ITUPublications
Recommandations

Union Internationale des Télécommunications
Secteur de la Normalisation

Recommandation

UIT-T X.1380 (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 enregistreurs de données fondés sur le nuage dans les environnements automobiles

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
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.1360–X.1369
Sécurité des systèmes de transport intelligents	**X.1370–X.1389**
Sécurité de la technologie des registres distribués	X.1400–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
SÉCURITÉ DE LA 5G	X.1800–X.1819

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

Recommandation UIT-T X.1380

Lignes directrices relatives à la sécurité des enregistreurs de données fondés sur le nuage dans les environnements automobiles

Résumé

Les enregistreurs de données de route (EDR) comptent parmi les composants les plus importants installés dans les véhicules automobiles en vue d'enregistrer l'état d'un véhicule, ses mouvements et les actes du conducteur au moment où un accident se produit. L'analyse des données de route permet de comprendre les causes d'un accident et d'utiliser les informations correspondantes pour améliorer la sécurité dans les environnements automobiles. Le système de stockage des données pour la conduite autonome est lui aussi un composant important permettant d'enregistrer des données qui donneront une image claire des interactions entre le conducteur et le système de conduite autonome. Or, les enregistreurs de données de route classiques enregistrent et gèrent toutes les données de manière locale, ce qui pourrait entraîner un risque de perte et de destruction des données.

On considère que l'informatique permet d'offrir un accès par le réseau à un ensemble modulable et élastique de ressources physiques ou virtuelles mutualisables, fournies et administrées à la demande et en libre-service. Des secteurs tels que celui de l'aviation essaient déjà d'appliquer des services en nuage aux systèmes d'enregistrement de données afin de renforcer la sécurité dans l'environnement aéronautique. Vu l'évolution actuelle de la connectivité entre véhicules, les enregistreurs EDR et les systèmes de stockage des données pour la conduite autonome seront mis en œuvre pour améliorer la sécurité en général. Toutefois, ces enregistreurs et systèmes présentent diverses vulnérabilités s'agissant de la collecte, du transfert, du stockage, de la gestion et de l'utilisation des données enregistrées en raison des spécificités de l'environnement automobile. Par conséquent, il est nécessaire d'étudier ces vulnérabilités, les exigences de sécurité et les cas d'utilisation pour les enregistreurs de données fondés sur le nuage dans les environnements automobiles.

La Recommandation UIT-T X.1380 donne des lignes directrices relatives à la sécurité des enregistreurs de données fondés sur le nuage dans les environnements automobiles. Elle décrit les menaces, les vulnérabilités, les exigences de sécurité et les cas d'utilisation pour les enregistreurs de données fondés sur le nuage dans les environnements automobiles.

Historique

Édition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1380	03-03-2023	17	11.1002/1000/15106

Mots clés

Nuage, systèmes de stockage des données pour la conduite automatisée (DSSAD) fondés sur le nuage, enregistreurs de données de route (EDR) fondés sur le nuage, enregistreurs de données, DSSAD, EDR, exigences de sécurité, menaces de sécurité.

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

AVANT-PROPOS

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

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

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

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

NOTE

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

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

TABLE DES MATIÈRES

Recommandation UIT-T X.1380

Lignes directrices relatives à la sécurité des enregistreurs de données fondés sur le nuage dans les environnements automobiles

1 Domaine d'application

La présente Recommandation énonce des lignes directrices relatives à la sécurité d'enregistreurs de données fondés sur le nuage tels que les enregistreurs de données de route (EDR) et les systèmes de stockage des données pour la conduite automatisée (DSSAD) dans les environnements automobiles. Elle indique les éléments techniques des systèmes d'enregistrement de données EDR et DSSAD. Elle décrit également les exigences de sécurité et les cas d'utilisation.

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. Toute Recommandation ou autre référence étant sujette à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. 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 authentification [b-UIT-T X.1252]: processus formalisé de vérification qui, s'il est concluant, aboutit à une identité authentifiée pour une entité.

3.1.2 système automatisé de maintien dans la voie [b-UN R157]: système qui est activé par le conducteur et qui maintient le véhicule dans sa voie.

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

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

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

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

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

3.1.8 système de stockage des données pour la conduite automatisée (DSSAD) [b-UN R157]: dispositif permettant de déterminer les interactions entre le système automatisé de maintien dans la voie (ALKS) et le conducteur humain.

3.1.9 enregistreur de données de route (EDR) [b-UN R160]: dispositif ou fonction d'un véhicule qui enregistre les données dynamiques des séries chronologiques pendant la période précédant immédiatement un événement (par exemple vitesse du véhicule par rapport au temps) ou pendant un accident (par exemple delta-v par rapport au temps), aux fins de récupération des données après l'accident. Au sens de la présente définition, les données sur les événements ne comprennent pas de données audio ni vidéo.

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

3.1.11 menace [b-ISO/IEC 27000]: cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un organisme.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 interface du nuage: passerelle du système en nuage, consistant en une interface pour les communications entre un système en nuage et des véhicules, des utilisateurs et des tiers.

3.2.2 gestionnaire général: composante d'un système en nuage qui régit les procédures de base du stockage et de la récupération des données de l'enregistreur de données de route (EDR)/du système de stockage des données pour la conduite automatisée (DSSAD), et vérifie les exigences de base des demandes des utilisateurs, des tiers ou des véhicules.

3.2.3 serveur neutre: serveur indépendant des constructeurs de véhicules, capable de communiquer des données d'enregistreur de données de route (EDR)/de système de stockage des données pour la conduite automatisée (DSSAD) anonymisées ou expurgées des informations d'identification du véhicule (VII).

3.2.4 gestionnaire de règles/politiques: composante d'un système en nuage, intégrée dans le gestionnaire général, qui actualise les règles/politiques.

3.2.5 coordonnateur de stockage: composante d'un système en nuage qui trie les données d'enregistreur de données de route (EDR)/de système de stockage des données pour la conduite automatisée (DSSAD) et les informations d'identification du véhicule (VII) aux fins de stockage et de recherche dans le nuage selon une politique prédéterminée.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ALKS	système automatisé de maintien dans la voie (*automated lane keeping systems*)
API	interface de programmation d'application (*application programming interface*)
CAN	gestionnaire de réseau de communication (*controller area network*)
DoS	déni de service (*denial of service*)
DSSAD	système de stockage des données pour la conduite automatisée (*data storage system for automated driving*)
ECU	module de gestion électronique (*electronic control unit*)
EDR	enregistreur de données de route (*event data recorder*)
FIFO	premier entré, premier sorti (*first-in-first-out*)
GDPR	règlement général sur la protection des données (*general data protection regulation*)
IVN	réseau embarqué (*in-vehicle network*)

JTAG	groupe d'action de test mixte (*joint test action group*)
MAC	code d'authentification de message (*message authentication code*)
MRM	manœuvre à risque minimal (*minimum risk manoeuvre*)
OBD	système d'autodiagnostic (*on-board diagnostic*)
OTA	over-the-air
PII	information d'identification personnelle (*personally identifiable information*)
SDU	services de diagnostic unifiés
TLS	sécurité dans la couche de transport (*transport layer security*)
V2X	véhicule à tout (*vehicle-to-everything*)
VII	information d'identification du véhicule (*vehicle identifiable information*)
VIN	numéro d'identification du véhicule (*vehicle identification number*)

5 Conventions

La présente Recommandation utilise les conventions suivantes:

L'expression "**il est obligatoire**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

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

6 Enregistreurs de données fondés sur le nuage

6.1 Enregistreurs de données de route fondés sur le nuage

On appelle EDR fondé sur le nuage un EDR qui se connecte à des systèmes en nuage (serveur dorsal) pour accroître l'accessibilité et la sécurité des données EDR dans les environnements de véhicules connectés et autonomes.

Un EDR est un dispositif installé aujourd'hui dans la plupart des véhicules pour enregistrer les informations relatives aux accidents ou aux collisions du véhicule afin d'améliorer la sécurité et la qualité de vie dans l'environnement du véhicule.

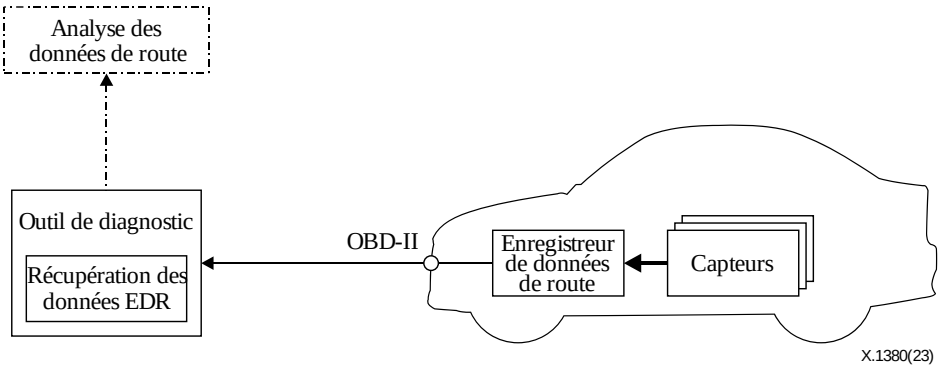

Figure 1 – EDR automobile conventionnel

L'EDR conventionnel, illustré à la Figure 1, est déclenché lorsqu'un événement se produit et que l'état du véhicule remplit certaines conditions (déploiement d'un coussin gonflable frontal, dépassement du seuil d'accélération/décélération, retournement du véhicule, etc.). À son déclenchement, l'EDR

collecte un ensemble prédéterminé de données transmis par des capteurs, puis stocke les données dans son dispositif de stockage interne à mémoire non volatile. Les données sont enregistrées en pratique dans un délai d'une durée comprise entre –5 secondes et +500 millisecondes de l'instant de déclenchement (appelé généralement T0). Les "–5 secondes" et "+500 millisecondes" sont spécifiées diversement selon les réglementations nationales et les constructeurs automobiles.

En règle générale, l'EDR est capable de stocker plus d'un événement sur le véhicule. Lorsque le dispositif de stockage atteint son plein de données relatives à des événements passés, les données les plus anciennes sont écrasées par les nouvelles. Lors d'événements spéciaux comme le déploiement d'un coussin gonflable, l'EDR conventionnel stocke les données recueillies et verrouille le stockage pour empêcher la manipulation ou l'écrasement des données.

Les données stockées sont récupérées au moyen du port du système d'autodiagnostic (OBD)-II par l'outil de diagnostic ou un outil de récupération spécifique et sont utilisées pour analyser la collision ou l'accident. La série de données minimum qui est recueillie est déterminée par la réglementation nationale en matière de véhicules ou la spécification du constructeur de véhicules. Par ailleurs, le format des données de route enregistrées diffère généralement d'un constructeur automobile à l'autre, et fréquemment d'un modèle de véhicule à l'autre. Un logiciel spécialisé est donc nécessaire pour récupérer et analyser les données de route.

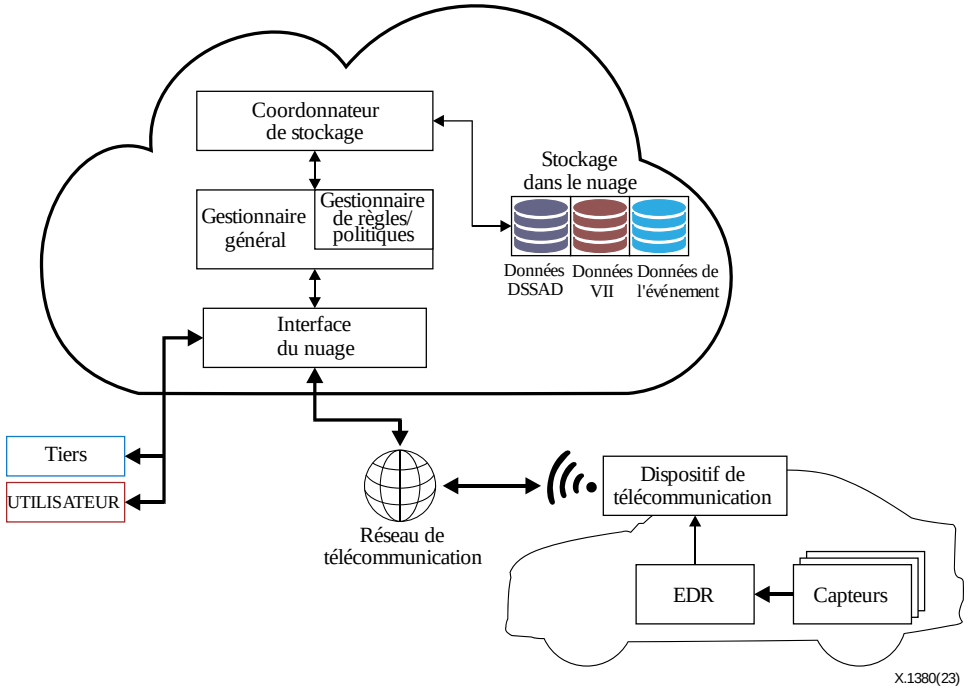

Figure 2 – EDR fondé sur le nuage

Un EDR fondé sur le nuage, décrit à la Figure 2, stocke les données de route sur les systèmes en nuage au moyen d'un dispositif de télécommunication connecté à l'EDR.

La série de données d'enregistrement peut être différente des séries de données EDR conventionnelles en raison des différences systématiques et environnementales entre un EDR conventionnel et un EDR fondé sur le nuage. En outre, un nouveau type de données du module de gestion électronique (ECU) guidant la conduite autonome est susceptible d'être ajouté, étant donné qu'il s'agit de données critiques qui aident à analyser les accidents de véhicules autonomes.

