ne sont pas étiquetées VLAN soient éliminées. Cependant, les exceptions suivantes peuvent se présenter. Pour la synchronisation temporelle, les messages sont envoyés via le protocole de précision temporelle, qui nécessite l'envoi de trames sans étiquettes VLAN, conformément à la norme [b-IEEE 802.1AS].

L'auteur d'une attaque faisant partie d'un réseau VLAN d'origine peut réaliser une attaque par double encapsulation en utilisant l'identificateur par défaut du réseau VLAN d'origine. L'auteur de l'attaque ajoute deux étiquettes à la trame: la première contient l'identificateur par défaut du réseau VLAN d'origine; et la seconde l'identificateur du réseau VLAN cible de l'auteur de l'attaque. Lorsque la trame avec les étiquettes ainsi ajoutées passe par le premier commutateur, la première étiquette est supprimée et la trame est transmise au commutateur suivant avec la deuxième étiquette. Ce commutateur transmet alors la trame au réseau VLAN cible en utilisant la deuxième étiquette restante. De cette façon, l'auteur de l'attaque peut envoyer le message au réseau VLAN cible. L'identificateur par défaut du réseau VLAN d'origine doit donc être modifié afin d'empêcher cette attaque.

## 9.4 Sécurité des commutateurs Ethernet dans le contexte de l'automobile

Le pont Ethernet IEEE, également connu sous le nom de commutateur Ethernet, offre intrinsèquement une base d'informations de transfert (FIB) comme moyen de base pour les processus de transmission et de commutation. Une telle base FIB contient une table d'adresses MAC.

NOTE 1 – La présente Recommandation utilise un modèle très abstrait de commutateur Ethernet, axé uniquement sur les fonctions de réseau susceptibles d'être concernées par les questions de sécurité. Un aperçu détaillé de toutes les fonctions de base du commutateur Ethernet est donné dans la norme [b-IEEE Std 802.1Q].

NOTE 2 – Par exemple, la norme [b-IEEE 802.1Q] décrit un modèle de règles (de politique) relatives au traitement des trames MAC Ethernet, qui distingue les règles d'entrée, de transmission et de sortie. Cela présente un intérêt particulier, notamment dans le contexte des réseaux VLAN.

Les commutateurs Ethernet classiques fournissent des mécanismes d'acquisition dynamique d'adresses destinés aux réseaux qui nécessitent une certaine souplesse. Lorsqu'une nouvelle unité ECU est connectée au port du commutateur, une entrée correspondant à l'adresse MAC d'un nœud d'extrémité Ethernet est automatiquement ajoutée à la table d'adresses MAC, afin que cette unité puisse communiquer avec d'autres unités ECU dans l'ensemble du domaine du réseau Ethernet, grâce à cette étape de commutation.

NOTE 3 – Il peut y avoir plusieurs commutateurs Ethernet sur le trajet de communication de bout en bout.

La fonction d'acquisition dynamique d'adresses MAC facilite les accès non autorisés au réseau et devrait être désactivée. Cette fonction peut être nécessaire dans le cas où des dispositifs externes de diagnostic doivent être utilisés à des fins de maintenance ou de diagnostic. Le commutateur devrait alors permettre de limiter la durée de validité des adresses MAC acquises de manière dynamique. Ces

deux recommandations semblent apparemment contradictoires, mais elles dépendent en fait du contexte opérationnel particulier du réseau Ethernet embarqué: avec ou sans connectivité externe, par exemple, un domaine de réseau Ethernet DoIP. Cette dépendance relative au contexte opérationnel du réseau peut amener à formuler des recommandations conditionnelles en matière de sécurité, en définissant par exemple une fenêtre temporelle limitée lorsque l'acquisition dynamique d'adresses est activée.

L'usurpation d'adresse MAC est une attaque bien connue contre les réseaux informatiques pouvant être mise en œuvre dans des scénarios d'attaque visant des véhicules. Pour protéger le réseau IVN, l'authentification et la fiabilité des dispositifs connectés au moyen d'un contrôle d'accès au réseau fondé sur le port devraient être garanties si une méthode d'accès différente est utilisée. Ce type de contrôle authentifie un composant avant de lui accorder l'accès au réseau. Le commutateur Ethernet ne communique avec le réseau que si l'authentification réussit.

Pour atténuer les attaques DoS, le commutateur doit empêcher les tempêtes de diffusion et prendre en charge des limites de débit fondées sur les ports pour la réception de paquets (voir le contrôle des paramètres du trafic Ethernet dans la Recommandation [b-UIT-T Y.1222]).

