التـوصيــة

ITU-T X.1380 (03/2023)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تطبيقات وخدمات آمنة (2) – أمن أنظمة النقل الذكية (ITS)

مبادئ توجيهية أمنية بشأن مسجِّلات بيانات الأحداث القائمة على الحوسبة السحابية في بيئات السيارات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب (1)	X.1149–X.1140
أمن التطبيقات (1)	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1309–X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1319–X.1310
أمن شبكة الكهرباء الذكية	X.1339–X.1330
البريد المعتمد	X.1349–X.1340
أمن إنترنت الأشياء (IoT)	X.1369–X.1350
أمن أنظمة النقل الذكية (ITS)	**X.1399–X.1370**
أمن سجل الحسابات الموزع	X.1429–X.1400
أمن التطبيقات (2)	X.1459–X.1450
أمن الويب (2)	X.1489–X.1470
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
الدفاع السيبراني	X.1599–X.1590
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680
الاتصالات الكمومية	
المصطلحات	X.1701–X.1700
مولِّد الأعداد العشوائية الكمومية	X.1709–X.1702
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1711–X.1710
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1719–X.1712
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1729–X.1720
أمن البيانات	
أمن البيانات الضخمة	X.1759–X.1750
حماية البيانات	X.1789–X.1770
أمن الاتصالات المتنقلة الدولية–2000	X.1819–X.1800

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1380

مبادئ توجيهية أمنية بشأن مسجِّلات بيانات الأحداث القائمة على الحوسبة السحابية في بيئات السيارات

ملخص

مسجلات بيانات الأحداث (EDR) هي واحدة من أهم المكونات التي جُهّزت بها مركبات الطرق الخاصة بالسيارات لتسجيل حالة المركبات وتحركاتها ومدخلات المستعمل أثناء حالات الاصطدام. ومن خلال تحليل بيانات الأحداث، يمكن فهم سبب الاصطدام واستعماله في نهاية المطاف لتحسين السلامة في بيئات السيارات. كما يُعتبر توافر نظام لتخزين البيانات في القيادة الآلية عنصراً هاماً لتسجيل البيانات من شأنه أن يوفّر صورة واضحة عن التفاعلات بين السائق ونظام القيادة الآلية. بيد أن المسجلات التقليدية لبيانات الأحداث تسجّل وتدير جميع البيانات محلياً، وقد يؤدي ذلك إلى احتمال ضياع البيانات أو تدميرها.

وتُعتبر الحوسبة السحابية مصدراً للتمكّن من النفاذ الشبكي إلى مجموعة قابلة للزيادة ومرنة من الموارد المادية أو الافتراضية التي يمكن تقاسمها والتزود بها وإدارتها حسب الطلب على أساس الخدمة الذاتية. وتحاول بالفعل صناعات، مثل صناعة الطيران، تطبيق الخدمات السحابية على أنظمة تسجيل بيانات الأحداث لزيادة السلامة في بيئة الطيران. ووفقاً للاتجاه الحالي للتوصيلية بين المركبات، ستُستخدم مسجلات بيانات الأحداث وأنظمة تخزين البيانات في القيادة الآلية لزيادة سلامتها بشكل عام. ولكن لديها مواطن ضعف متعددة في عملية جمع ونقل وتخزين وإدارة واستخدام البيانات المسجلة، بحسب الخصائص التي تتميز بها بيئة المركبة. ولذلك، لا بد من دراسة مواطن الضعف هذه ومتطلبات الأمن وحالات الاستعمال فيما يتعلق بمسجلات البيانات القائمة على الحوسبة السحابية في بيئات السيارات.

وتقدم التوصية ITU-T X.1380 المبادئ التوجيهية الأمنية لمسجلات البيانات القائمة على الحوسبة السحابية في بيئات السيارات. وتصف التهديدات ومواطن الضعف ومتطلبات الأمن وحالات الاستعمال فيما يتعلق بمسجلات البيانات القائمة على الحوسبة السحابية في بيئات السيارات.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1380	2023-03-03	17	11.1002/1000/15106

مصطلحات أساسية

الحوسبة السحابية، نظام تخزين البيانات للقيادة الآلية (DSSAD) القائم على الحوسبة السحابية، مسجل بيانات الأحداث (EDR) القائم على الحوسبة السحابية، مسجلات البيانات، نظام تخزين البيانات للقيادة الآلية (DSSAD)، مسجل بيانات الأحداث (EDR)، متطلبات الأمن، التهديدات الأمنية.