À la différence de l'EDR conventionnel, où de nouvelles données de route écrasent les données d'incident non verrouillées, l'EDR fondé sur le nuage peut enregistrer les données de route sur le stockage en nuage sans écraser des données. Ainsi, l'EDR fondé sur le nuage peut contenir l'intégralité des données enregistrées pour un véhicule sans suppression. C'est là un des principaux avantages de

l'EDR fondé sur le nuage, qui aide considérablement la recherche sur la sécurité routière en utilisant l'intégralité des données EDR.

Les données EDR recueillies et stockées auprès des services en nuage devraient être accessibles aux utilisateurs ou à des tiers lorsqu'une partie dûment autorisée sollicite des données EDR selon la procédure régulière. À la livraison aux parties des données EDR demandées, une procédure d'authentification devrait permettre de vérifier la validité de la demande.

Outre les fonctions de stockage et de transmission des données EDR, l'EDR fondé sur le nuage communique aussi les mises à jour des règles/politiques concernant le système. Tout utilisateur ou tiers peut solliciter les mises à jour des règles/politiques concernant le dispositif EDR du véhicule et de la politique connexe du système en nuage. Une telle demande nécessite un niveau d'autorisation et de vérification de sécurité plus élevé que dans le cas des procédures ordinaires de stockage et de récupération.

Dans le système EDR fondé sur le nuage de la Figure 2, les entités des systèmes en nuage sont définies pour fonctionner à un niveau plus élevé que les fonctionnalités de l'EDR fondé sur le nuage. L'interface en nuage est une passerelle du système en nuage et conserve le journal des accès spécifiés. Le gestionnaire général commande les procédures élémentaires de stockage et de récupération des données EDR. Il vérifie les exigences de base concernant les demandes de l'utilisateur, de tiers ou d'un véhicule, et exécute aussi les mises à jour des règles/politiques avec l'assistance des gestionnaires intégrés de règles/politiques. Le coordonnateur de stockage stocke et récupère les données de route selon une politique prédéterminée. La politique peut inclure le filtrage des données EDR récupérées dans le stockage en nuage par l'auteur de la demande eu égard à sa qualité. Elle peut aussi inclure la méthode de stockage et la procédure de récupération des données EDR sur le stockage en nuage.

6.2 Système fondé sur le nuage de stockage des données pour la conduite automatisée

On appelle système de stockage de données pour la conduite automatisée (DSSAD) un système permettant de savoir qui a demandé à conduire et qui était le conducteur (les deux pouvant être différents, notamment lors des procédures de transition) en stockant un ensemble de données qui donnent une idée précise des interactions entre le conducteur et le système de conduite automatisée. Le DSSAD a été consacré par le Règlement ONU N° 157 [b-UN R157]. Le Règlement reconnaît le DSSAD comme une exigence pour les véhicules à conduite automatisée.

Le DSSAD stocke des informations comme l'activation et la désactivation du système de conduite automatisée, les demandes de transition, les manœuvres d'urgence, etc. Lorsque l'état du système automatisé est désactivé ou qu'une transition est demandée, le motif du changement d'état est stocké dans la DSSAD. Les parties prenantes peuvent déterminer qui a demandé à conduire et qui était chargé effectivement de la conduite en analysant les données DSSAD, qui enregistrent l'interaction entre le système automatisé et le conducteur.

Le DSSAD fondé sur le nuage, décrit à la Figure 3, stocke les données DSSAD sur les systèmes en nuage au moyen d'un dispositif de communications connecté au DSSAD. Le processus de livraison des données DSSAD au système en nuage est identique à celui de l'EDR en nuage. La différence est que des données DSSAD sont envoyées au lieu de données EDR. Les DSSAD transmettent périodiquement des données DSSAD au système en nuage. Les DSSAD sont donc en mesure de répondre de façon souple aux problèmes découlant des limites du stockage DSSAD.

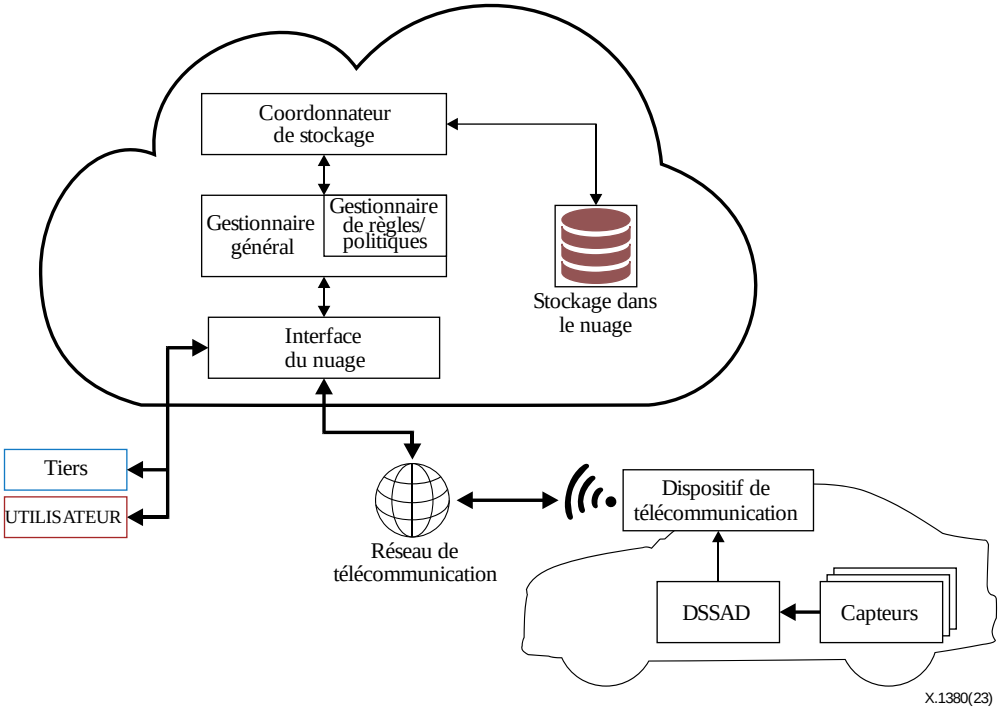

Figure 3 – DSSAD fondé sur le nuage

6.3 Comparaison entre l'EDR et le DSSAD

La comparaison entre l'EDR et le DSSAD est illustrée au Tableau 1.

Tableau 1 – Comparaison entre l'EDR et le DSSAD

	EDR	DSSAD
Objet	Analyse et reconstitution des accidents	Clarification de la responsabilité du véhicule à des moments précis; qui a été invité à conduire et qui était le conducteur
Condition de déclenchement	Événement (par exemple, accident): événement physique à la suite duquel le seuil de déclenchement est atteint	Interaction: modification de l'état de fonctionnement du système, ou demande de modification de l'état de fonctionnement du système
Données recueillies	Ensemble prédéterminé de données utiles pour l'analyse des accidents	Ensemble prédéterminé de données relatives à la commande et à la responsabilité du véhicule
Instant de stockage	Enregistrement des données lorsque le système est déclenché (momentané)	Enregistrement des données pendant toute la durée de la conduite
Moment du transfert	À chaque instant de stockage, au contact mis/coupé	

7 Conception d'un système fondé sur le nuage d'enregistrement des données

7.1 Gestion des données dans le cadre d'un EDR

Un EDR sert à stocker les informations du véhicule concernant certains événements comme le déploiement d'un coussin gonflable. Les données enregistrées dans l'EDR sont utilisées pour l'analyse et la reconstitution des accidents. Ainsi, l'EDR enregistre l'heure de l'événement et l'état du véhicule au moment où l'événement s'est produit.

7.1.1 Durée d'enregistrement des données de route

La Figure 4 décrit comment l'EDR enregistre un événement. Lorsque l'EDR détecte un certain événement, il définit le moment précis où celui-ci est survenu comme le temps zéro (T_0), puis collecte les données préalablement désignées pendant une période d'enregistrement prédéterminée, qui correspond à une durée prédéfinie. T_0^n désigne le moment de survenue du énième événement. Le temps d'enregistrement peut être différent selon les types d'événements car les conditions de déclenchement sont différentes pour chacun. T_{pre} indique le temps qui précède l'événement particulier. T_{post} désigne le temps écoulé après l'événement particulier. L'intervalle de temps peut être décrit comme suit: $[(T_0 - T_{pre}) \sim (T_0 + T_{post})]$.

Lorsque plusieurs événements surviennent successivement, comme décrit à la Figure 4, l'EDR enregistre les données EDR indépendamment du chevauchement des périodes de survenue. La Figure 4 a) indique les périodes enregistrées des événements qui ne présentent pas de chevauchement. La Figure 4 b) indique les périodes enregistrées des événements qui se chevauchent.

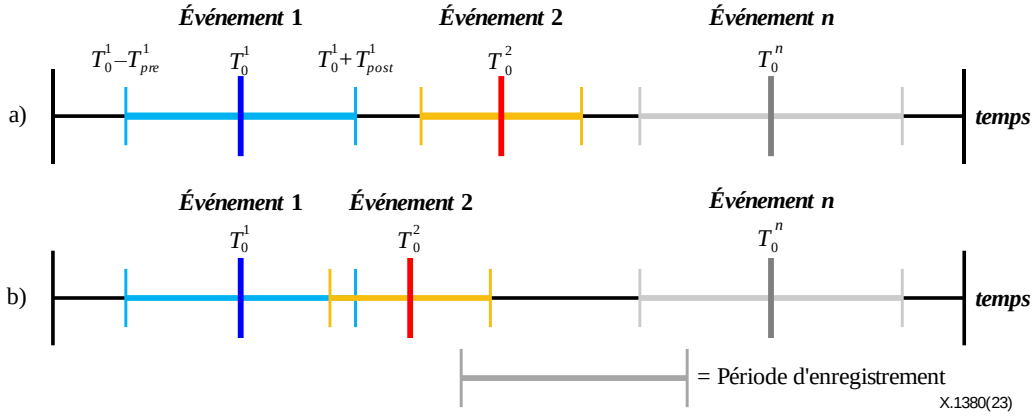

Figure 4 – Période d'enregistrement d'un EDR: a) événements ne présentant pas de chevauchement; b) événements présentant un chevauchement

7.1.2 Blocage des données dans le dispositif de stockage du véhicule

On distingue plusieurs dispositifs de stockage embarqués pour les données EDR. Les conditions prédéterminées étant diverses, plusieurs événements peuvent survenir successivement. Le processus de stockage de l'EDR suit la procédure FIFO (premier entré, premier sorti). Si tous les dispositifs de stockage EDR sont déjà remplis par les événements précédents, les nouvelles données écrasent les plus anciennes. Néanmoins, certaines conditions de déclenchement d'événements prédéterminés, comme le déploiement d'un coussin gonflable frontal, nécessitent le verrouillage du stockage des données après l'écriture des données enregistrées afin que les données stockées ne puissent pas être écrasées. La Figure 5 montre un exemple de procédures d'enregistrement EDR à deux dispositifs de stockage. Elle indique, en a), le processus de stockage des données pour les événements suivants sans condition de verrouillage des données: l'événement 3 s'enregistre sur le dispositif de stockage en écrasant les données de route les plus anciennes. D'autre part, b) et c) indiquent le processus de stockage des données pour les événements suivants avec condition de verrouillage des données: l'événement suivant ne peut être enregistré dans le dispositif de stockage en cas de verrouillage des données. Dans le processus c), en particulier, l'événement 3 ne peut être sauvegardé dans aucun dispositif de stockage car les deux sont pleins et verrouillés par les données des événements antérieurs (événements 1 et 2). Dès lors, la politique doit fixer quelles données seront verrouillées en priorité dans les dispositifs de stockage.