En ce qui concerne la sécurité du commutateur, l'intégrité des données de gestion de la configuration du commutateur doit être garantie et cela ne devrait être possible qu'au moyen d'un mécanisme de programmation sécurisé ou d'un protocole de gestion sécurisé pour les mises à jour.

– En général, les fonctions de sécurité nécessaires à l'exploitation et à la gestion des commutateurs Ethernet dans les applications automobiles qui intègrent leur propre processeur sont les suivantes: Stockage sécurisé.

  Un stockage sécurisé garantit la confidentialité et l'intégrité des données stockées. Les données telles que les clés et les commandes MAC devraient être protégées au moyen d'un stockage sécurisé tel qu'un module HSM.

– Démarrage sécurisé

  Le démarrage sécurisé vérifie l'intégrité du logiciel à chaque cycle de démarrage. Lors d'un démarrage initial, un code d'authentification de message pour l'image du logiciel est généré et stocké de manière sécurisée. Au démarrage suivant, si le code d'authentification de message généré est le même que celui qui a été stocké, l'intégrité du logiciel est assurée.

– Interface de débogage sécurisée

  Une interface de débogage sécurisée empêche les accès non autorisés à cette interface. Il est généralement recommandé de supprimer les interfaces de débogage, afin qu'il ne soit pas possible de se connecter à une entité de débogage. Toutefois, si ces interfaces sont nécessaires pour la garantie ou la maintenance d'un produit, seules les entités autorisées devraient pouvoir y accéder.

– Mise à jour sécurisée des logiciels

  La mise à jour sécurisée d'un logiciel permet la reprogrammation d'un logiciel uniquement si l'authenticité de ce logiciel est confirmée. Le fournisseur du logiciel génère une signature numérique au moyen de sa clé privée et la joint à l'image du logiciel lorsqu'il envoie cette dernière. Le destinataire vérifie que la signature numérique est générée par le fournisseur au moyen de la clé publique de ce dernier, afin de s'assurer de l'authenticité du logiciel.

# Appendice I

## Description de certains protocoles de réseaux embarqués fondés sur Ethernet, avec des points d'extrémité de communication situés dans des nœuds de calcul AUTOSAR ou autres qu'AUTOSAR

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

Il existe un certain nombre de protocoles de communication pour les réseaux fondés sur Ethernet et, dans de nombreux cas d'utilisation relatifs aux communications à l'intérieur des véhicules fondées sur Ethernet, l'un ou plusieurs de ces protocoles sont déployés. De plus, les nœuds de calcul des réseaux IVN peuvent non seulement être exploités via un système reposant sur des architectures logicielles fondées sur AUTOSAR (comme la plate-forme AUTOSAR classique, ou la plate-forme AUTOSAR adaptative), mais également en utilisant des architectures de communication logicielles autres qu'AUTOSAR.

On suppose donc fondamentalement qu'un réseau IVN est composé d'un mélange de nœuds de calcul AUTOSAR et autres qu'AUTOSAR, dans le contexte de l'ingénierie IVN Ethernet ou Internet.

### I.1 Aperçu général et domaine d'application

Le présent Appendice décrit brièvement les protocoles destinés à être utilisés pour les communications à l'intérieur des véhicules fondées sur Ethernet, comme le montre la Figure I.1.

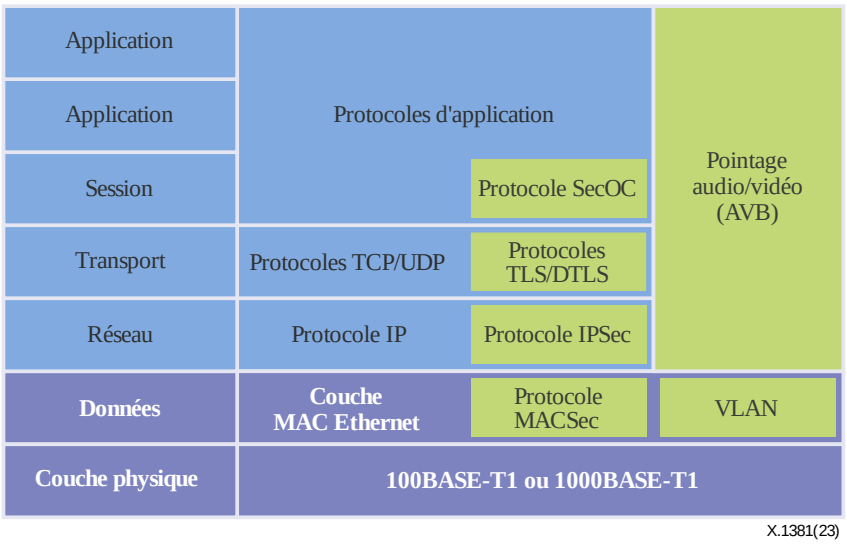


**Figure I.1 – Prise en charge de services de communication fondés ou non sur IP sur Ethernet avec protocoles de sécurité associés selon les couches destinés aux réseaux embarqués**

Il convient de noter que la Figure I.1 porte sur les services de transport de communication et non sur les protocoles de couche session et application. Par exemple, l'intergiciel modulable orienté service, fondé sur AUTOSAR fonctionnant sur le protocole IP, qui est un protocole de couche session et présentation utilisé pour les services de communication orientés service fondés sur le protocole IP, n'entre pas dans le cadre de la présente Recommandation.