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة الأمم المتحدة المتخصصة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع/حقوق تأليف ونشر برمجيات يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

1 مجال التطبيق 1
2 المراجع 1
3 التعاريف 1
1.3 المصطلحات المعرَّفة في وثائق أخرى 1
2.3 المصطلحات المعرفة في هذه التوصية 2
4 الاختصارات والأسماء المختصرة 2
5 الاصطلاحات 3
6 أنظمة مسجل البيانات القائم على الحوسبة السحابية 3
1.6 نظام مسجل بيانات الأحداث القائم على الحوسبة السحابية 3
2.6 نظام تخزين البيانات القائم على الحوسبة السحابية للقيادة الآلية 6
3.6 مقارنة بين المسجّل EDR والنظام DSSAD 7
7 تصميم نظام مسجل البيانات القائم على الحوسبة السحابية 7
1.7 إدارة البيانات في مسجل بيانات الأحداث 7
2.7 إدارة بيانات النظام DSSAD 10
3.7 المعلومات المحددة لهوية المركبة (VII) 11
4.7 الأنظمة السحابية للمسجل EDR والنظام DSSAD 12
8 تحليل التهديدات الأمنية 13
1.8 الأصول الأمنية والأهداف الأمنية ذات الصلة 13
2.8 التهديدات الأمنية 13
9 متطلبات الأمن 19
1.9 بدء التشغيل الآمن 19
2.9 السجل الآمن 20
3.9 الاتصالات الآمنة 20
4.9 النفاذ الآمن 20
5.9 التحديث الآمن 21
6.9 العلاقة بين التهديدات المحدَّدة ومتطلبات الأمن 21
10 المبادئ التوجيهية لتنفيذ أنظمة مسجلات البيانات القائمة على الحوسبة السحابية 21
1.10 فصل أماكن التخزين السحابي 21
2.10 تسجيل الخدمات السحابية 25
11 حالات استعمال مسجلات البيانات القائمة على الحوسبة السحابية في بيئة السيارات 27
1.11 الحالة 1: حادث اصطدام بين مركبتين 27
2.11 الحالة 2: حادث اصطدام بين مركبة ودراجة 28
التذييل I 30
بيبليوغرافيا 31

مبادئ توجيهية أمنية بشأن مسجِّلات بيانات الأحداث القائمة على الحوسبة السحابية في بيئات السيارات

1 مجال التطبيق

تقدم هذه التوصية المبادئ التوجيهية الأمنية لمسجلات البيانات القائمة على الحوسبة السحابية، من قبيل مسجل بيانات الأحداث (EDR) ونظام تخزين البيانات للقيادة الآلية (DSSAD) في بيئات السيارات. وتتضمن هذه التوصية الاعتبارات التقنية المتعلقة بأنظمة تسجيل البيانات، وهي مسجل بيانات الأحداث (EDR) ونظام تخزين البيانات للقيادة الآلية (DSSAD). وبالإضافة إلى ذلك، يقدم أيضاً مشروع التوصية هذا متطلبات الأمن وحالات الاستعمال.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع للمراجعة، يشجَّع مستعملو هذه التوصية على بحث إمكانية تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية.

والإشارة إلى وثيقة في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.1371] التوصية ITU-T X.1371 (2020)، *التهديدات الأمنية التي تتعرض لها المركبات الموصولة*.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 الاستيقان (authentication) [b-ITU-T X.1252]: عملية تحقق رسمية تؤدي، في حال نجاحها، إلى هوية مستيقَّنة لكيان.

2.1.3 النظام الآلي للبقاء في ممر السير (automated lane keeping system) [b-UN R157]: نظام يشغله السائق ويُبقي المركبة داخل ممر سيرها.

3.1.3 الترخيص (authorization) [b-ITU-T X.800]: منح الحقوق، الذي يتضمن إتاحة النفاذ استناداً إلى حقوق النفاذ.

4.1.3 التيسّر (availability) [b-ITU-T X.800]: خاصية إمكانية النفاذ وإمكانية الاستعمال بناءً على طلب من كيان مرخص له.

5.1.3 الاستيقانية (authenticity) [b-ITU-T X.641]: حماية من أجل الاستيقان المتبادل واستيقان أصل البيانات.

6.1.3 المساءلة (accountability) [b-ITU-T X.800]: خاصية تضمن أن أعمال كيان ما يمكن إسنادها إلى ذلك الكيان حصراً.

7.1.3 السرية (confidentiality) [b-ITU-T X.800]: خاصية عدم إتاحة المعلومات أو الكشف عنها لأشخاص غير مرخص لهم أو لكيانات أو عمليات غير مرخص لها.

8.1.3 نظام تخزين البيانات للقيادة الآلية (data storage system for automated driving) (DSSAD) [b-UN R157]: النظام الذي يمكّن من تحديد التفاعلات بين الأنظمة الآلية للبقاء في ممر السير (ALKS) والسائق البشري.

9.1.3 مسجل بيانات الأحداث (event data recorder) (EDR) [b-UN R160]: جهاز أو وظيفة في مركبة لتسجيل بيانات السلاسل الزمنية الدينامية للمركبة خلال الفترة الزمنية التي تسبق مباشرةً وقوع حدث ما (مثلاً سرعة المركبة مقابل الوقت)، أو خلال حادث اصطدام (مثلاً التغير في السرعة مقابل الزمن)، ويقصد منها استخراج هذه البيانات بعد حادث الاصطدام. ولأغراض هذا التعريف، لا تتضمن بيانات الأحداث بيانات سمعية وبصرية.