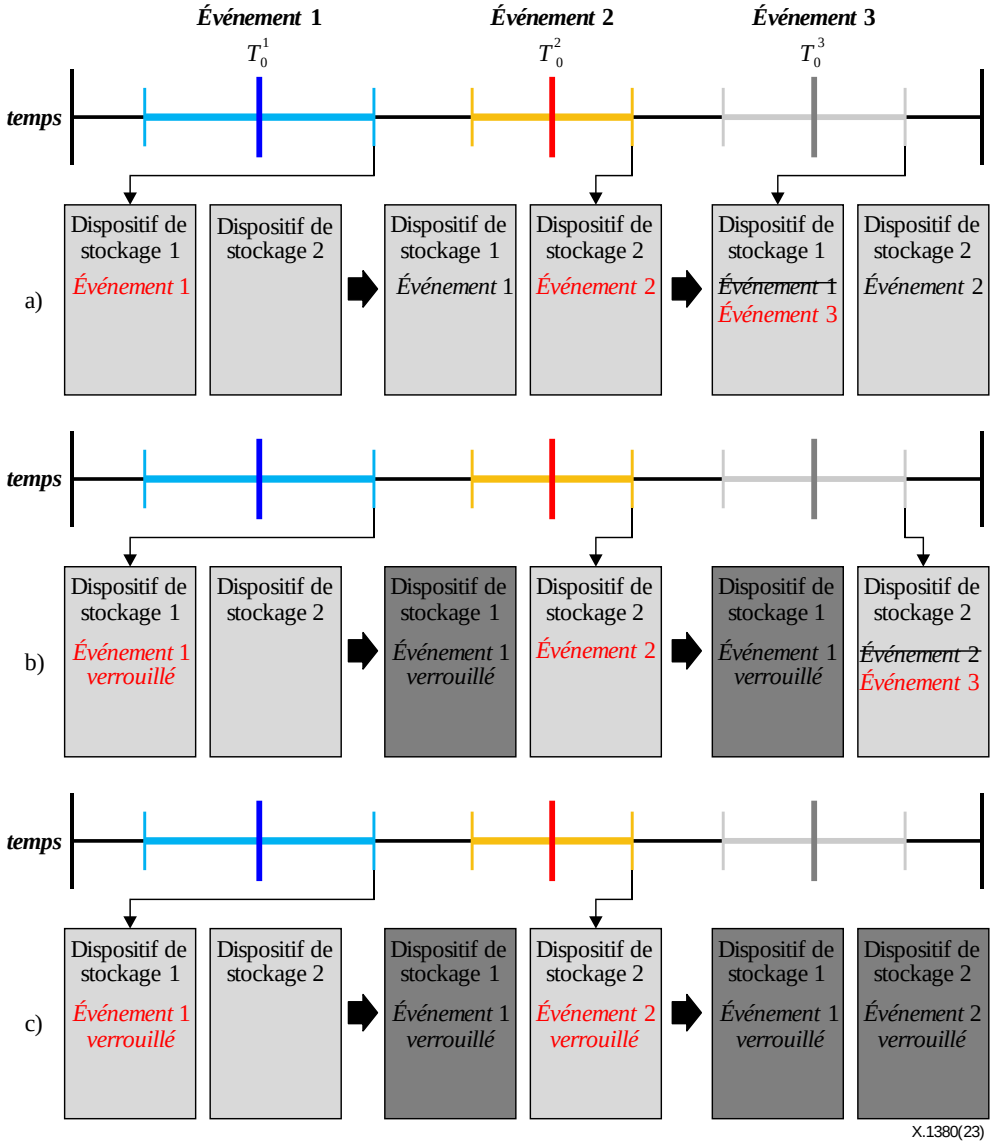

Figure 5 – Exemple d'enregistrement EDR à deux dispositifs de stockage: a) sans verrouillage des données; b) avec condition de verrouillage des données uniquement pour l'événement 1; c) avec condition de verrouillage des données pour l'événement 1 et l'événement 2

7.1.3 Extension de la série de données

La série de données EDR conventionnelle est généralement soumise aux règles fixées par les administrations nationales ou les constructeurs automobiles. Cette série doit être étendue pour prendre en charge les véhicules connectés et autonomes. Ainsi, les données provenant de capteurs de type radar et lidar utilisés dans les véhicules à conduite autonome peuvent être décisives pour enquêter sur les accidents. En outre, les certificats stockés utilisés dans les communications de véhicule à tout (V2X) au cours de l'événement peuvent être essentiels dans l'environnement des véhicules connectés. Qui plus est, les journaux stockés par un système de détection des intrusions (IDS) concernant les anomalies et les signatures d'intrusion sont essentiels pour déterminer si l'événement est survenu en raison de cyberattaques.

7.2 Gestion des données d'un DSSAD

7.2.1 Durée d'enregistrement dans le contexte d'un DSSAD

La Figure 6 illustre entre un EDR et un DSSAD concernant la durée d'enregistrement des données. Le DSSAD enregistre toutes les interactions prédéfinies entre le système automatisé et le conducteur, tandis que l'EDR enregistre pendant une durée prédéterminée au moment où survient un événement déclencheur. Les données enregistrées dans l'EDR et le DSSAD sont dès lors utiles pour déterminer qui commandait le véhicule au moment de l'accident.

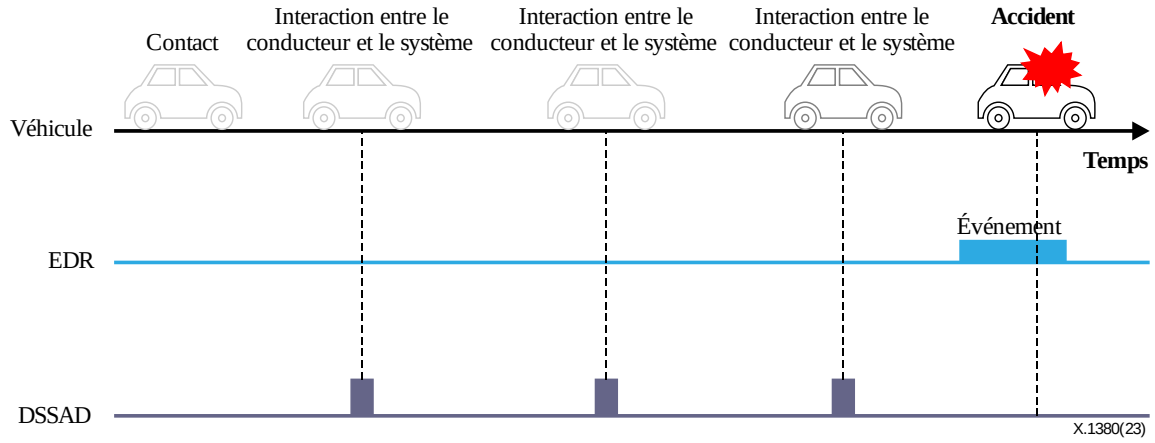

Figure 6 – Durée d'enregistrement des données dans le contexte d'un EDR et d'un DSSAD

Le DSSAD fondé sur le nuage devrait transmettre les données au système en nuage selon une politique prédéfinie. Lorsque la capacité de stockage du DSSAD du véhicule atteint sa limite, les données récentes peuvent écraser les données antérieures selon la procédure FIFO.

7.2.2 Verrouillage des données sur le dispositif de stockage du véhicule

Le processus de stockage DSSAD suit la procédure FIFO (premier arrivé, premier sorti) tout comme le processus de stockage EDR. Si le dispositif de stockage DSSAD est plein, les données nouvelles écrasent les plus anciennes. Néanmoins, la condition de déclenchement d'un événement prédéterminé de verrouillage des données dans le dispositif de stockage EDR impose que les données soient verrouillées sur le dispositif de stockage DSSAD après l'écriture des données, tout en empêchant l'écrasement de données stockées. Le format des données DSSAD verrouillées est déterminé par la politique du dispositif du stockage des données. Le format des données DSSAD verrouillées peut différer de celui des données DSSAD normales.

Après le verrouillage, les données DSSAD verrouillées peuvent être transmises au système en nuage. La transmission des données DSSAD verrouillées peut être prioritaire sur d'autres transmissions de données comme les données DSSAD normales et les données EDR verrouillées. Après confirmation que la transmission est terminée, les données transmises peuvent être supprimées du support de stockage DSSAD du véhicule.

7.2.3 Format des données

Si l'EDR a pour objet d'enregistrer les données d'un événement, l'objectif du DSSAD est de déterminer à qui la responsabilité est imputable à un moment déterminé (en général, celui de l'accident).

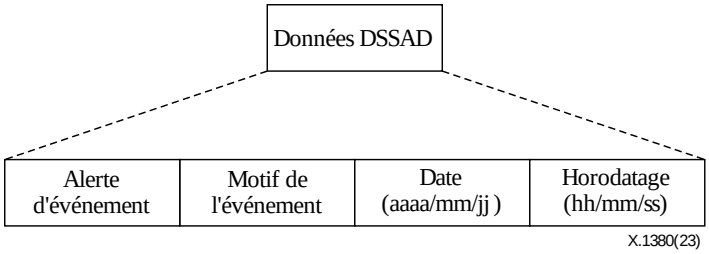

Figure 7 – Format des données DSSAD

Les données DSSAD comportent quatre champs, comme indiqué à la Figure 7 (voir la Recommandation ONU Nº 157 [b-UN R157]).

L'alerte d'événement est un champ qui indique le type d'interaction entre le conducteur et le système, à titre d'exemple les demandes de transition et les manœuvres d'urgence.

Le champ du motif de l'événement indique pourquoi l'alerte d'événement est survenue. Ce champ comporte le motif détaillé de la transition. Les motifs sont énumérés dans la partie 8.2 de la Recommandation ONU Nº 157 [b-UN R157].

Le champ de la date indique la date à laquelle l'alerte d'événement a été créée. Les données de ce champ se présentent sous la forme année/mois/jour.

Le champ horodatage renseigne sur l'heure à laquelle l'alerte d'événement a été produite. Les données de ce champ se présentent sous la forme "heure/minute/seconde et fuseau horaire". De par les caractéristiques du DSSAD, l'horodatage doit être très précis. Un seul horodatage peut être autorisé pour des données DSSAD multiples enregistrées simultanément dans la résolution temporelle de données DSSAD particulières. Si des événements multiples surviennent en l'espace d'une seconde, ces événements peuvent avoir le même horodatage. Dans ce cas, les données DSSAD devraient en indiquer la séquence temporelle.

7.3 Information d'identification du véhicule (VII)

Lorsque le système EDR/DSSAD transmet ses données à des systèmes en nuage, la VII doit être prise en considération pour identifier les données. La VII peut être un numéro de plaque d'immatriculation, un certificat de véhicule, un VIN, ou tout autre élément pouvant servir à l'identification du véhicule. La VII peut être considérée comme une information d'identification personnelle (PII).

S'agissant des environnements de véhicules du futur, il y a lieu de tenir compte des situations où plusieurs utilisateurs se partagent un véhicule unique, dans le cadre, par exemple, du covoiturage. Dans les cas où chaque utilisateur souhaite utiliser des systèmes EDR/DSSAD fondés sur le nuage pendant qu'il conduit, le véhicule partagé devrait être capable de distinguer entre chaque utilisateur pendant la conduite. Il est toutefois difficile d'identifier chaque utilisateur en l'absence de processus obligatoire pour qu'un véhicule recueille les données des utilisateurs (exemple: cartes d'identité des utilisateurs). Les informations relatives à l'utilisateur pourraient être obtenues à l'aide de systèmes personnalisés tels qu'une clé numérique sur smartphone utilisant un processus d'authentification faisant appel au certificat unique de l'utilisateur. Les informations relatives à l'utilisateur pourraient ainsi être recueillies et transmises avec la VII.

Comme on l'a vu au § 6.1, les données EDR sont recueillies lorsque le véhicule est exposé à des événements déclencheurs prédéterminés, tandis que les données DSSAD le sont à chaque interaction entre le véhicule et le conducteur. Dès lors que l'EDR et le DSSAD sont rattachés à un véhicule et que des données sont recueillies pour chaque véhicule, l'identification de chaque véhicule constitue une tâche essentielle pour tout système EDR/DSSAD fondé sur le nuage. La VII est donc constituée des éléments suivants:

– **Information sur le véhicule** (obligatoire): données d'identification d'un véhicule spécifique, à titre d'exemple le VIN.

– **Information sur l'utilisateur** (facultative): données d'identification de l'utilisateur ou du conducteur.

La Figure 8 indique le processus de transmission de l'EDR/du DSSAD du véhicule au nuage.

L'EDR/le DSSAD recueille les données provenant de chaque capteur et de l'ECU du réseau embarqué selon des règles prédéfinies, puis les transmet au dispositif de télécommunication. Celui-ci ajoute la VII aux données EDR/DSSAD recueillies et envoie le tout au système en nuage. Les données EDR/DSSAD et la VII reçues par l'interface en nuage sont transférées au coordonnateur de stockage, puis stockées conformément à la politique du système en nuage.

Les données EDR/DSSAD stockées dans le système en nuage ne peuvent être consultées que par des utilisateurs autorisés. Dès lors, les utilisateurs qui souhaitent obtenir des informations du système en nuage doivent envoyer des informations d'authentification pour prouver leur identité. Le système en nuage communique alors les données EDR/DSSAD aux utilisateurs authentifiés.

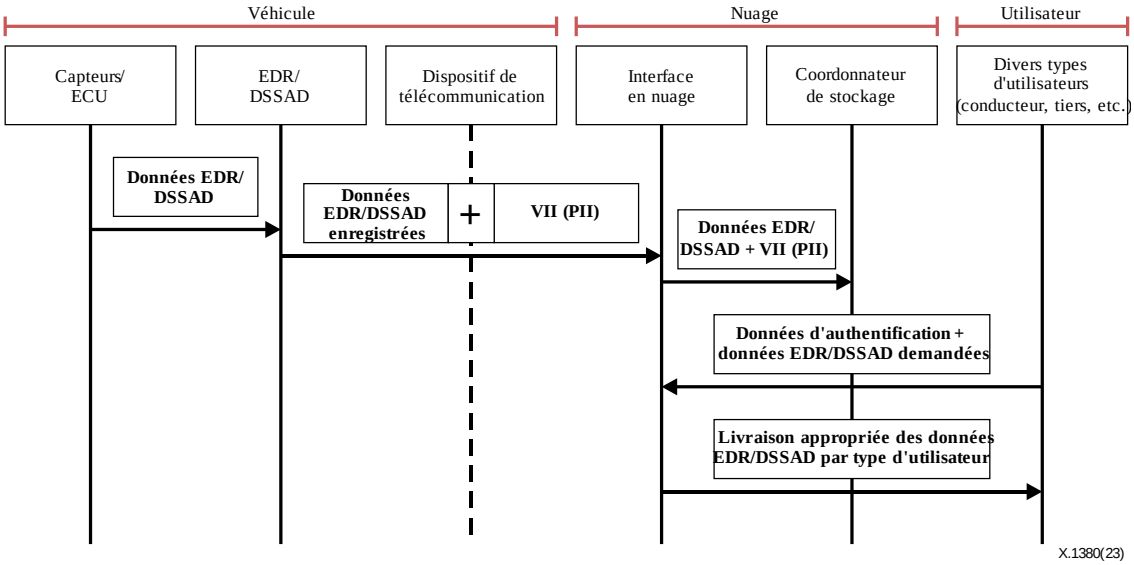

Figure 8 – Flux des données dans les EDR/DSSAD fondés sur le nuage

7.4 Systèmes en nuage pour EDR et DSSAD

7.4.1 Meilleure accessibilité des données enregistrées

L'EDR conventionnel comporte un point d'accès par le port OBD-II. Les données EDR ne peuvent être récupérées et exploitées qu'au moyen du port OBD-II et de l'outil de diagnostic du véhicule. C'est la raison pour laquelle les données EDR sont rarement utilisées par les propriétaires de véhicules, bien qu'ils détiennent la propriété des données.