## I.2 Protocoles de sécurité des couches inférieures (limite inférieure incluse) utilisés pour garantir la sécurité des communications embarquées fondées sur l'architecture AUTOSAR

Il convient de rappeler que l'architecture AUTOSAR est une architecture logicielle, et qu'elle exclut de ce fait les architectures de déploiement. Le système logiciel suivant peut donc être mappé aux éléments du processeur de nombreuses manières (en utilisant la concomitance ou le parallélisme, en remplaçant la pile de communication fondée sur l'architecture AUTOSAR par une pile disponible sur le marché, etc.).

Ethernet fait partie des normes d'AUTOSAR, depuis la publication de la norme classique 4.0 [b-Autosar 654] de ce partenariat. Dans l'architecture AUTOSAR, la pile de communication Ethernet est parallèle (dans l'architecture logicielle) aux instances de pile CAN, LIN et FlexRay.

Le routeur de transfert des unités de données de protocole (PDU) AUTOSAR est chargé d'acheminer, à l'intérieur des nœuds de calcul, les unités PDU AUTOSAR entre les applications AUTOSAR et les interfaces de réseau associées au point d'extrémité de communication.

NOTE 1 – En conséquence, dans l'architecture AUTOSAR, il y a un chevauchement entre la fonction de routeur de transfert des unités PDU et les fonctions classiques de routage du trafic au niveau des points d'extrémité de communication dans les architectures autres qu'AUTOSAR, mais il ne faut pas confondre ces fonctions.

Le message généré par l'application est envoyé au routeur de transfert des unités PDU, qui transmet un message à l'interface correspondante ou au module de protocole de transport correspondant. Chaque interface/module de protocole de transport transmet le message à une interface de réseau par l'intermédiaire d'un pilote approprié. Dans le cas d'Ethernet, le routeur de transfert des unités PDU envoie un message à un adaptateur de connexion (c'est-à-dire un point d'accès aux services de la couche 4 pour une communication TCP ou UDP), qui le transmet à l'interface Ethernet via un module utilisant le protocole TCP/IP. La Figure I.2 montre le flux de commande et de données dans la pile de communication AUTOSAR étendue.