10.1.3 سلامة البيانات (data integrity) [b-ITU-T X.800]: خاصية بقاء البيانات على حالتها دون أن يطرأ عليها تغيير أو تلف بطريقة غير مرخص بها.

11.1.3 التهديد (threat) [b-ISO/IEC 27000]: سبب محتمل لحادث غير مرغوب فيه قد يُلحق ضرراً بنظام ما أو منظمة ما.

2.3 المصطلحات المعرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 سطح بيني سحابي (cloud interface): بوابة في نظام سحابي تشكل سطحاً بينياً للاتصالات بين نظام سحابي من جهة ومركبات ومستعملين وأطراف ثالثة من جهة أخرى.

2.2.3 المدير العام (general manager): مكوّن من مكوّنات النظام السحابي ينظم الإجراءات الأساسية لتخزين واستخراج بيانات مسجل بيانات الأحداث/نظام تخزين البيانات للقيادة الآلية (DSSAD) ويتحقق من المتطلبات الأساسية للطلب الوارد من مستعمل أو طرف ثالث أو مركبة.

3.2.3 مخدم محايد (neutral server): مخدم مستقل عن مصنعي المركبات يمكن أن يوفر معلومات مغفلة الهوية أو محدّدة لهوية المركبة أو بيانات مسجل بيانات الأحداث/نظام تخزين البيانات للقيادة الآلية (DSSAD) المحذوفة من المعلومات المحددة لهوية المركبة.

4.2.3 مدير قاعدة/سياسة عامة (rule/policy manager): مكوّن نظام سحابي يحدِّث القاعدة/السياسة العامة ويشكّل جزءاً من المدير العام.

5.2.3 منسق التخزين (storage coordinator): مكوّن نظام سحابي يفْصل بيانات مسجل بيانات الأحداث/نظام تخزين البيانات للقيادة الآلية (DSSAD) عن المعلومات المحدّدة لهوية المركبة، لتخزين البيانات واستخراجها في التخزين السحابي وفقاً لسياسة محددة مسبقاً.

4 الاختصارات والأسماء المختصرة

تستخدم هذه التوصية المختصرات التالية:

ALKS أنظمة الإبقاء في ممر السير *(Automated Lane Keeping Systems)*

API السطح البيني لبرمجة التطبيقات *(Application Programming Interface)*

CAN شبكة منطقة وحدة التحكم *(Controller Area Network)*

DoS رفض الخدمة *(Denial of Service)*

DSSAD نظام تخزين البيانات للقيادة الآلية *(Data Storage System for Automated Driving)*

ECU وحدة التحكم الإلكتروني *(Electronic Control Unit)*

EDR مسجل بيانات الأحداث *(Event Data Recorder)*

FIFO حسب ترتيب الدخول *(First-in-first-out)*

GDPR اللائحة العامة لحماية البيانات *(General Data Protection Regulation)*

IVN شبكة داخل المركبة *(In-Vehicle Network)*

JTAG فريق عمل الاختبار المشترك *(Joint Test Action Group)*

MAC شفرة استيقان الرسائل *(Message Authentication Code)*

MRM مناورة بأدنى حدّ من المخاطر *(Minimum Risk Manoeuvre)*

OBD التشخيص على متن المركبة *(On-Board Diagnostic)*

OTA عبر الأثير *(Over-the-air)*

PII المعلومات المحدِّدة لهوية الأشخاص *(Personally Identifiable Information)*

TLS أمن طبقة النقل *(Transport Layer Security)*

UDS خدمات التشخيص الموحدة *(Unified Diagnostic Services)*

V2X من مركبة إلى كل شيء *(Vehicle-to-everything)*

VII المعلومات المحدّدة لهوية المركبة *(Vehicle Identifiable Information)*

VIN الرقم المحدّد لهوية المركبة *(Vehicle Identification Number)*

5 الاصطلاحات

تستخدم هذه التوصية الاصطلاحين التاليين:

كلمات "**يلزم/يُتطلب/يتعين**" التي تدل على متطلب يجب التقيد به تماماً ولا يسمح بأي انحراف عنه في حال ادعاء الامتثال لهذه التوصية.

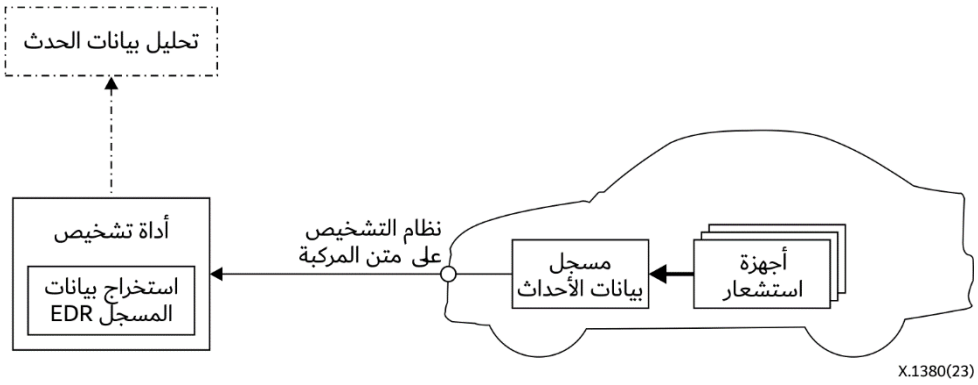
كلمة "**يُوصى**" التي تدلّ على متطلب يُوصى به لكنه غير إلزامي في المطلق. وبالتالي لا يتعين توفر هذا المتطلب لزعم الامتثال.