Par ailleurs, l'EDR/DSSAD fondé sur le nuage permet aux utilisateurs une meilleure accessibilité aux données EDR/DSSAD en téléchargeant ces données dans des environnements en nuage. Les utilisateurs ou des tiers peuvent utiliser leurs données d'identification VII ou prédéterminées pour charger leurs données EDR/DSSAD en vue d'une utilisation ultérieure. Cette possibilité permet d'envisager une expansion évolutive des données EDR/DSSAD et de faire progresser la sécurité routière.

7.4.2 Actualisation des règles/politiques

Un système EDR/DSSAD fondé sur le nuage offre une fonction d'actualisation des règles/politiques. Les règles définissent les modalités de traitement des données dans un véhicule et les politiques définissent les modalités de traitement des données dans le nuage. Les règles sont constituées de la condition d'événement, du type de données à enregistrer, de la durée d'enregistrement des divers types de données et de la procédure de transmission des données au niveau du véhicule. Dans le contexte de l'EDR/DSSAD fondé sur le nuage, les politiques comprennent l'autorisation d'accès aux données accordée aux parties. Elles sont administrées par le coordonnateur de stockage au niveau des systèmes en nuage concernant le stockage des données EDR/DSSAD.

Les systèmes EDR/DSSAD fondés sur le nuage offrent une fonction d'actualisation des règles/politiques. En général, les services nationaux chargés de la réglementation définissent la série de données de route obligatoire et les conditions y relatives. Lorsque la réglementation est actualisée par les autorités, et sur demande valable de l'utilisateur ou du tiers autorisé, le système EDR/DSSAD fondé sur le nuage exécute les mises à jour des règles/politiques sur le véhicule et dans le nuage.

8 Analyse des menaces de sécurité

8.1 Biens protégés et objectifs de sécurité connexes

On entend par bien protégé tout objet de données, toute fonction ou toute ressource qu'il est nécessaire de protéger. En ce qui concerne les systèmes EDR/DSSAD fondés sur le nuage, on a répertorié les biens et les objectifs de sécurité connexes indiqués ci-après au Tableau 2.

Tableau 2 – Biens protégés et objectifs de sécurité connexes

Biens protégés	Description	Objectifs de sécurité connexes
Données EDR/DSSAD stockées dans le véhicule	Les données EDR/DSSAD recueillies au niveau du véhicule	Intégrité
Règles EDR/DSSAD stockées dans le véhicule	Les règles EDR/DSSAD susceptibles d'être actualisées par une politique du nuage	Intégrité
Micrologiciel EDR/DSSAD	Le micrologiciel du dispositif EDR/DSSAD	Intégrité
Paquet hertzien	Le paquet hertzien utilisé pour actualiser les règles EDR/DSSAD	Confidentialité, intégrité
Trafic de bus	Le trafic de bus transmis dans le réseau embarqué (IVN)	Confidentialité, intégrité
Journal EDR/DSSAD	Le journal d'audit du dispositif EDR/DSSAD	Intégrité, responsabilité
Communications avec les outils de débogage/diagnostic	Les communications entre le dispositif EDR/DSSAD et les outils de débogage ou de diagnostic.	Confidentialité, authenticité
Communications avec le serveur dorsal	Les communications entre le serveur dorsal et les véhicules ou les utilisateurs/tiers.	Confidentialité, authenticité, disponibilité
Politiques du nuage	Les politiques du nuage.	Intégrité
VII	Les données privées utilisées pour identifier les utilisateurs/véhicules.	Confidentialité

Tableau 2 – Biens protégés et objectifs de sécurité connexes

Biens protégés	Description	Objectifs de sécurité connexes
Journal du nuage	Les journaux d'audit des politiques du nuage, les demandes des utilisateurs/tiers et d'autres actes pouvant avoir une incidence sur la sécurité du nuage.	Intégrité, responsabilité
Données EDR/DSSAD stockées dans le nuage	Les données EDR/DSSAD reçues des véhicules.	Intégrité

8.2 Menaces de sécurité

Le présent paragraphe décrit les menaces de sécurité dans les systèmes d'enregistrement de données fondés sur le nuage. Les menaces générales identifiées dans les véhicules connectés sont décrites dans la Recommandation [UIT-T X.1371].

8.2.1 Menaces pour la confidentialité

Les données livrées aux systèmes d'enregistrement de données fondés sur le nuage constituent généralement des données privées des utilisateurs. La propriété des données et l'étendue de leur collecte peuvent varier selon la réglementation applicable au véhicule, mais les données du système d'enregistrement de données sont généralement réputées constituer des VII. Le non-respect de la confidentialité des données dans les systèmes d'enregistrement des données fondés sur le nuage peut être considéré comme une atteinte à la vie privée des utilisateurs. Ainsi, l'écoute illicite du réseau et le branchement clandestin sur le réseau peuvent faire partie des menaces habituelles pour la confidentialité.

– **Écoute illicite**: dans les réseaux hertziens que constituent les services fondés sur le nuage, une écoute des médias constitue une attaque potentielle dont la réalisation est aisée. L'auteur de l'attaque peut renifler des messages, y compris les VII, dans les systèmes d'enregistrement de données fondés sur le nuage, de deux façons. Il peut d'abord intervenir entre le véhicule et le serveur en nuage. En pareil cas, il peut y avoir divulgation des données de route provenant des véhicules et des données d'actualisation des règles/politiques provenant d'un serveur en nuage.

  En deuxième lieu, l'attaque peut intervenir entre l'utilisateur/le tiers et les systèmes en nuage. En pareil cas, il peut y avoir divulgation des données de route du système en nuage et des demandes d'actualisation des règles/politiques émanant de l'utilisateur/de tiers.

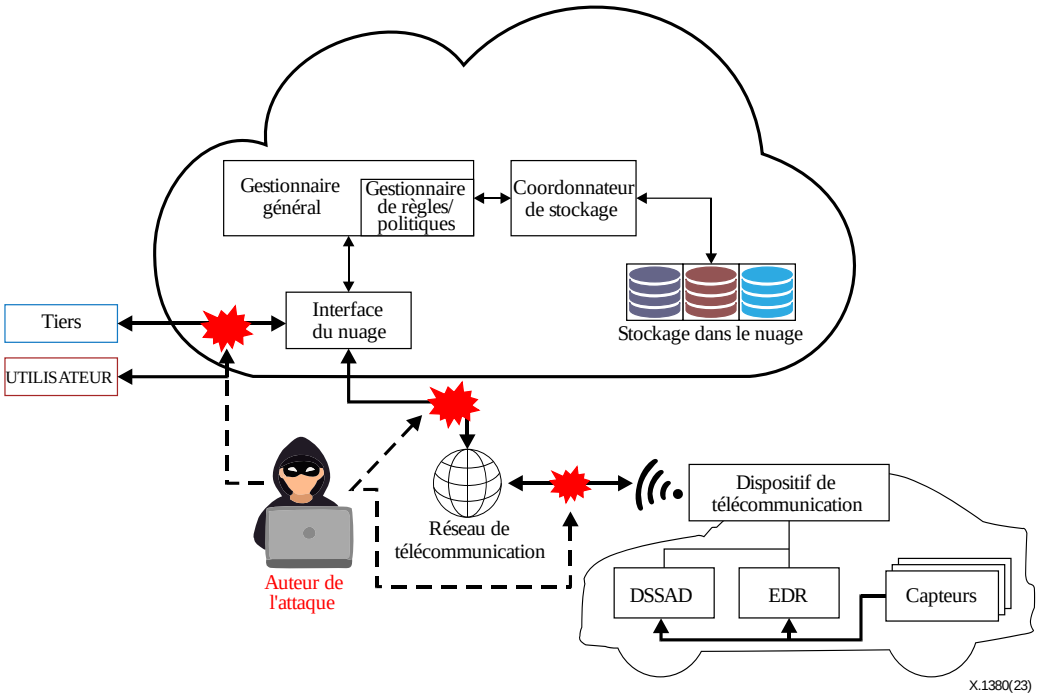

Figure 9 – Écoute illicite de systèmes d'enregistrement de données fondés sur le nuage

En troisième lieu, l'auteur d'une attaque peut intercepter et analyser le paquet hertzien transmis pour actualiser les règles EDR. À ce stade, il peut envoyer de fausses règles pour compromettre les mesures de sécurité.

– **Reniflage par branchement clandestin**: une attaque physique possible consiste à se brancher directement sur un réseau embarqué. Les véhicules modernes comportent plusieurs bus de gestionnaire de réseau de communication (CAN); l'accès à chaque bus est rigoureusement contrôlé par une passerelle de sécurité (ou un pare-feu embarqué). Il n'est pas possible de surveiller l'intégralité du trafic de tous les bus CAN si l'auteur de l'attaque n'obtient pas le privilège de la passerelle de sécurité. Ainsi, l'auteur de l'attaque peut tenter d'accéder physiquement au véhicule cible par branchement clandestin pour renifler l'ensemble du trafic des bus CAN, y compris les données EDR/DSSAD.

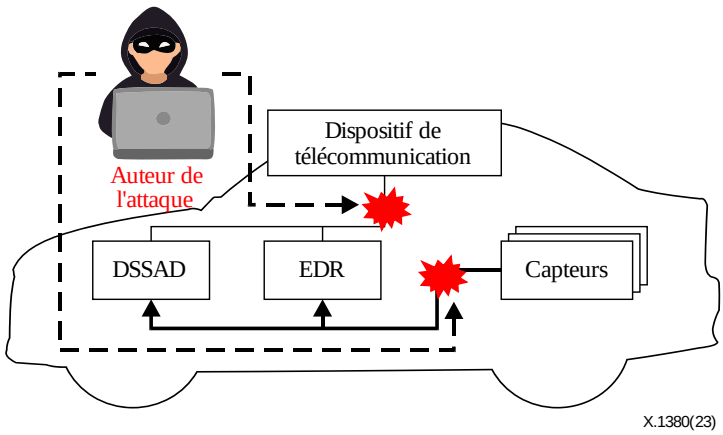

Figure 10 – Branchement clandestin sur un système d'enregistrement de données fondé sur le nuage

8.2.2 Menaces contre l'intégrité

Les données EDR sont utilisées pour analyser les collisions ou accidents de véhicule, et les données DSSAD pour déterminer à qui la responsabilité est imputable. Il doit donc être veillé à ce que les données ne soient pas altérées pendant leur stockage et leur transit. L'intégrité est un des objectifs de sécurité les plus importants de journaux d'audit comme les données EDR/DSSAD. Celui qui cherche à compromettre l'intégrité de ces données peut recourir aux méthodes indiquées ci-après.

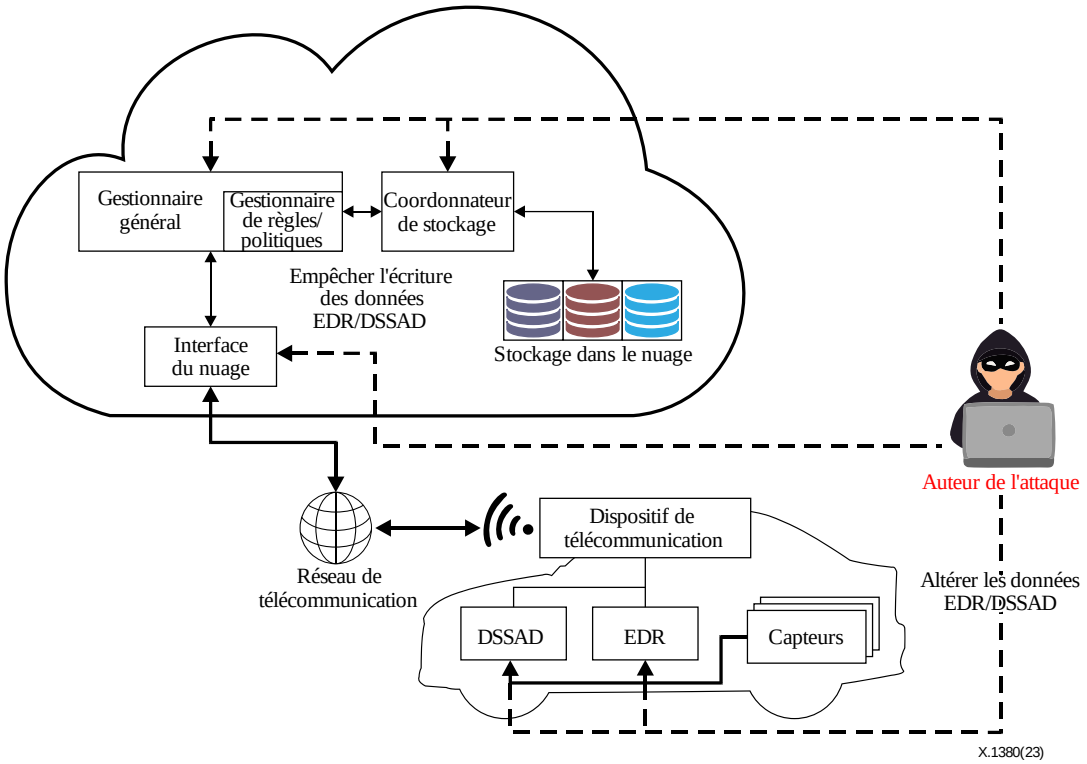

Figure 11 – Manipuler le flux de contrôle d'un système d'enregistrement de données fondé sur le nuage

En manipulant le flux de contrôle d'un système d'enregistrement de données fondé sur le nuage, l'auteur d'une attaque peut altérer des données EDR/DSSAD ou empêcher l'écriture de données EDR/DSSAD. Par exemple, l'auteur d'une attaque identifie l'interface de débogage de la carte à circuit imprimé (PCB) de l'EDR/DSSAD, parvient à y accéder et utilise l'interface pour manipuler le code exécuté. Il peut également manipuler le micrologiciel ou les règles EDR/DSSAD du système EDR/DSSAD. Il peut de même modifier le trafic du bus et manipuler le journal de l'EDR/DSSAD.