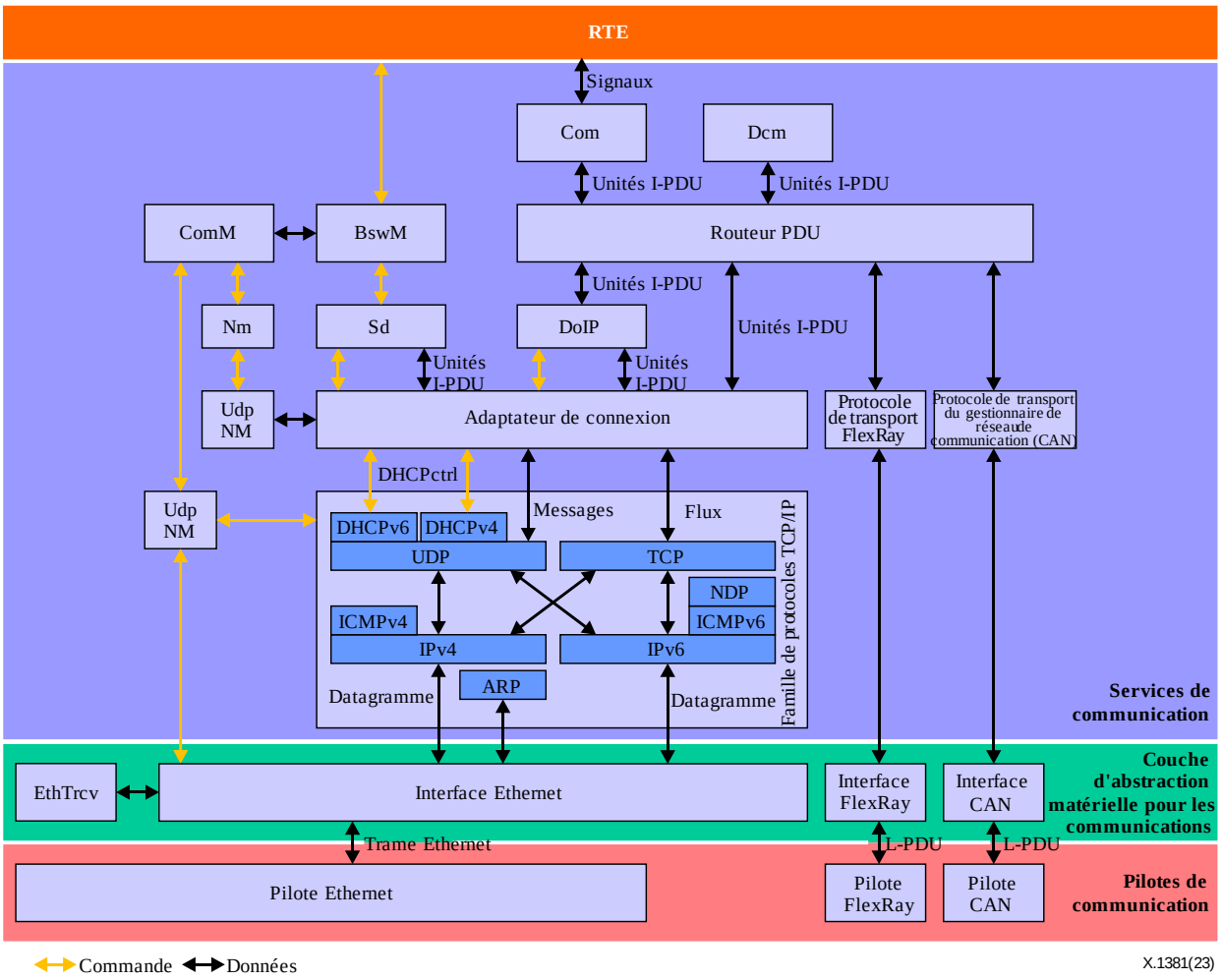


**Figure I.2 – Pile de communication AUTOSAR étendue (architecture logicielle uniquement) (Source: [b-AUTOSAR 617])**

NOTE 2 – AUTOSAR a introduit la notation PDU, qui diffère de la sémantique PDU existante utilisée dans le domaine des TIC (comme précisé dans la Recommandation [b-UIT-T X.200]). Les unités I-PDU, N-PDU ou L-PDU situées à l'intérieur du système logiciel AUTOSAR sont mappées, ou apparaissent au niveau des interfaces de communication sur les réseaux en tant qu'unité PDU de la couche x, en général appelée unité (Lx)-PDU, en fonction de la pile de protocole utilisée.

### I.2.1 Communication de bord sécurisée

Les services de chiffrement d'AUTOSAR sont assurés par le service de chiffrement, le matériel de sécurité abstrait et le pilote de chiffrement, appelés collectivement la pile de chiffrement. Le pilote de chiffrement dépend du microcontrôleur et fournit l'interface capable d'accéder au matériel. La fonction abstraite du matériel de sécurité fournit une interface commune sous la forme d'un intergiciel entre le service de chiffrement et le matériel de sécurité. L'interface commune assure l'indépendance entre un pilote de chiffrement, qui dépend du matériel de sécurité, et un service de chiffrement qui est un service de couche supérieure. Le gestionnaire de services de chiffrement (CSM) est le seul module inclus dans le service de chiffrement.

La communication de bord sécurisée (SecOC) est un service du gestionnaire CSM qui garantit l'intégrité des messages de communication.

L'objectif du service SecOC est de fournir des mécanismes d'authentification pratiques et efficaces sur le plan des ressources au niveau des logiciels (ou de la couche de protocole) d'une unité PDU. Ce type de mécanisme d'authentification utilise un code d'authentification de message fondé sur un algorithme de chiffrement symétrique, car il devrait permettre de minimiser la consommation de ressources supplémentaire imposée aux systèmes d'ancienne génération.

Le service SecOC utilise un gestionnaire CSM pour générer et vérifier un code d'authentification de message. Un gestionnaire CSM peut accélérer le calcul d'un code d'authentification de message à l'aide d'un module HSM.

On trouve dans la Figure I.3 un aperçu général fonctionnel du service SecOC.

Un émetteur génère une unité PDU sécurisée en ajoutant une étiquette d'authentification contenant un code d'authentification de message et une valeur d'actualisation à l'unité PDU. La valeur d'actualisation peut être une valeur de compteur ou un horodatage.