6 أنظمة مسجل البيانات القائم على الحوسبة السحابية

1.6 نظام مسجل بيانات الأحداث القائم على الحوسبة السحابية

نظام مسجّل بيانات الأحداث (EDR) القائم على الحوسبة السحابية هو نظام مسجل بيانات الأحداث الموصول بأنظمة سحابية (المخدم الخلفي) لزيادة إمكانية النفاذ وأمن بيانات EDR في بيئات المركبات الموصولة والذاتية القيادة.

وهو جهاز مثبت في معظم السيارات اليوم يسجّل المعلومات المتعلقة بحوادث الاصطدام أو حوادث السير التي تتعرض لها المركبات، لتحسين السلامة ونوعية الحياة في بيئة المركبات.

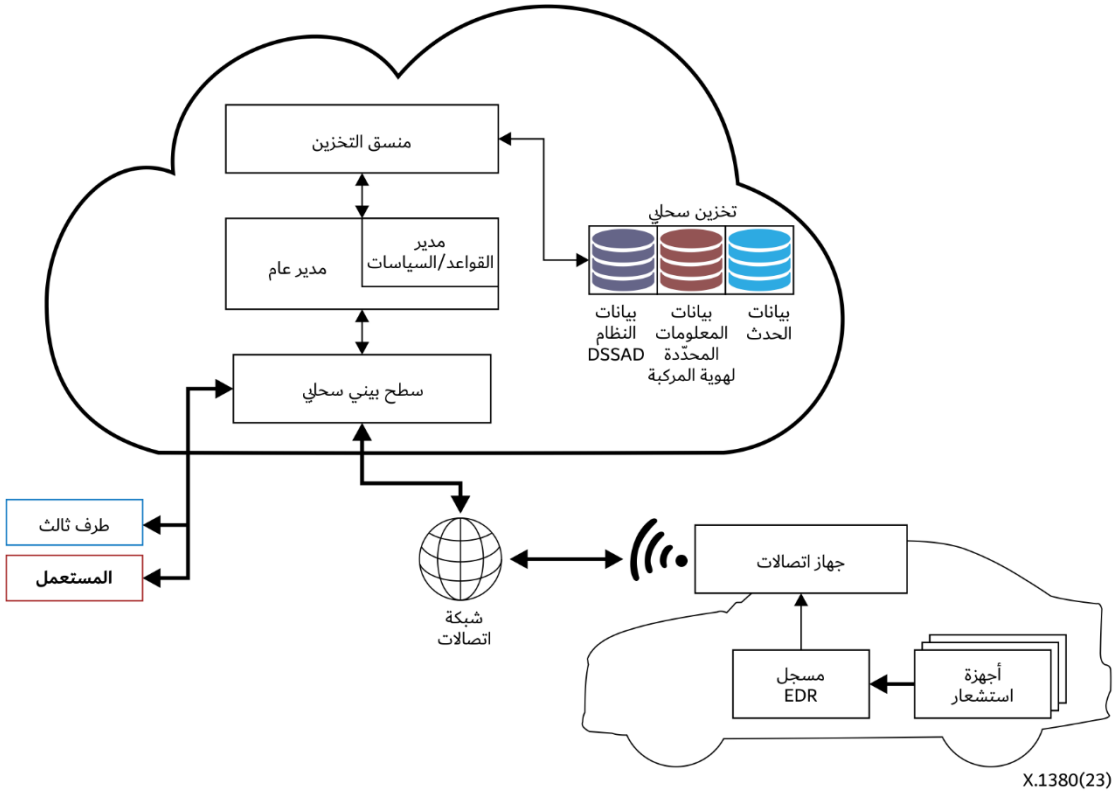


الشكل 1 – مسجل بيانات الأحداث التقليدي في السيارات

يبدأ تشغيل مسجل بيانات الأحداث التقليدي، على النحو المبين في الشكل 1، عندما يكون هناك حدث تواجه فيه حالة المركبة ظروفاً معينة، مثل نشر الوسادة الهوائية الأمامية، وتجاوز عتبة التسارع/التباطؤ، والانقلاب، وما إلى ذلك. وعندما يبدأ المسجل في العمل، يقوم بجمع مجموعة بيانات محددة سلفاً من أجهزة الاستشعار ثم يخزّن البيانات في مخزنه الداخلي باستخدام ذاكرة مستقرة. ويبدأ تسجيل البيانات عملياً قبل 5 ثوان (–5 ثوان) من لحظة بدء التشغيل (ويشار إليها عادة بالرمز T0) حتى 500 ملليثانية (+500 ملليثانية) من لحظة بدء التشغيل. وتختلف هاتان المدتان "–5 ثوان" و"+500 ملليثانية" باختلاف اللوائح الوطنية أو مصنعي المركبات.