Pour ce qui est du système en nuage, l'auteur de l'attaque peut accéder au stockage et manipuler les données EDR, les journaux d'audit et la politique en nuage au moyen de logiciels malveillants et d'interfaces de programmation d'applications (API) non sûres.

La Figure 11 illustre l'attaque par manipulation du flux de contrôle du système d'enregistrement de données fondé sur le nuage.

8.2.3 Menaces pour l'authenticité

Les attaques par intercepteur, par usurpation d'identité et par répétition constituent des formes courantes de menaces pour l'authenticité.

– **Attaque par intercepteur**: dans un système d'enregistrement de données fondé sur le nuage, l'auteur d'une attaque peut intercepter les messages transmis entre un véhicule et le nuage ou entre le nuage et un utilisateur, et les retransmettre ensuite après les avoir arbitrairement

manipulés. L'expéditeur ne se rend pas compte que le destinataire, inconnu de lui, commet une attaque pour tenter d'accéder au message ou de modifier celui-ci avant de le retransmettre au véritable destinataire. L'auteur de l'attaque se rend ainsi maître de l'ensemble de la communication entre les parties.

– **Attaque par usurpation d'identité**: une attaque par usurpation d'identité peut être réalisée de quatre manières dans un système d'enregistrement de données fondé sur le nuage.

- Fausse demande de récupération de données EDR/DSSAD adressée au système en nuage.
- Fausse demande d'actualisation de règles adressée au système en nuage concernant un véhicule.
- Demande de stockage de fausses données EDR/DSSAD adressée au système en nuage.
- Fausse actualisation des règles du système EDR/DSSAD du véhicule.

Les attaques par usurpation d'identité peuvent porter gravement atteinte à l'intégrité générale du système d'enregistrement de données fondé sur le nuage, étant capables de générer de fausses données de route ou de modifier les règles/politiques d'événement. Ces attaques peuvent aussi divulguer des données privées stockées dans le système en nuage.

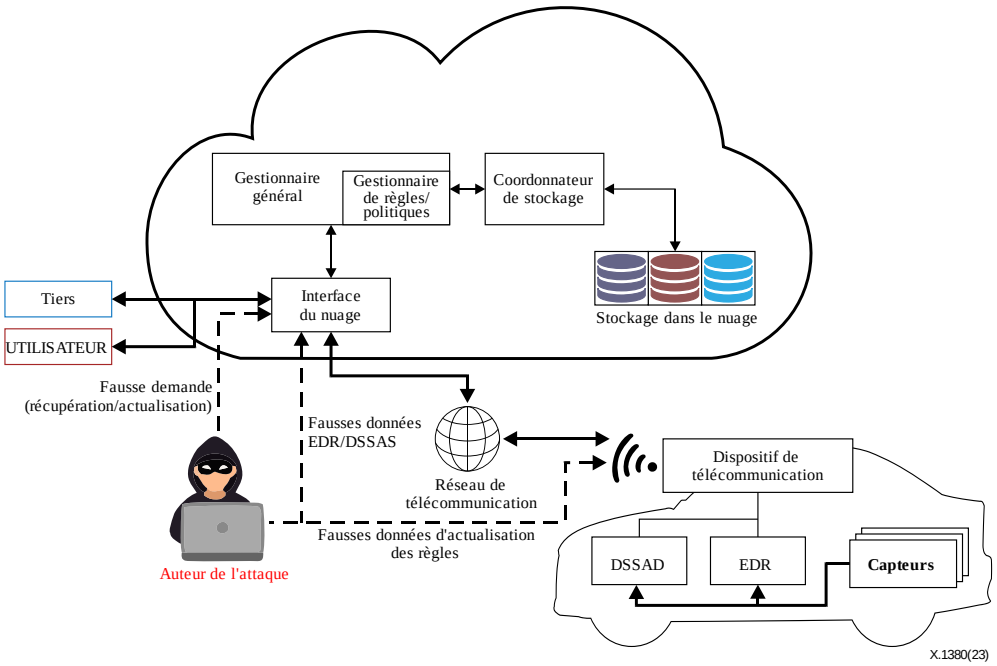

Figure 12 – Attaque par usurpation d'identité visant un système d'enregistrement de données fondé sur le nuage

– **Attaque par répétition**: la duplication de données EDR/DSSAD et le rétablissement non souhaité de règles/politiques antérieures font partie des conséquences possibles d'une attaque par répétition.

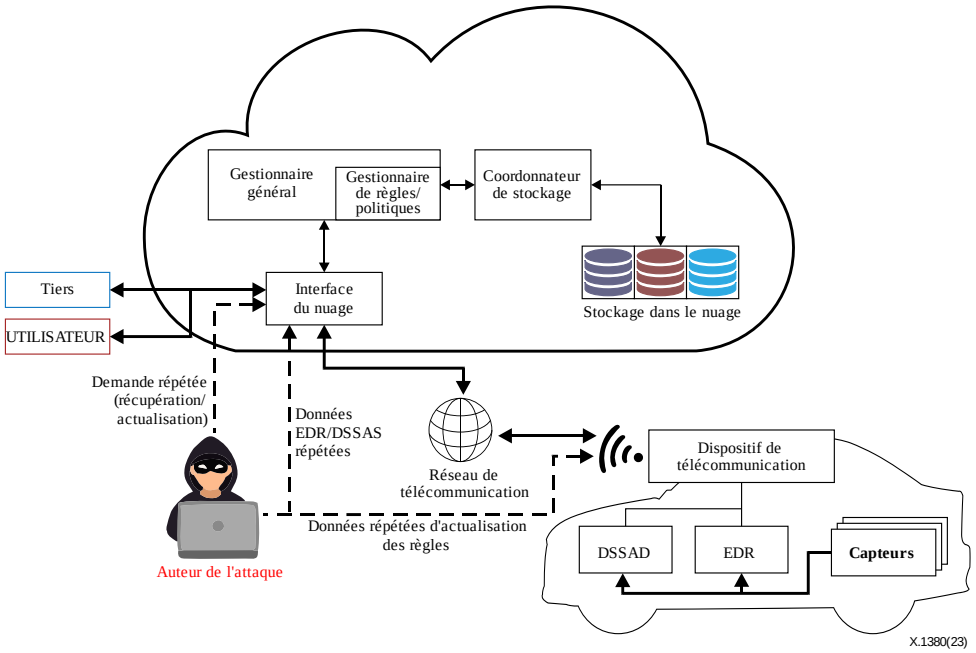

Figure 13 – Attaque par répétition visant un système d'enregistrement de données fondé sur le nuage

– **Accès physique**: si l'auteur de l'attaque peut accéder au véhicule via le port de débogage, une autre série d'attaques peut être exécutée. L'interface la plus courante de port de débogage est le groupe d'action de test mixte (JTAG). L'accès via JTAG permet de lire et écrire dans la mémoire, ce qui permet de manipuler le micrologiciel et de compromettre les mesures de sécurité.

  Le diagnostic constitue un autre moyen d'accès physique au véhicule. L'auteur d'une attaque peut accéder au port OBD-II au moyen d'outils de diagnostic ou directement à une passerelle dotée de fonctions de diagnostic à distance. Les services de diagnostic unifiés (SDU) sont un protocole standard de diagnostic permettant d'observer et de manipuler le réseau embarqué et les calculateurs du véhicule.

8.2.4 Menaces pour la disponibilité

La disponibilité est déterminante pour tout système d'enregistrement de données fondé sur le nuage car des informations utiles peuvent devoir être stockées à tout moment sur les accidents ou collisions. L'attaque par déni de service (DoS) est la plus connue des menaces pour la disponibilité.

– **Attaque DoS**: les attaques DoS peuvent avoir de graves conséquences pour les systèmes d'enregistrement de données fondé sur le nuage car leurs auteurs tentent de bloquer les principaux moyens de communication, de stockage ou de gestion des données EDR/DSSAD, ce qui retire toute utilité au système d'enregistrement de données fondé sur le nuage pour ce qui est de l'analyse des accidents. Ainsi, lors d'une attaque DoS, l'inondation du canal du réseau au moyen d'un fort volume de messages produits par l'auteur de l'attaque peut paralyser les nœuds du réseau voire la totalité des systèmes en nuage. Les nœuds du réseau (au niveau du véhicule ou du système en nuage) ne parviendront pas à traiter l'immense quantité de données reçues, ce qui provoquera un dysfonctionnement du stockage des données EDR/DSSAD au niveau du système en nuage ou de l'actualisation des règles/politiques sur le véhicule ou dans le nuage.

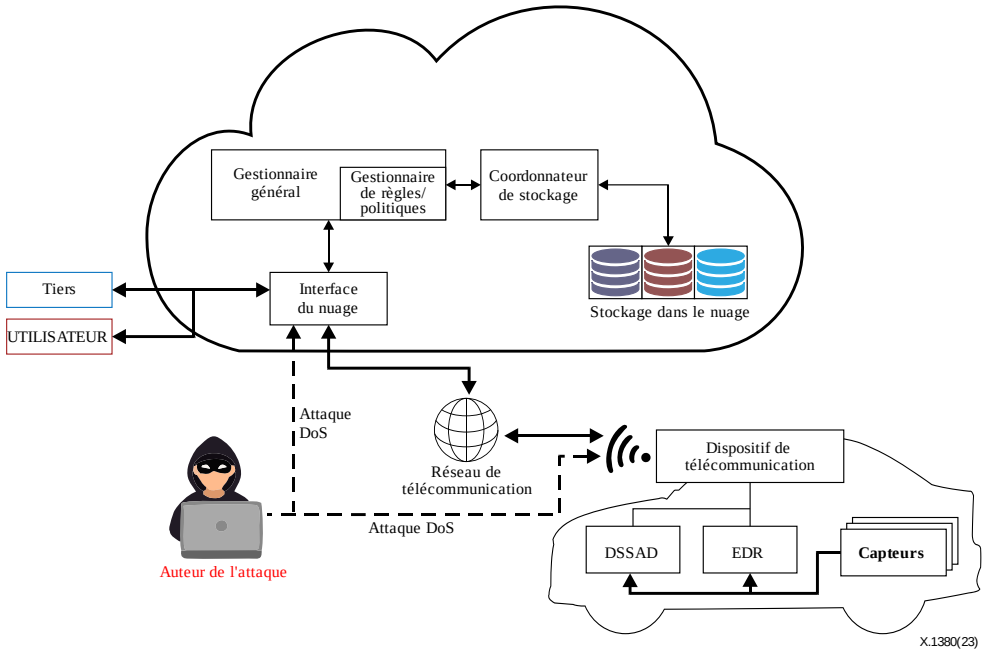

Figure 14 – Attaque DoS visant un système d'enregistrement de données fondé sur le nuage

8.2.5 Menaces pour la responsabilité

– **Perte de la traçabilité des événements**: des composantes du système en nuage comme le gestionnaire de règles/politiques et le coordonnateur de stockage fonctionnent d'après la série de règles/politiques installée par l'utilisateur autorisé. La gestion du journal des changements de règles/politiques est dont particulièrement importante du point de vue de la responsabilité. L'auteur d'une attaque peut créer la confusion en altérant ou en supprimant le journal des événements.

9 Exigences de sécurité

9.1 Démarrage sécurisé

Il est recommandé de vérifier l'intégrité du micrologiciel stocké dans la mémoire du dispositif EDR/DSSAD avant ou pendant l'exécution. Il est aussi recommandé de vérifier l'intégrité des règles EDR/DSSAD et leur configuration ainsi que les données d'étalonnage.

Le processus de protection des micrologiciels et des règles est constitué de deux étapes. Dans un premier temps, au moment de l'installation du micrologiciel et des règles, leur authenticité est vérifiée avant leur écriture dans la mémoire interne, et ils sont ensuite configurés comme étant le micrologiciel et les règles en vigueur. Dans un deuxième temps, on vérifiera lors de chaque démarrage l'intégrité du micrologiciel et des règles en vigueur.

Il est recommandé d'utiliser pour le mécanisme de démarrage sécurisé des moyens cryptographiques symétriques ou asymétriques afin de vérifier l'intégrité du micrologiciel et des règles par rapport au niveau de sécurité approprié. Il est aussi recommandé que les dispositifs EDR et DSSAD utilisent une ancre de confiance matérielle, par exemple un module matériel de sécurité (HSM), pour stocker les clés cryptographiques en toute sécurité et accélérer le calcul des algorithmes cryptographiques.

9.2 Journal sécurisé

Il est impératif de garantir l'intégrité des données d'enregistrement à l'aide de méthodes cryptographiques sécurisées. Les données EDR/DSSAD constituant des éléments de preuve pour certaines situations, elles doivent être protégées contre les manipulations non autorisées.