Un récepteur vérifie l'étiquette d'authentification contenue dans l'unité PDU sécurisée reçue, c'est-à-dire qu'il génère le code d'authentification de message sur la base des données de l'unité PDU sécurisée reçue et le compare au code d'authentification de message reçu.

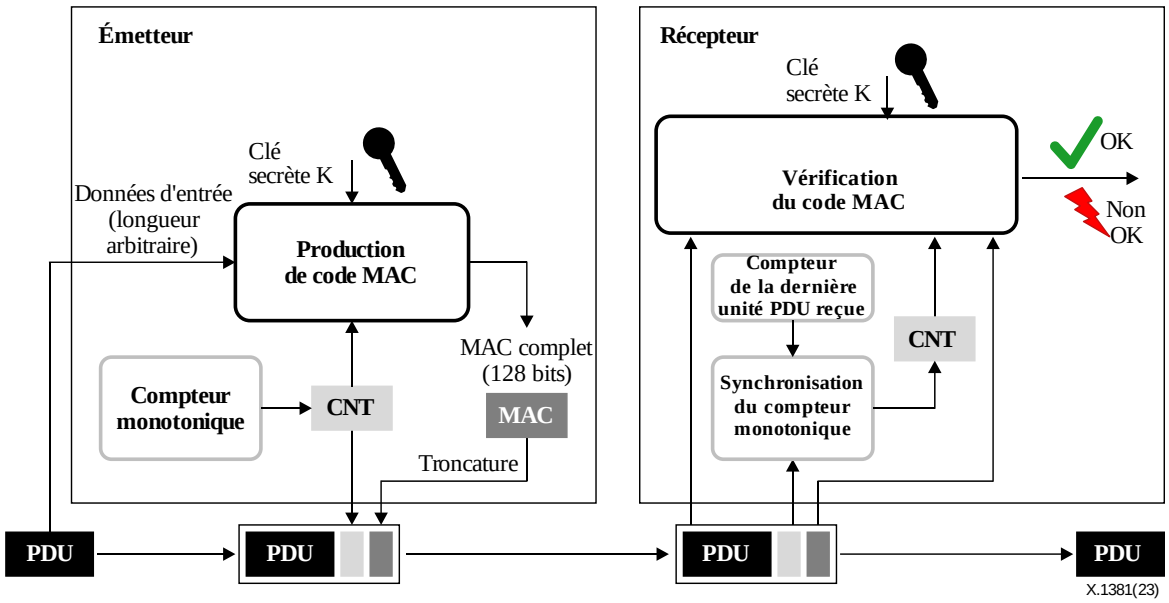


**Figure I.3 – Authentification de message et vérification de l'actualisation [b-Autosar 654]**

### I.2.2 Sécurité de la couche transport

Le protocole TLS fournit des services de communication sécurisée de bout en bout par le biais de protocoles de transport fiables tels que le protocole TCP.

AUTOSAR ne prend pas en charge les versions du protocole TLS antérieures à TLS 1.2.

NOTE – Voir également la référence [b-IETF RFC 8996] en ce qui concerne le déclassement de TLS 1.0 et de TLS 1.1.

Pour utiliser le protocole TLS dans AUTOSAR, le gestionnaire de service de chiffrement autorise la réalisation des tâches de chiffrement et des opérations relatives aux clés utilisées par le sous-module TLS et IPsec. On trouvera des exigences et des spécifications détaillées dans la norme [b-AUTOSAR 617].

### I.2.3 Sécurité de la couche transport en mode datagramme

Ce sujet fera l'objet d'un complément d'étude, qui figurera dans une prochaine édition de la présente Recommandation.

### I.2.4 Sécurité du protocole Internet

En principe, IPsec est le protocole natif de sécurité de couche réseau pour les réseaux IP, qui prend en charge l'authentification et le chiffrement. Le protocole IPsec est facultatif pour le protocole IPv4, mais obligatoire pour le protocole IPv6. Le déploiement du protocole IPsec dans les TIC, si tant est que le protocole y soit déployé, est généralement limité aux réseaux IP couvrant de petites zones, mais pas de grandes zones, en raison de la disponibilité limitée de la connectivité IP totale de bout en bout (par exemple interruptions dues à des passerelles de camouflage de la topologie IP ou à des passerelles de sécurité IP).

Toutefois, les réseaux IP embarqués appartiennent à la catégorie des réseaux de (très) petite taille et sont soumis à une seule autorité de gestion de réseau, ce qui ne doit pas empêcher l'utilisation du protocole IPsec, limité aux domaines de réseau IP embarqués.