وعموماً، يستطيع مسجّل بيانات الأحداث أن يخزّن أكثر من حدث يجري على متن المركبة. وعندما يمتلئ المخزن ببيانات أحداث سابقة، تُكتب فوق البيانات الأقدم بياناتٌ محدّثة جديدة. وفي الأحداث الخاصة مثل نشر الوسادة الهوائية، يخزّن المسجل التقليدي البيانات المجمعة ويقفل نظام تخزين البيانات لمنع التلاعب بها أو الكتابة فوقها.

وتستخرج أداة التشخيص أو أداة الاستخراج المعيَّنة البيانات المخزنة عبر منفذ نظام التشخيص على متن المركبة وتُستخدم لتحليل الاصطدام أو حادث السير. والحجم الأدنى لمجموعة البيانات المجمَّعة محدّد بموجب اللوائح الوطنية للمركبات أو تصميمات مصنعي المركبات. كما أن أنساق بيانات الأحداث المسجلة تختلف عادةً باختلاف مصنّع المركبة، وغالباً ما تختلف باختلاف طراز المركبة. ولذلك، عند استخراج بيانات الأحداث وتحليلها، يلزم استخدام برمجية استخراج متخصصة.



الشكل 2 – مسجّل بيانات الأحداث القائم على الحوسبة السحابية

يخزّن مسجل بيانات الأحداث (EDR) القائم على الحوسبة السحابية، الوارد وصفه في الشكل 2، بيانات الأحداث المتعلقة بالأنظمة السحابية من خلال جهاز اتصالات موصول بمسجّل بيانات الأحداث.

وقد تختلف مجموعة بيانات التسجيل عن مجموعات بيانات مسجل بيانات الأحداث التقليدي نظراً للاختلافات المنهجية والبيئية بين مسجل بيانات الأحداث التقليدي ومسجّل بيانات الأحداث القائم على الحوسبة السحابية. وكذلك، يمكن إضافة نوع جديد من البيانات المستمدة من وحدة التحكم الإلكتروني (ECU) التي تحكم القيادة الذاتية لأنها البيانات المهمة التي تساعد في تحليل حوادث المركبات ذاتية القيادة.

وخلافاً لمسجل بيانات الأحداث التقليدي، الذي يكتب بيانات الأحداث الجديدة فوق بيانات الأحداث غير المؤمنة، يمكن لمسجّل بيانات الأحداث القائم على الحوسبة السحابية أن يسجل بيانات الأحداث في التخزين السحابي دون الكتابة فوق البيانات. وبالتالي، يمكن أن يحتوي مسجل البيانات القائم على الحوسبة السحابية على بيانات للمركبة مسجَّلة بالكامل دون أي حذف. وهذه واحدة من أكبر الفوائد التي يتميّز بها مسجل بيانات الأحداث القائم على الحوسبة السحابية مما ساعد كثيراً البحوث المتعلقة بالسلامة على الطرق إذ تمكّنت من استعمال كامل البيانات التي تتيحها مسجلات بيانات الأحداث.

وينبغي أن تكون البيانات المجمعة والمخزنة في الخدمات السحابية باستخدام مسجلات بيانات الأحداث متاحة للمستعملين أو لأي طرف ثالث إذا طلب أي طرف بيانات هذه المسجلات متّبعاً الإجراءات الواجبة ومتحلياً بالترخيص اللازم. وعند تسليم البيانات المطلوبة من هذه المسجلات إلى الأطراف، ينبغي أن تجرى عملية استيقان للتحقق من صلاحية الطلب.

وبالإضافة إلى وظيفتي تخزين بيانات هذه المسجلات وتقديمها، يُجري أيضاً مسجل بيانات الأحداث القائم على الحوسبة السحابية تحديثات على قواعد/سياسات النظام. ويمكن لأي مستعمل أو طرف ثالث أن يطلب تحديث قواعد/سياسات مسجل بيانات الأحداث في المركبة، والسياسات ذات الصلة في نظام الحوسبة السحابية. وسيستلزم الطلب سلطةً أعلى وتحققاً أمنياً أشد مما تتطلبه أي عمليات تخزين واستخراج عادية.