Dans le cas du système en nuage, le gestionnaire général devrait établir un journal dans chacun des cas suivants:

– Tentatives d'authentification des utilisateurs/tiers.

– Mises à jour des politiques.

Il est recommandé de stocker les journaux de manière sécurisée. Des mesures cryptographiques, notamment un code d'authentification de message (MAC), peuvent être rattachées aux journaux et/ou stockées dans un dispositif sécurisé muni d'un contrôle d'accès approprié. La durée minimum de conservation des journaux devrait être définie selon la politique d'un prestataire de services en nuage ou la réglementation du pays considéré.

9.3 Communications sécurisées

Les systèmes d'enregistrement de données fondés sur le nuage disposent de plusieurs canaux de communication:

– Communication entre les systèmes en nuage et les véhicules.

– Communication entre les utilisateurs/tiers.

– Communication entre les ECU, les capteurs et les actionneurs dans les véhicules.

Il est recommandé de veiller à la confidentialité et à l'authenticité des messages échangés dans les communications entre le système en nuage et les véhicules ou les utilisateurs/tiers. La confidentialité et l'authenticité peuvent être réalisées au moyen de mesures cryptographiques comme la sécurité de la couche de transport (TLS).

Il est aussi recommandé de garantir la disponibilité pour les communications entre le système en nuage et le véhicule. Dès lors, une très grande quantité de données EDR et DSSAD en provenance de nombreux véhicules doit être stockée comme il convient dans le dispositif de stockage en nuage.

Il est recommandé de veiller à l'intégrité des messages et données échangés dans les communications entre les ECU, les capteurs et les actionneurs des véhicules afin de produire des données EDR/DSSAD correctes, dans la mesure où les données provenant des ECU et des capteurs sont liées aux accidents ou aux activités de conduite.

9.4 Accès sécurisé

Il est recommandé de désactiver des interfaces de débogage du dispositif EDR/DSSAD comme le JTAG qui ne sont pas indispensables au service normal, et ces interfaces ne devraient pas contourner le démarrage sécurisé. Les méthodes de désactivation des interfaces de débogage sont classées comme suit:

– Suppression permanente.

– Désactivation sous condition en appliquant un contrôle d'accès.

Lorsque les interfaces de débogage sont réactivées pour l'analyse du retour de garantie, elles ne devraient être accessibles que par des parties autorisées et authentifiées. Il est recommandé de limiter les privilèges des applications recevant des données sur les interfaces matérielles et logicielles conformément au principe du moindre privilège.

Il est recommandé de protéger les fonctions et les données critiques pour la sécurité en rapport avec les commandes et les demandes de diagnostic au moyen d'un mécanisme cryptographique. Cela implique que tout sujet demandant à accéder au dispositif EDR/DSSAD soit authentifié avant de pouvoir envoyer des commandes.

9.5 Mises à jour sécurisées

Il est recommandé que la procédure de mise à jour des microprogrammes et des règles garantisse l'authenticité et l'intégrité: seuls pourront être exécutés les paquets de mise à jour authentifiés et non modifiés. En outre, il est recommandé de ne pas faire revenir le micrologiciel et les règles à une version antérieure pour empêcher toute utilisation malveillante de failles de sécurité antérieures. Il est aussi recommandé que les paquets hertziens soient transmis par un canal sécurisé protégé par des méthodes cryptographiques.

9.6 Liens entre les menaces répertoriées et les exigences de sécurité

Le Tableau 3 ci-dessous indique la correspondance entre les menaces répertoriées au paragraphe 8 et les exigences de sécurité.

Tableau 3 – Liens entre les menaces répertoriées et les exigences de sécurité

Exigences de sécurité	Menaces	Objectifs de sécurité
Démarrage sécurisé	Manipulation du flux de contrôle: – manipulation du micrologiciel; – manipulation des règles EDR/DSSAD.	Intégrité des règles EDR/DSSAD stockées dans les véhicules. Intégrité du micrologiciel de l'EDR/DSSAD.
Journal sécurisé	Manipulation du flux de contrôle: – manipulation des journaux. Perte de la traçabilité des événements.	Intégrité des données EDR/DSSAD au niveau des véhicules. Intégrité du journal dans le nuage.
Communications sécurisées	Écoute illicite. Reniflage par branchement clandestin. Manipulation du flux de contrôle. Attaque par intercepteur. Attaque par usurpation d'identité. Attaque par répétition. Attaque par déni de service.	Confidentialité et/ou intégrité du trafic du bus. Confidentialité et authenticité des communications avec les systèmes dorsaux. Disponibilité des systèmes dorsaux.
Accès sécurisé	Accès physique.	Confidentialité et/ou authenticité des communications avec les outils de débogage/diagnostic.
Mises à jour sécurisées	Écoute illicite. Manipulation du flux de contrôle: – manipulation des règles EDR/DSSAD. Attaque par usurpation d'identité.	Confidentialité et intégrité du paquet hertzien

10 Principes généraux de mise en œuvre pour les systèmes d'enregistrement de données fondés sur le nuage

Une protection stricte des données est indispensable à l'utilisation et à la gestion des données EDR/DSSAD dans tout système d'enregistrement de données fondé sur le nuage. Ces systèmes sont également utiles à la recherche-développement de véhicules plus sûrs du fait que des données enregistrées non accessibles pas un enregistreur de données conventionnel y sont utilisées. La présente section énonce les principes généraux de mise en œuvre d'un système d'enregistrement de données fondé sur le nuage.

10.1 Séparation du stockage dans le nuage

En raison du caractère essentiel de la VII dans tout système EDR/DSSAD fondé sur le nuage, il est impératif de protéger ces éléments de manière sécurisée. Une séparation physique des données EDR/DSSAD et de la VII y relative est indispensable dans les systèmes EDR/DSSAD fondés sur le nuage. Elle n'apporte pas seulement des avantages sur le plan de la sécurité, mais aussi des fonctions supplémentaires comme la communication de données EDR/DSSAD de tiers sans risque d'atteinte à la confidentialité. Le stockage doit être physiquement séparé et géré séparément dans des unités de stockage indépendantes. Le stockage de la VII (appelé base de données VII dans la Figure 15) demande un niveau de sécurité plus élevé que les autres catégories de données du fait de son importance relative.

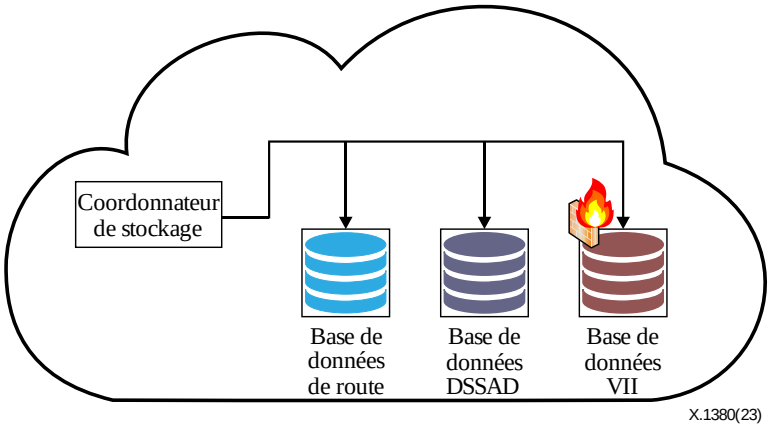

Figure 15 – Séparation du stockage

10.1.1 Procédure de stockage des données

Pour garantir la confidentialité et l'authenticité des données de communication avec un serveur dorsal, un canal sécurisé devrait être établi au préalable, avant tout envoi de données EDR/DSSAD d'un véhicule au système en nuage.

Lorsque des données sont livrées au coordonnateur de stockage depuis un véhicule via une interface en nuage, le coordonnateur de stockage sépare les données EDR/DSSAD et la VII. Après la séparation, il génère les données de liaison pour corréler les données EDR/DSSAD et la VII. Ensuite, les deux séries de données sont stockées dans des dispositifs de stockage différents (bases de données). Comme on l'indique à la Figure 16, la VII et les EDR/DSSAD corrélées par les données de liaison sont stockées dans la base de données VII et la base de données événements/DSSAD comme il convient. À l'issue de la procédure de stockage, son résultat (succès ou échec) devrait être consigné dans le journal.

Un des aspects les plus importants des procédures de stockage des données est la conformité à la réglementation utile, notamment au règlement général sur la protection des données (GDPR). Il est donc recommandé d'avoir obtenu le consentement du propriétaire des données avant de collecter toute donnée du véhicule.

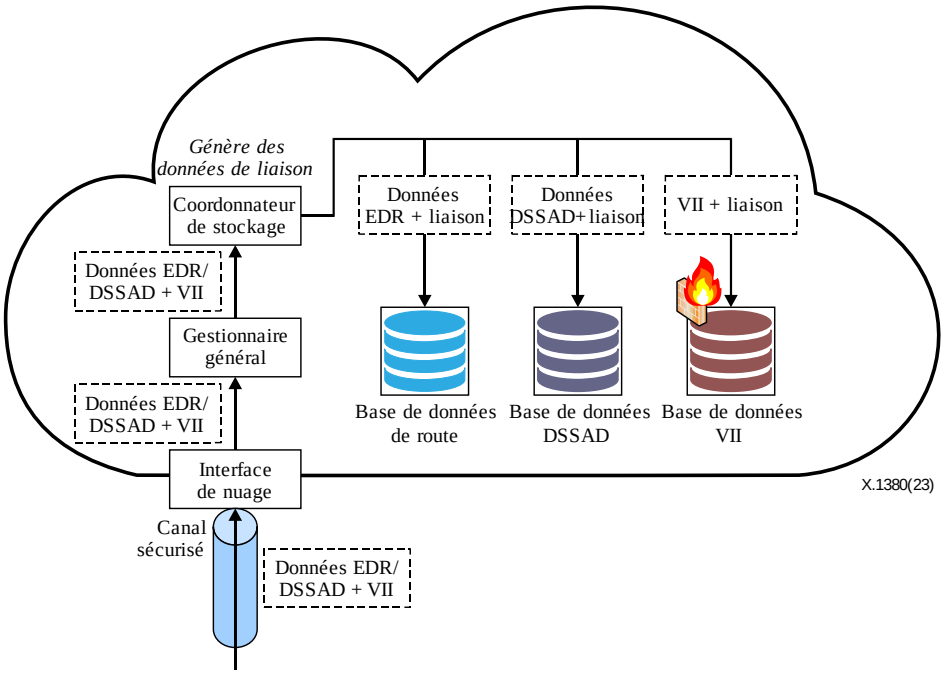

Figure 16 – Procédure de stockage de la séparation de stockage

10.1.2 Procédure de récupération des données

La procédure de récupération des données EDR/DSSAD débute par la demande de récupération des données EDR/DSSAD de l'utilisateur/du tiers. Quand l'utilisateur/le tiers accède au système en nuage, l'interface du nuage doit authentifier l'utilisateur/le tiers et consigner toutes les tentatives dans le journal. Si l'authentification réussit, le coordonnateur de stockage utilise la VII présentée pour trouver les données de liaison dans la base de données VII (voir Figure 17 a)). À l'aide des données de liaison ainsi trouvées, le coordonnateur de stockage recherche les données EDR/DSSAD. Une fois les données EDR/DSSAD trouvées, le coordonnateur de stockage communique celles-ci au demandeur, selon la procédure de contrôle d'accès du gestionnaire général, qui est différenciée en fonction du niveau d'autorisation du demandeur. La récupération de données VII est autorisée moyennant certaines restrictions et le niveau d'autorisation requis est plus élevé. En revanche, les données EDR/DSSAD expurgées de la VII peuvent être récupérées par le tiers. Les données EDR/DSSAD peuvent être récupérées sans appliquer le processus de recherche VII lorsque les données VII sont supprimées et transférées sur un serveur neutre séparé (voir la Figure 17 b)).

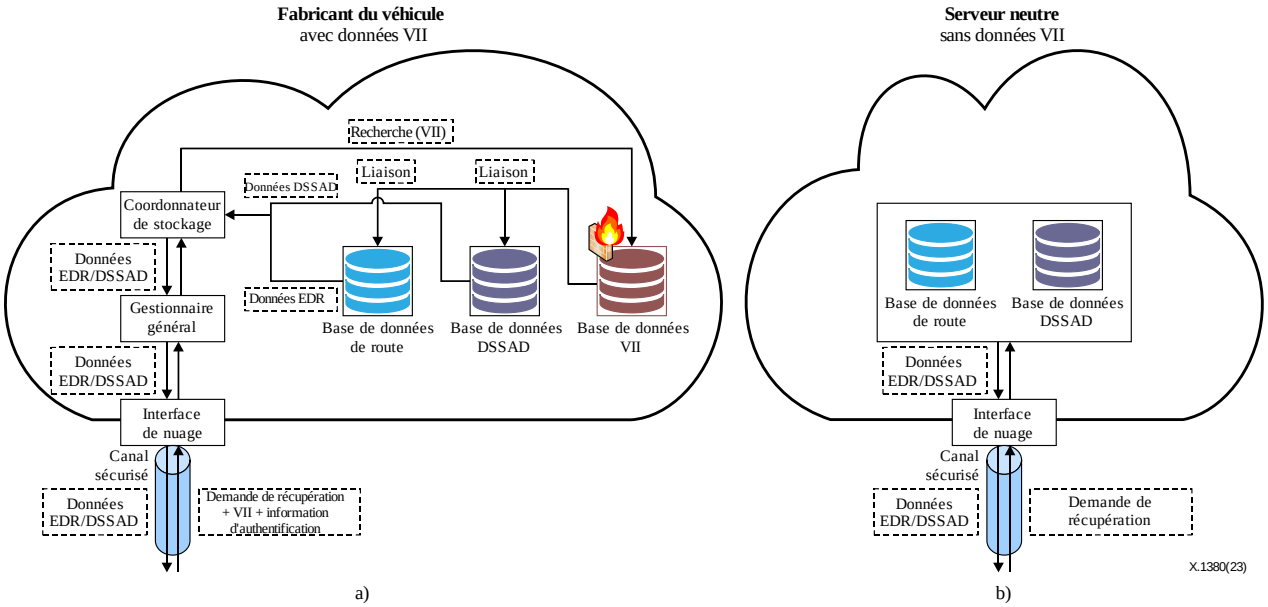

Figure 17 – Procédure de récupération de la séparation de stockage

10.1.3 Procédure de suppression des données

Le système en nuage de l'EDT/DSSAD doit obtenir le consentement de l'utilisateur, y compris la date d'expiration ou la durée des données enregistrées dans le cas des données VII collectées. Lorsque la date d'expiration ou la durée spécifiée des données enregistrées arrive à échéance, les données collectées devraient être supprimées automatiquement du système en nuage.