Conformément à la norme [b-AUTOSAR 617], le mode tunnel du protocole IPsec n'est actuellement pas disponible dans l'architecture AUTOSAR. Seul le mode transport peut être utilisé. L'architecture ne prend pas non plus en charge le protocole IPv6 et la multidiffusion. On trouvera des exigences et des spécifications détaillées dans la norme [b-AUTOSAR 970].

NOTE – Cette édition de la présente Recommandation ne contient pas de considérations de sécurité propres aux versions IP pour le protocole IPsec.

## I.3 Communication de diagnostic sur le protocole Internet

Le protocole DoIP est utilisé à des fins de diagnostic, sans aucun moyen de sécurité intégré.

DoIP est un protocole de transport fondé sur IP spécifié dans la norme [b-ISO 13400-2]. Il permet de transférer des messages entre des services SDU dans un véhicule et un équipement de test externe via l'Ethernet. Le protocole DoIP dépend des protocoles suivants:

– DHCP;

– ICMP;

– recherche d'adresse MAC fondée sur l'adresse IP (IPv4: ARP, IPv6: protocole de découverte de voisin).

Dans le protocole UDP, chaque datagramme contient uniquement un message DoIP. En ce qui concerne les données fondées sur le protocole TCP, l'en-tête sépare les différents messages DoIP dans le flux de données.

Il convient d'utiliser le port TCP 13400 bien connu et enregistré par l'autorité IANA pour les communications DoIP (demandes de diagnostic et réponses de diagnostic) de l'équipement de diagnostic externe vers l'ECU du véhicule.

Le protocole DoIP ne prévoit aucun mécanisme pour la sécurité des communications. Les messages ne sont ni authentifiés ni chiffrés de quelque manière que ce soit. Par conséquent, lors de la conception de services DoIP, il convient d'envisager d'utiliser différentes couches de protocoles de sécurité.

## I.4 Sécurité des commandes d'accès aux médias

MACsec est un protocole normalisé de sécurité [b-IEEE 802.1AE] qui permet de sécuriser les communications pour tout le trafic sur la couche liaison de données. Le protocole MACsec prend en charge la sécurité de bout en bout ou bond par bond au niveau des connexions de couche 2 Ethernet (c'est-à-dire des "liaisons" de bout en bout ou des liaisons locales) entre les nœuds d'extrémité Ethernet ou les nœuds de commutation. Le protocole MACsec comprend l'authentification et le chiffrement, ou le déchiffrement, ce qui permet d'identifier et de prévenir la plupart des menaces de sécurité, y compris les attaques par déni de service, par intrusion, par intercepteur, par usurpation d'identité, par écoute passive et par réexécution.

# Appendice II

## Passerelles de véhicule avec connectivité Ethernet, IP ou Internet

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

### II.1 Motifs

Une passerelle centrale, une passerelle périphérique de véhicule ou une passerelle de véhicule de manière générale joue un rôle déterminant dans l'architecture de sécurité des communications embarquées, en particulier pour les domaines et les services de communication de réseau IP et Ethernet. L'emplacement topologique dans le réseau d'une passerelle centrale en tant que passerelle périphérique de véhicule suppose et détermine un rôle de passerelle de sécurité entre les domaines de réseau interne et externe du véhicule.

La spécification et la normalisation de tels types d'élément de réseau sont généralement associées à des considérations de sécurité explicites ou même à des lignes directrices et des spécifications en matière de sécurité.

### II.2 Objectif du présent Appendice

Le présent Appendice donne une liste non exhaustive des normes relatives aux passerelles de véhicule présentant un intérêt pour la sécurité, qui pourraient être utiles, par exemple parce qu'elles fournissent des informations complémentaires sur la sécurité des communications, dans le cadre de la présente Recommandation. Le présent Appendice pourrait faire l'objet de mises à jour dans des éditions ultérieures de la présente Recommandation.

### II.3 Recommandations relatives aux passerelles de véhicule sélectionnées contenant des informations sur la sécurité

Le présent paragraphe énumère les Recommandations relatives à la sécurité, sans pour autant considérer que ces Recommandations sont exclusivement liées à la sécurité:

– [b-UIT-T F.749.1]: contient les exigences fonctionnelles relatives à la sécurité;

– [b-UIT-T F.749.2]: contient des paragraphes consacrés aux exigences de sécurité pour les communications et aux exigences de sécurité pour les couches supérieures;

– [b-UIT-T H.550]: les aspects liés à la sécurité se rapportent essentiellement à la gestion de la sécurité des passerelles de véhicule;

– [b-UIT-T H.560]: les aspects liés à la sécurité se rapportent essentiellement à l'interface de communication des passerelles de véhicule utilisées pour les communications externes.