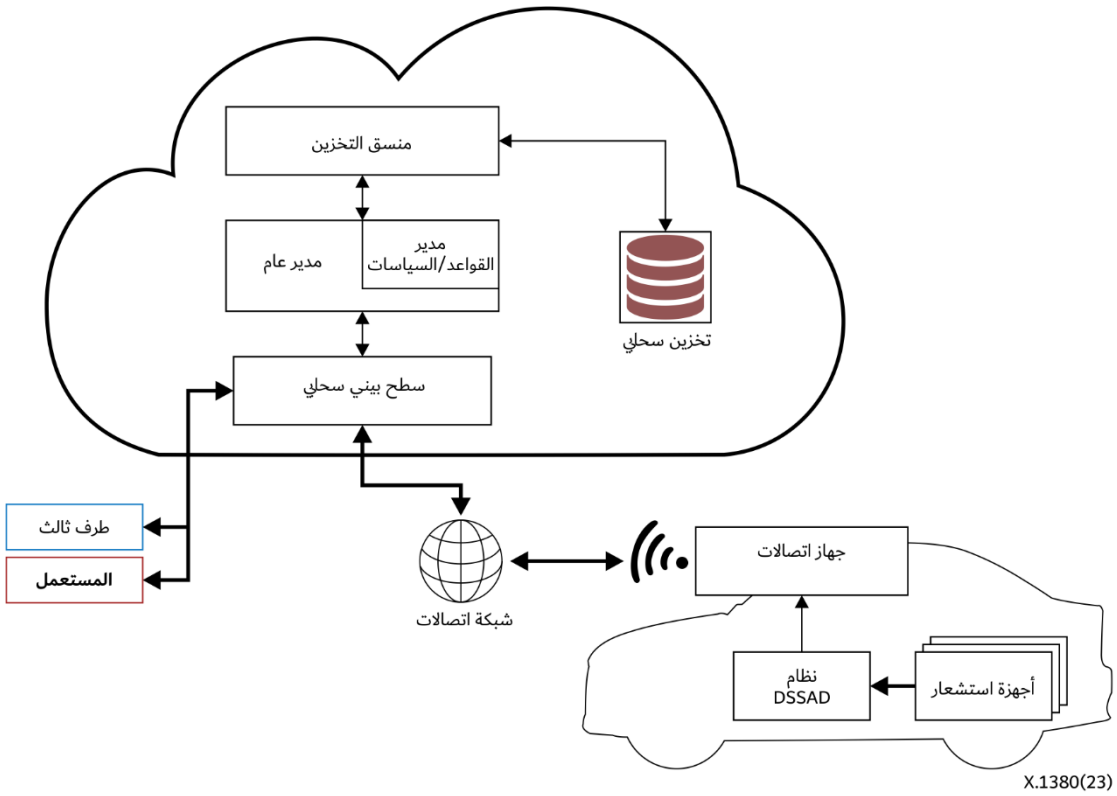
وفي نظام مسجل بيانات الأحداث القائم على الحوسبة السحابية والمعروض في الشكل 2، تحدَّد الكيانات الموجودة داخل الأنظمة السحابية لأداء وظائف إلى جانب وظائف مسجل بيانات الأحداث القائم على الحوسبة السحابية. ويُعدّ السطح البيني السحابي بوابة للنظام السحابي، ويحتفظ بسجل عمليات النفاذ المعيَّنة. وينظم المدير العام الإجراءات الأساسية لتخزين واستخراج بيانات مسجل بيانات الأحداث. ويتحقق من المتطلبات الأساسية للطلب المقدم من المستعمل/الطرف الثالث أو المركبة، وينفّذ أيضاً التحديثات المدخلة على القواعد/السياسات بمساعدة مديري القواعد/السياسات المدمجين. ويقوم منسّق التخزين بتخزين بيانات الأحداث واستخراجها وفقاً لسياسات محدَّدة مسبقاً. وقد تشمل السياسات فرز بيانات مسجل بيانات الأحداث، المستخرجة من التخزين السحابي تبعاً لسلطة مقدم الطلب. وقد تتضمن أيضاً منهجيةَ العملية الرامية إلى تخزين بيانات المسجل في التخزين السحابي واستخراجها منه.

2.6 نظام تخزين البيانات القائم على الحوسبة السحابية للقيادة الآلية

نظام تخزين البيانات للقيادة الآلية (DSSAD) هو نظام يرمي إلى إلقاء الضوء على من يطلب القيادة ومن يقوم بالقيادة (يمكن أن يكونا مختلفين، خاصة أثناء إجراءات الانتقال) من خلال تخزين مجموعة من البيانات التي توفر صورة واضحة عن التفاعلات بين السائق ونظام القيادة الآلية. وقد أُقرّ بنظام تخزين البيانات للقيادة الآلية في اللائحة [b-UN R157]. وتقر اللائحة بالنظام DSSAD كمتطلب لمركبات القيادة الآلية.

ويخزّن النظام DSSAD معلومات مثل تشغيل نظام القيادة الآلية وإبطاله وطلبات الانتقال ومناورات الطوارئ، وما إلى ذلك. وعند إبطال حالة النظام الآلي أو طلب الانتقال، يخزَّن سبب تغيير الحالة في النظام DSSAD. ويمكن لأصحاب المصلحة أن يوضحوا مَن طَلَب القيادة ومن كان المسؤول الفعلي عنها، من خلال تحليل بيانات النظام DSSAD التي تسجّل التفاعلات بين النظام الآلي والسائق.