Lorsque les utilisateurs demandent la suppression de leurs données avant la date d'expiration, les systèmes en nuage doivent supprimer les données conformément à la demande. Lorsqu'un utilisateur sollicite la suppression, l'interface du nuage doit authentifier l'utilisateur et consigner toutes les tentatives dans le journal. Si l'authentification réussit, le coordonnateur de stockage doit utiliser la VII présentée pour trouver les données de liaison stockées dans la base de données VII. Une fois ces données trouvées, le coordonnateur de stockage doit rechercher les données EDR/DSSAD et supprimer celles-ci une fois trouvées. Le coordonnateur de stockage doit ensuite stocker le journal où est consigné le résultat de la suppression et communiquer le résultat à l'auteur de la demande.

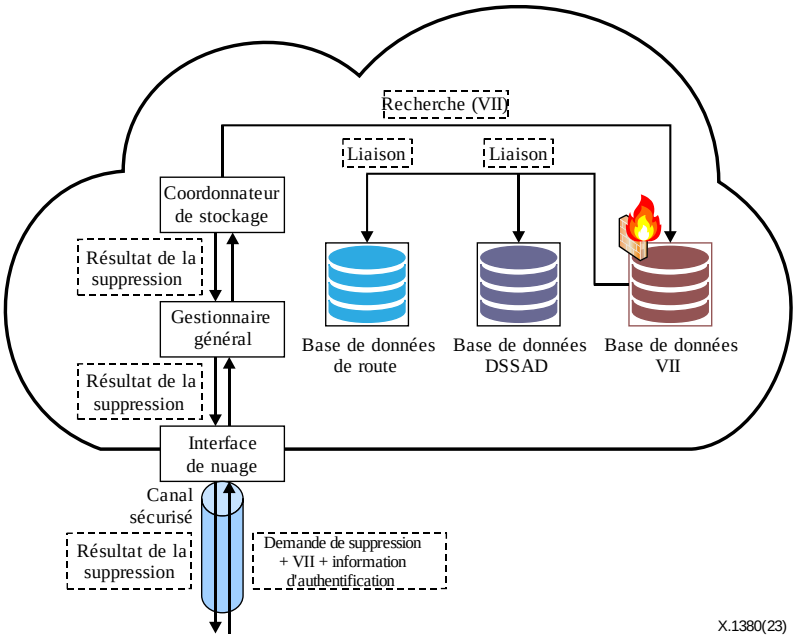

Figure 18 – Procédure de suppression de la séparation de stockage

10.2 Enregistrement auprès du service en nuage

La Figure 19 indique la procédure d'enregistrement des dispositifs d'enregistrement de données fondés sur le nuage dans les environnements automobiles.

En l'espèce, si une demande d'authentification en vue de l'enregistrement auprès d'un service d'enregistrement de données fondé sur le nuage, c'est-à-dire une demande authentification d'un véhicule, est envoyée par un véhicule en mode exécution de service (étape 1), l'identité du véhicule devrait être vérifiée à l'aide, par exemple, de l'algorithme de signature numérique d'un système de chiffrement de clé publique (étape 2). Dans ce cas précis, la demande d'authentification du véhicule peut être faite moyennant la transmission, au système du service d'enregistrement de données fondé sur le nuage, d'un message signé avec une clé privée du véhicule. À l'issue de la vérification effectuée lors de l'étape 2, s'il est établi que l'identité du véhicule n'est pas valide, le système du service d'enregistrement de données fondé sur le nuage génère une réponse d'échec de l'authentification qu'il transmet au véhicule (étape 3).

À l'issue de la vérification effectuée lors de l'étape 2, s'il est établi que l'identité du véhicule est valide, le système du service d'enregistrement de données fondé sur le nuage génère une réponse d'authentification pour le véhicule et la lui transmet (étape 4).

Lorsque la réponse d'authentification est reçue, c'est-à-dire une fois l'authentification du véhicule menée à bien, après qu'un usager a fourni et sélectionné les informations d'enregistrement pour le service d'enregistrement de données fondé sur le nuage, notamment les types de données d'enregistrement et la période considérée, etc., le véhicule transmet les informations d'enregistrement correspondantes au système du service d'enregistrement de données fondé sur le nuage afin de demander l'enregistrement auprès dudit service (étape 5).

Ensuite, si une demande d'enregistrement auprès du service d'enregistrement de données fondé sur le nuage, qui comprend les informations d'enregistrement pour ledit service, est soumise par le véhicule, le système du service d'enregistrement de données fondé sur le nuage crée, sur la base des informations d'enregistrement, une politique de sécurité utilisant des informations d'enregistrement du service telles que les types de données d'enregistrement et la période d'enregistrement, etc., puis stocke/enregistre les informations (étape 6).

Après cela, le système service d'enregistrement de données fondé sur le nuage attribue un pseudonyme à chaque véhicule (étape 7), génère un message de demande de certificat afin de demander la création d'un certificat de pseudonyme pour le pseudonyme attribué à chaque véhicule, et transmet le message au centre d'authentification (étape 8).

Le système du service d'enregistrement de données fondé sur le nuage vérifie si le certificat de pseudonyme est obtenu ou non auprès du centre d'authentification (étape 9). À l'issue de cette opération, si le certificat de pseudonyme est obtenu, le système du service d'enregistrement de données fondé sur le nuage stocke le certificat dans la base de données des informations. Le certificat de pseudonyme pourra être un message portant la signature numérique du centre d'authentification. Il est possible de garantir la justification du pseudonyme grâce au certificat de pseudonyme.

Plusieurs pseudonymes peuvent être attribués à chaque véhicule. Étant donné que le pseudonyme ne contient pas d'informations associées à l'identité de chaque véhicule, il est possible de protéger les informations PII de chaque véhicule.

Si la notification est reçue, le système du service d'enregistrement de données fondé sur le nuage génère les informations d'enregistrement auprès du service pour chaque véhicule, les stocke dans la base de données correspondante et les transmet à chaque véhicule (étape 10). En l'espèce, les informations d'enregistrement au service d'enregistrement de données fondé sur le nuage peuvent comprendre un pseudonyme attribué à chaque véhicule, un certificat de pseudonyme pour le pseudonyme, etc. Chaque véhicule, c'est-à-dire chaque utilisateur du véhicule, pour lequel le service d'enregistrement de données fondé sur le nuage est enregistré, peut réaliser des enregistrements de

données fondés sur le nuage en communiquant avec le centre en nuage et les autres véhicules et en utilisant pour ce faire les informations d'enregistrement au service d'enregistrement de données fondé sur le nuage fournies par ledit service.

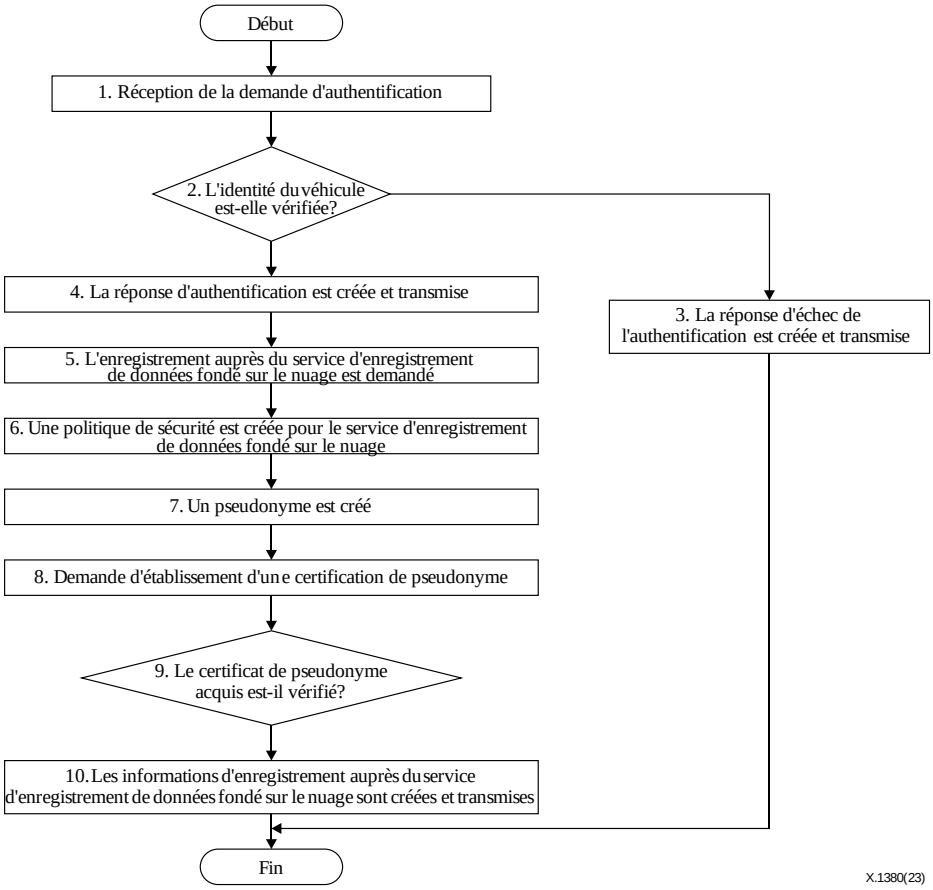

Figure 19 – Enregistrement auprès d'un service d'enregistrement de données fondé sur le nuage

La procédure de désenregistrement d'un service d'enregistrement de données fondé sur le nuage peut être envisagée pour des cas d'utilisation comme la location de véhicules, les véhicules d'occasion, etc., où le nouveau propriétaire ou conducteur du véhicule ne souhaite pas communiquer de données EDR/DSSAD au système en nuage.

11 Cas d'utilisation des enregistreurs de données fondés sur le nuage dans les environnements automobiles

Lorsqu'un accident se produit, les données EDR/DSSAD peuvent être mises à profit pour en analyser la cause et déterminer si le véhicule et le conducteur sont responsables. La Figure 20 illustre le flux des données EDR/DSSAD. Les données EDR/DSSAD générées dans le véhicule sont transmises au nuage par communication hertzienne. Un propriétaire de véhicule, un fabricant, des fournisseurs ou des tiers autorisés (par exemple, compagnies d'assurance) peuvent utiliser les données EDR/DSSAD du nuage.

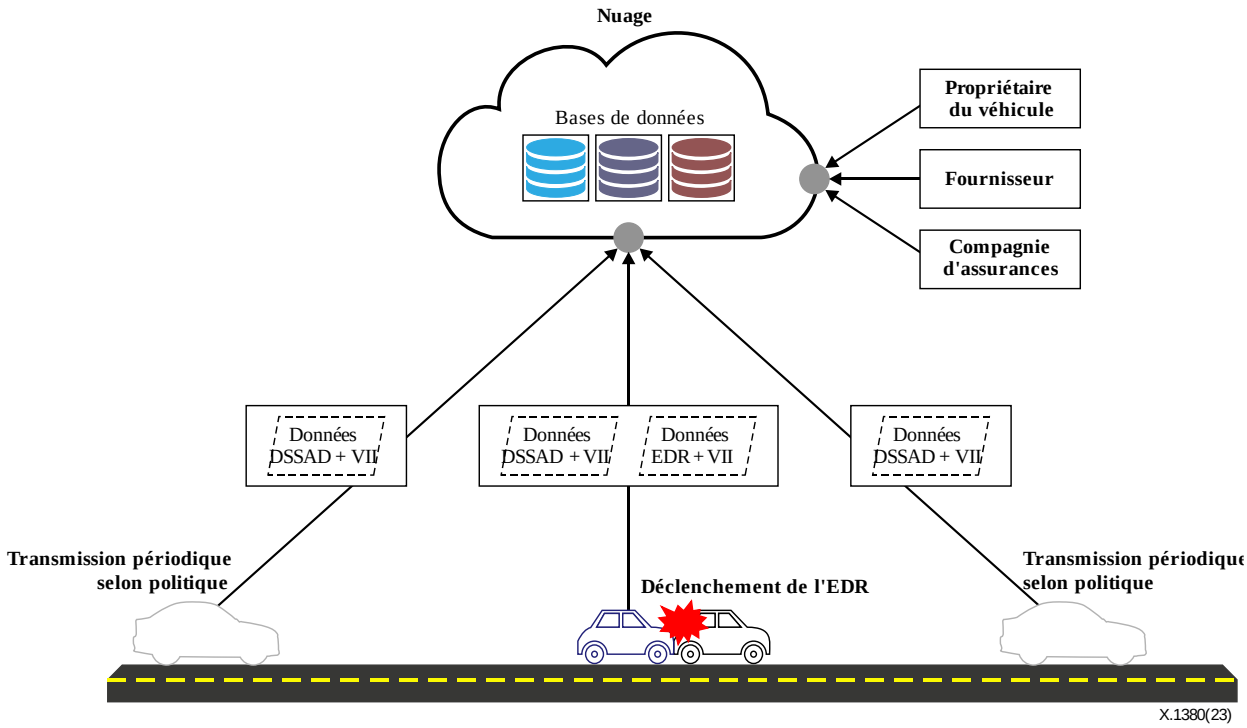

Figure 20 – Le flux des données EDR/DSSAD

Un système d'enregistrement de données fondé sur le nuage présente de nombreux avantages. D'une part, les données EDR/DSSAD sont aisées à obtenir, même en situation de risque potentiel (incendie du véhicule, inondation de véhicule, etc.). D'autre part, les analystes autorisés des accidents peuvent acquérir plus facilement les données auprès du système en nuage que des ECU des véhicules directement.