# Appendice III

## Sécurité des systèmes de transport intelligents embarqués

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

### III.1 Considérations générales

La notion de système ITS comprend une architecture de communication de véhicule qui couvre le système de communication interne du véhicule et l'interconnexion avec les systèmes et services de communication extérieurs du véhicule. L'élément de réseau et de communication le plus important dans l'architecture globale est la station dite ITS embarquée (voir par exemple [b-ETSI EN 302 665] et [b-ETSI TR 101 607]).

La station ITS correspond à un réseau de communication embarqué qui peut être fondé sur l'Ethernet et offre des services de communication IP ou non IP. Une telle solution technique pour les systèmes ITS correspondrait au champ d'application de la présente Recommandation.

### III.2 Réseaux embarqués de systèmes ITS

Une architecture de réseau embarqué spécifiée par un système ITS comprend les mêmes éléments de réseau que ceux décrits dans le corps de la présente Recommandation, à savoir la passerelle ITS de véhicule, l'hôte ITS de véhicule, le routeur ITS de véhicule, le routeur périphérique ou la passerelle ITS de véhicule, etc. Par conséquent, les lignes directrices relatives à la sécurité des systèmes ITS s'appliquent aussi dans une très large mesure à la présente Recommandation, en particulier lorsque les technologies de communication (c'est-à-dire les protocoles et les piles de protocoles) et l'architecture de communication sont identiques.

### III.3 Sécurité ITS

La présente Recommandation n'a pas pour objet d'évaluer la sécurité définie par les systèmes ITS. Toutefois, il pourrait être utile, pour compléter les connaissances, en particulier en ce qui concerne la sécurité des communications, de consulter les analyses des menaces, des vulnérabilités et des risques menés dans le cadre des systèmes ITS, des lignes directrices en matière de sécurité des systèmes ITS, des services de sécurité ou d'une architecture de sécurité. Voir [b-ETSI TS 102 731] pour obtenir plus de renseignements et d'autres références en matière de sécurité.

# Bibliographie


[b-UIT-T F.749.1] Recommandation UIT-T F.749.1 (2015), *Exigences fonctionnelles pour les passerelles de véhicule*.

[b-UIT-T F.749.2] Recommandation UIT-T F.749.2 (2017), *Exigences de service pour les plates-formes de passerelle de véhicule*.

[b-UIT-T G.7710] Recommandation UIT-T G.7710/Y.1701 (2020), *Prescriptions de la fonction de gestion d'équipements communs*.

[b-UIT-T G.8013] Recommandation UIT-T G.8013/Y.1731 (2015), *Fonctions et mécanismes d'exploitation, d'administration et de maintenance (OAM) pour les réseaux basés sur l'Ethernet.*

[b-UIT-T H.550] Recommandation UIT-T H.550 (2017), *Architecture et entités fonctionnelles des plates-formes de passerelle de véhicule.*

[b-UIT-T H.560] Recommandation UIT-T H.560 (2017), *Interface de communication entre des applications externes et une plate-forme de passerelle de véhicule*.

[b-UIT-T M.3010] Recommandation UIT-T M.3010 (2000), *Principes des réseaux de gestion des télécommunications.*

[b-UIT-T M.3702] Recommandation UIT-T M.3702 (2010), *Services communs de gestion – Gestion des notifications – Spécifications et analyse – Indépendance vis-à-vis du protocole.*

[b-UIT-T M.3703] Recommandation UIT-T M.3703 (2010), *Services communs de gestion – Gestion des alarmes – Spécifications et analyse indépendantes vis-à-vis du protocole.*

[b-UIT-T M.3705] Recommandation UIT-T M.3705 (2013), *Services de gestion communs – Gestion des journaux – Exigences et analyse indépendantes du protocole*.

[b-UIT-T X.200] Recommandation UIT-T X.200 (1994), *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base: le modèle de référence de base.*

[b-UIT-T X.641] Recommandation UIT-T X.641 (1997), *Technologies de l'information – Qualité de service: Cadre général*.

[b-UIT-T X.703] Recommandation UIT-T X.703 (1997), *Technologies de l'information – Architecture de gestion répartie ouverte.*

[b-UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*

[b-UIT-T X.1039] Recommandation UIT-T X.1039 (2016), *Mesures de sécurité techniques pour la mise en œuvre des dimensions de sécurité UIT-T X.805*.

[b-UIT-T Y.1222] Recommandation UIT-T Y.1222 (2004), *Gestion du trafic et des encombrements dans les réseaux Ethernet*.