ويقوم النظام DSSAD القائم على الحوسبة السحابية، الذي يرد وصفه في الشكل 3، بتخزين بيانات النظام DSSAD في الأنظمة السحابية من خلال جهاز اتصالات موصول بنظام DSSAD. والعملية التي تُقدَّم بها بيانات النظام DSSAD إلى النظام السحابي هي نفسها المتَّبعة في مسجّل بيانات الأحداث القائم على الحوسبة السحابية. والفرق هو أن بيانات نظام DSSAD ترسل بدلاً من بيانات مسجل بيانات الأحداث. ويرسل النظام DSSAD دورياً بياناته إلى النظام السحابي. وبالتالي، يمكن لأنظمة DSSAD أن تستجيب بمرونة للمشاكل التي تسبّبها القيود على قدرة النظام DSSAD على التخزين.



الشكل 3 – النظام DSSAD القائم على الحوسبة السحابية

3.6 مقارنة بين المسجّل EDR والنظام DSSAD

ترد في الجدول 1 مقارنة بين المسجل EDR والنظام DSSAD.

الجدول 1 – مقارنة بين المسجّل EDR والنظام DSSAD

	EDR	DSSAD
الغرض	تحليل الحوادث وإعادة تحديد مجرياتها	توضيح المسؤولية عن المركبة في أوقات محددة؛ من كان مطلوباً منه القيادة ومن كان المسؤول عن القيادة
الظروف المسبّبة	الحدث (مثلاً اصطدام): حادث مادي يتسبب في بلوغ عتبة الإطلاق	التفاعل: تغيّر حالة تشغيل النظام، أو طلب تغيير حالة تشغيل النظام
البيانات المجمعة	مجموعة بيانات محددة مسبقاً لازمة لتحليل الاصطدام	مجموعة بيانات محددة مسبقاً ذات صلة بالتحكم في المركبة والمسؤولية عنها
وقت التخزين	تسجيل البيانات عند بلوغ عتبة الإطلاق (مؤقتاً)	تسجيل البيانات خلال كامل مدة القيادة
توقيت التحميل	كل وقت للتخزين، وتشغيل/إيقاف المحرك	

7 تصميم نظام مسجل البيانات القائم على الحوسبة السحابية

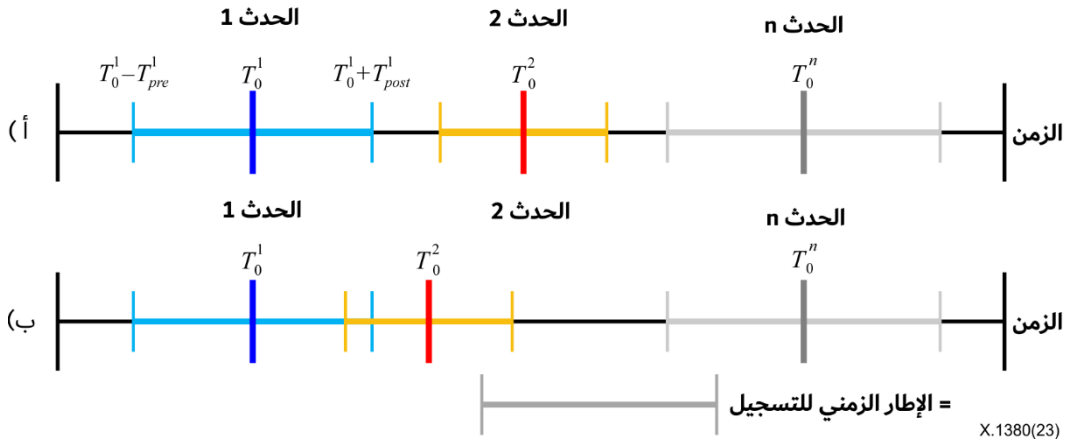
1.7 إدارة البيانات في مسجل بيانات الأحداث

الغرض من مسجل بيانات الأحداث (EDR) هو تخزين معلومات المركبة بشأن أحداث محددة من قبيل نشر الوسادة الهوائية. وتستخدم البيانات المسجلة في مسجل بيانات المعدات (EDR) لتحليل الاصطدام وإعادة تحديد مجرياته. ولذلك، يسجل المسجل EDR لحظة وقوع حدث ما وحالة المركبة وقت وقوع الحدث.

1.1.7 وقت تسجيل بيانات الأحداث

يوضح الشكل 4 كيف يقوم مسجل بيانات الأحداث بتسجيل حدث ما. فعندما يقوم مسجل بيانات الأحداث بالكشف عن حدث معيَّن، يحدّد وقت وقوع الحدث على أنه T_0 الخاص بالحدث الواقع، ثم يَجمع البيانات المعيَّنة خلال إطار زمني للتسجيل محدَّد مسبقا، يمثّل مدة زمنية محددة مسبقاً. ويشير الرمز T_0^n إلى وقت وقوع الحدث رقم n. وقد يكون الإطار الزمني للتسجيل مختلفاً باختلاف أنواع الأحداث لأن لكل نوع من الأحداث ظروفا مسببة مختلفة. ويشير الرمز T_{pre} إلى الوقت الذي يسبق الحدث المحدد. ويشير الرمز T_{post} إلى الوقت الذي يلي الحدث المحدد. ويمكن وصف الإطار الزمني بأنه $[(T_0 - T_{pre}) \sim (T_0 + T_{post})]$.