11.1 Cas 1: Collision entre véhicules

La Figure 21 illustre un scénario dans l'ordre chronologique lorsqu'un véhicule équipé d'un système automatique de maintien dans la voie (ALKS) circule sur la route. L'accident se produit en e) et un événement EDR est déclenché. Le nuage stocke les données EDR/DSSAD de a), au moment où l'ALKS est activé, à e), lorsque l'accident survient. Les données EDR/DSSAD stockées livrent les informations suivantes:

L'ALKS étant activé par le conducteur à 10:19:10, le système assume le contrôle du véhicule. Après 1 minute 50 secondes, la météo se dégrade et l'ALKS adresse une demande de transition au conducteur du véhicule, mais le conducteur ne réagit pas. L'ALKS engage alors automatiquement une manœuvre à risque minimal (MRM) à 10:22:00. L'accident se produit à 10:22:30.

Par l'analyse des données EDR/DSSAD, il est possible de vérifier la période et les circonstances de l'accident. Les systèmes d'enregistrement de données basés fondés sur le nuage stockent les données EDR/DSSAD dans le dispositif de stockage du système en nuage selon une politique de transfert de données prédéfinie. La collecte d'informations sur l'accident est donc facilitée par rapport à la récupération directe des données EDR sur le véhicule.

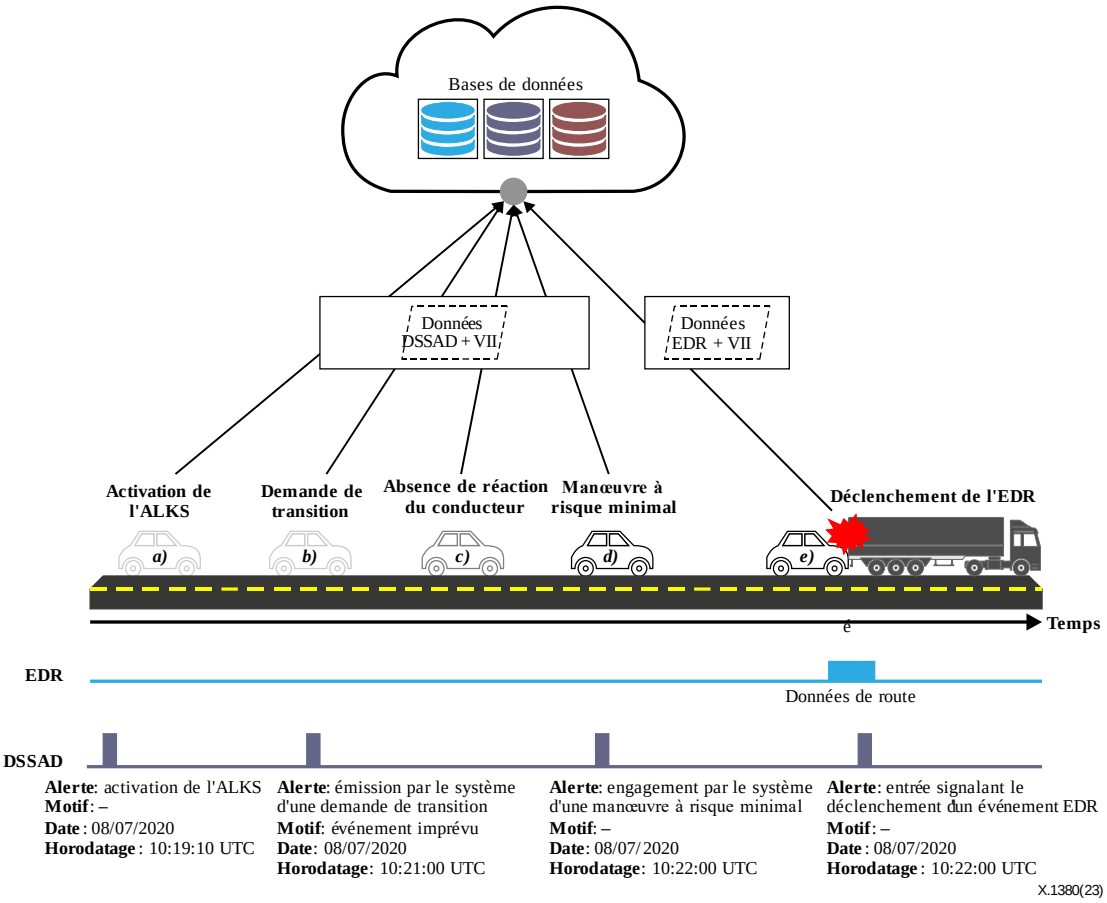

Figure 21 – Collision entre véhicules

11.2 Cas 2: Collision entre un véhicule et une bicyclette

La Figure 22 illustre dans l'ordre chronologique un scénario dans lequel un véhicule équipé d'un ALKS circule sur la route. Le véhicule entre en collision avec un faible impact avec une bicyclette au point c), mais vu la faiblesse relative de l'impact, l'EDR n'est pas déclenché. Cependant, toutes les données DSSAD récentes sont transférées sur le nuage. Les données EDR/DSSAD stockées livrent les informations suivantes:

> L'ALKS est activé par le conducteur à 07:10:00. Après 15 secondes, le conducteur actionne directement la commande de direction et l'ALKS est alors désactivé. La collision entre le véhicule et la bicyclette survient à 07:10:16.

Dans le cas d'espèce, l'impact sur le véhicule est si faible que la condition de déclenchement de l'EDR n'est pas remplie, et aucune donnée EDR n'est recueillie. Néanmoins, la situation de l'accident peut être simulée et analysée facilement en détail car les données DSSAD ont été stockées dans le système en nuage.

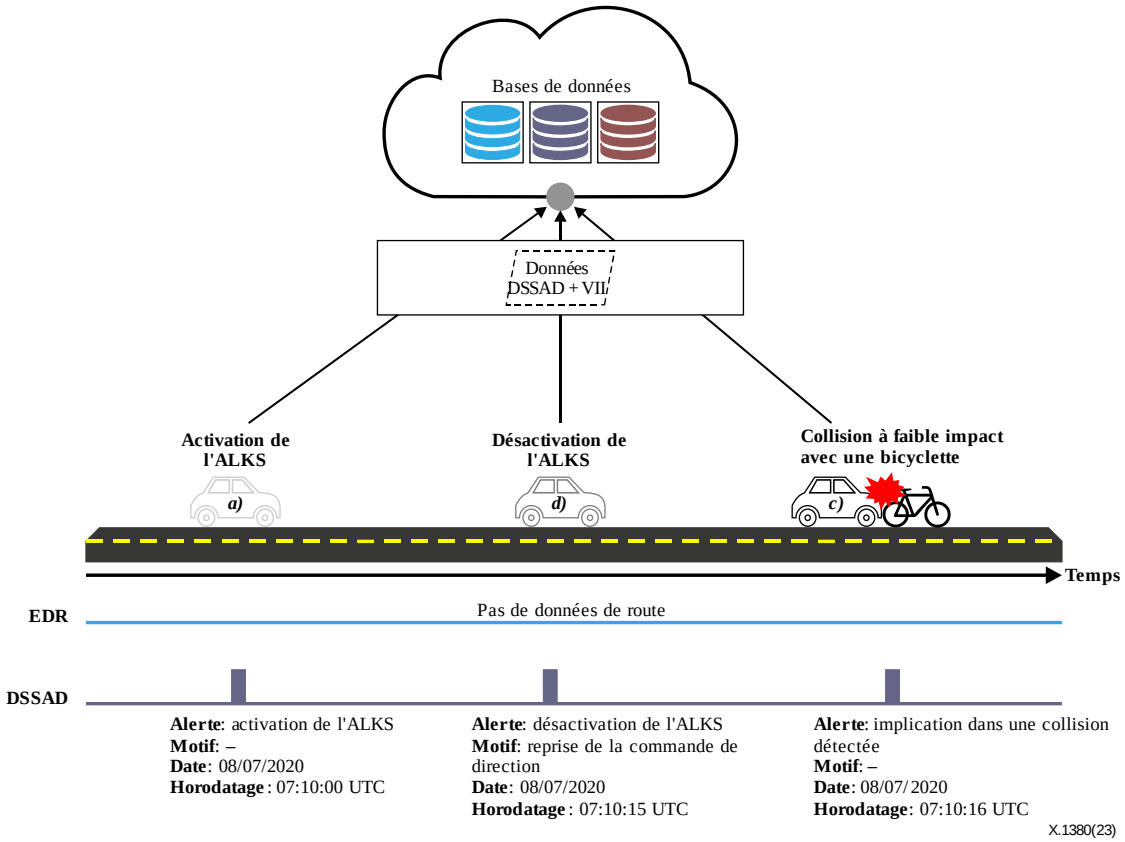

Figure 22 – Collision entre un véhicule et une bicyclette

Appendice I

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

Exemple de série de données EDR conventionnelle

L'exemple de série de données présenté ici indique les éléments de données essentiels requis pour les enregistreurs de données électroniques conventionnels aux États-Unis d'Amérique, l'organisme de réglementation compétent étant l'Administration nationale de la sécurité routière (NHTSA).

Tableau I.1 – Éléments de données essentiels requis pour les EDR conventionnels [b-NHTSA EDR]

Rubrique	Éléments de données	Durée de l'enregistrement	Taux d'échantillonnage	Plage	Précision	Résolution
1	Delta-v longitudinal	De 0 à 250 ms, ou de 0 à la fin de l'événement plus 30 ms si cette période est plus courte	100/s	De –100 à +100 km/h	±10%	1 km/h
2	Delta-v maximal longitudinal	De 0 à 300 ms, ou de 0 à la fin de l'événement plus 30 ms si cette période est plus courte	s.o.	De –100 à +100 km/h	±10%	1 km/h
3	Temps, delta-v maximal longitudinal	De 0 à 300 ms, ou de 0 à la fin de l'événement plus 30 ms si cette période est plus courte	s.o.	De 0 à 300 ms, ou de 0 à la fin de l'événement plus 30 ms si cette période est plus courte	±3 ms	2,5 ms
4	Vitesse indiquée par le véhicule	De –5,0 à 0 s	2/s	De 0 à 200 km/h	±1 km/h	1 km/h
5	Position de l'accélérateur ou de la pédale d'accélérateur (en % du maximum)	De –5,0 à 0 s	2/s	De 0 à 100%	±5%	1%
6	État du frein de service	De –5,0 à 0 s	2/s	Actif/inactif	s.o.	Actif/inactif
7	Cycle d'allumage (accident)	–1,0 s	s.o.	De 0 à 60 000	±1 cycle	1 cycle
8	Cycle d'allumage (téléchargement)	Au moment du téléchargement	s.o.	De 0 à 60 000	±1 cycle	1 cycle
9	État de la ceinture de sécurité (conducteur)	–1,0 s	s.o.	Actif/inactif	s.o.	Actif/inactif
10	État du témoin d'avertissement du coussin gonflable	–1,0 s	s.o.	Actif/inactif	s.o.	Actif/inactif

Tableau I.1 – Éléments de données essentiels requis pour les EDR conventionnels [b-NHTSA EDR]

Rubrique	Éléments de données	Durée de l'enregistrement	Taux d'échantillonnage	Plage	Précision	Résolution
11	Délai de déploiement du coussin gonflable frontal, conducteur (première étape, dans le cas de systèmes de coussins gonflables à déploiement progressif)	Événement	s.o.	De 0 à 250 ms	±2 ms	1 ms
12	Délai de déploiement du coussin gonflable frontal, passager avant droit (première étape, dans le cas de systèmes de coussins gonflables à déploiement progressif)	Événement	s.o.	De 0 à 250 ms	±2 ms	1 ms
13	Événement multiple, nombre d'événements (1 ou 2)	Événement	s.o.	1,2	s.o.	1,2
14	Délai entre les événements 1 et 2	Si nécessaire	s.o.	De 0 à 5,0 s	0,1 s	0,1 s
15	Données enregistrées complètes	Après les autres données	s.o.	Oui/non	s.o.	Oui/non

Bibliographie

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

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

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*.

[b-UN R157] Règlement ONU N° 157, *Prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne leur système automatisé de maintien dans la voie*.

[b-UN R160] Additif 159 – Règlement ONU N° 160, *Prescriptions uniformes relatives à l'homologation des véhicules à moteur en ce qui concerne l'enregistreur de données de route*.

[b-NHTSA EDR] NHTSA, *Final regulatory evaluation: Event data recorders (EDRs)*.

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	Équipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2023