[b-UIT-T X.1252] Recommandation UIT-T X.1252 (2021), *Termes et définitions de base relatifs à la gestion d'identité.*

[b-UIT-T Y.1730] Recommandation UIT-T Y.1730 (2004), *Prescriptions relatives aux fonctions d'exploitation, d'administration et de maintenance dans les réseaux à base Ethernet et les services Ethernet*.

[b-UIT-T Y.2770] Recommandation UIT-T Y.2770 (2012), *Spécifications relatives au contrôle approfondi des paquets dans les réseaux de prochaine génération.*

[b-UIT-T Y.2771] Recommandation UIT-T Y.2771 (2014), *Cadre pour l'inspection approfondie des paquets.*

[b-Autosar 617] AUTOSAR 617 (2021), *Specification of TCP/IP stack*, AUTOSAR CP R21-11.

[b-Autosar 654] AUTOSAR 654 (2017), *Specification of secure onboard communication*, AUTOSAR CP Release 4.3.1.

[b-Autosar 970] AUTOSAR 970 (2019), *Requirements on IPsec Protocol*, AUTOSAR FO R19-11.

[b-ETSI EN 302 665] Norme européenne ETSI EN 302 665 V1.1.1 (2010), *Intelligent transport systems (ITS); Communications architecture.*

[b-ETSI TR 101 607] Rapport technique ETSI TR 101 607 V1.2.1 (2020), *Intelligent transport systems (ITS); Cooperative ITS (C-ITS); Release 1*.

[b-ETSI TS 102 731] Spécification technique ETSI TS 102 731 V1.1.1 (2010), *Intelligent transport systems (ITS); Security; Security services and architecture.*

[b-IEEE 802.1] IEEE 802.1 (Internet). *Welcome to the IEEE 802.1 Working Group*. Disponible à l'adresse suivante [consulté le 30-06-2022]: https://1.ieee802.org/.

[b-IEEE 802.1AE] IEEE 802.1AE-2018, *IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) security*.

[b-IEEE 802.1AS] IEEE 802.1AS (Internet), *Standard for Local and metropolitan area networks – Timing and synchronization for time-sensitive applications in bridged local area networks.* Disponible à l'adresse suivante [consulté le 30-06-2022]: https://www.ieee802.org/1/pages/802.1as.html.

[b-IEEE 802.1CB] IEEE 802.1CB-2017, *IEEE Standard for local and metropolitan area networks – Frame replication and elimination for reliability*.

[b-IEEE 802.1Q] IEEE 802.1Q-2018, *IEEE Standard for local and metropolitan area network – Bridges and bridged networks.*

[b-IEEE 802.1Qat] IEEE 802.1Qat (Internet), *Standard for Local and metropolitan area networks – Virtual bridged local area networks – Amendment 9: Stream reservation protocol (SRP).* Disponible à l'adresse suivante [consulté le 30-06-2022]: https://www.ieee802.org/1/pages/802.1at.html.

[b-IEEE 802.1Qav] IEEE 802.1Qav-2009, *IEEE Standard for Local and metropolitan area networks – Virtual bridged local area networks amendment 12: Forwarding and queuing enhancements for time-sensitive streams*.

[b-IEEE 1722-2016] IEEE 1722-2016, *Standard for a Transport Protocol for Time-Sensitive Applications in Bridged Local Area Networks*.

[b-IETF RFC 2827] IETF RFC 2827 (1997), *Network ingress filtering: Defeating IP source address spoofing denial of service attacks.*

[b-IETF RFC 4953] IETF RFC 4953 (2007), *Defending TCP against spoofing attacks.*

[b-IETF RFC 6020] IETF RFC 6020 (2010), *YANG – A data modeling language for the network configuration protocol (NETCONF)*.

[b-IETF RFC 6575] IETF RFC 6575 (2012), *Address resolution protocol (ARP) mediation for IP interworking of layer 2 VPNs*.

[b-IETF RFC 6959] IETF RFC 6959 (2013), *Source address validation improvement (SAVI) threat scope.*

[b-IETF RFC 8996] IETF RFC 8996 (2021), *Deprecating TLS 1.0 and TLS 1.1*.

[b-ISO 13400-2] Norme internationale ISO 13400-2:2019, *Véhicules routiers – Communication de diagnostic au travers du protocole internet (DoIP) – Partie 2: Protocole de transport et services de la couche réseau*

[b-ISO 14229-5] Norme internationale ISO 14229-5:2022, *Véhicules routiers – Services de diagnostic unifiés (SDU) – Partie 5: SDU sur l'implémentation du protocole internet (SDUsurIP).*

[b-ISO/SAE 21434] Norme internationale ISO/SAE 21434:2021, *Véhicules routiers – ingénierie de la cybersécurité*.

# 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 |

Publié en Suisse
Genève, 2023