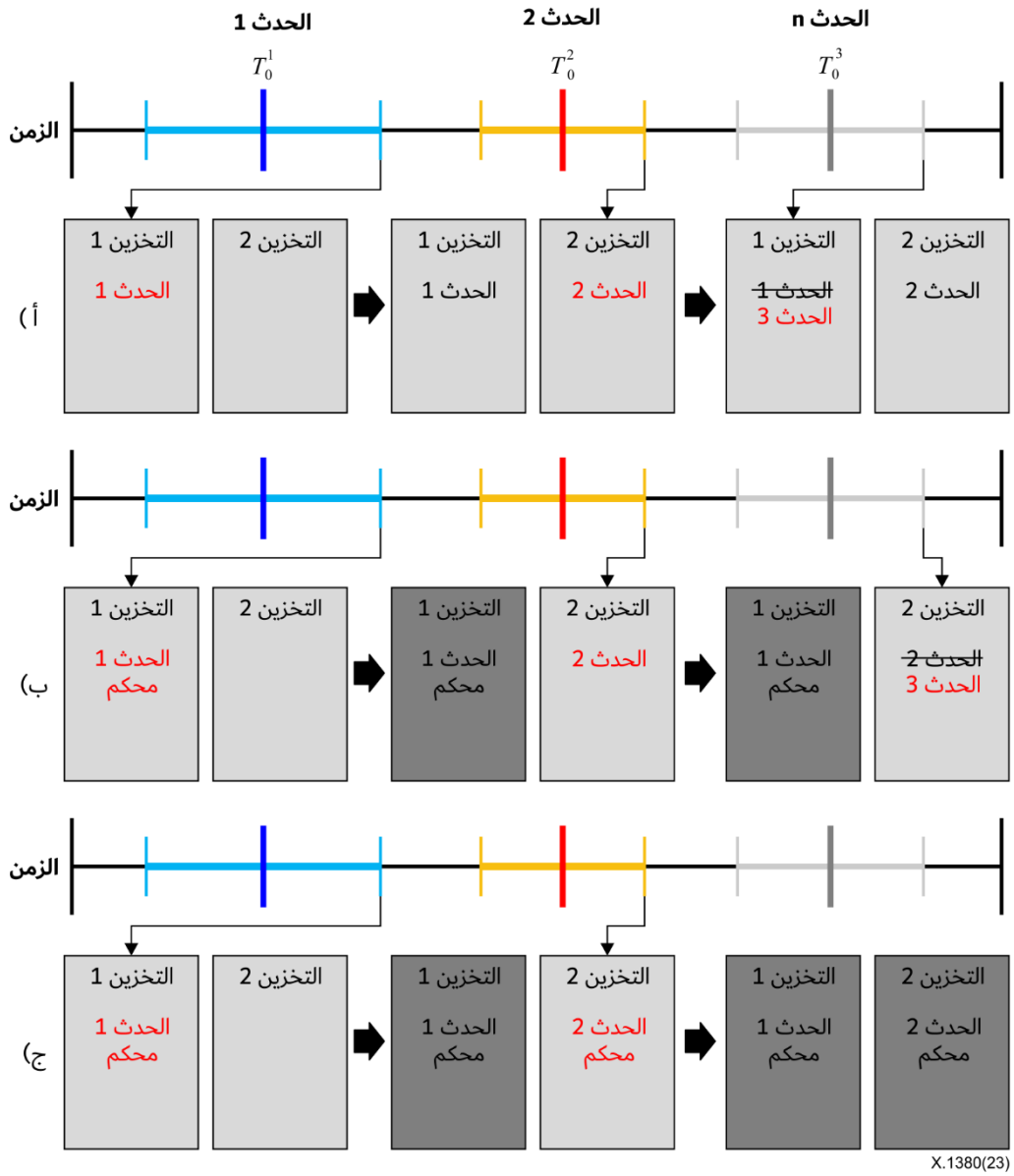
وفي حالة وقوع أحداث متعددة لاحقاً، على النحو الموضح في الشكل 4، يقوم مسجّل بيانات الأحداث بتسجيل البيانات التي يجمعها بغض النظر عن التداخلات في الإطار الزمني. ويبيّن الشكل 4 (أ) الأطر الزمنية المسجلة لأحداث غير متداخلة. ويبين الشكل 4 (ب) الأطر الزمنية المسجلة لأحداث متداخلة.



الشكل 4 – الإطار الزمني للتسجيل في نظام مسجل بيانات الأحداث:
(أ) الأحداث غير المتداخلة، و(ب) الأحداث المتداخلة

2.1.7 إحكام البيانات في نظام التخزين في المركبة

هناك العديد من الأجهزة على متن المركبة التي تخزّن بيانات مسجل بيانات الأحداث. ونظراً لتعدّد الظروف المحدَّدة مسبقاً، يمكن أن تقع أحداث متعددة في وقت لاحق. وتتَّبع عمليةُ التخزين التي يجريها مسجل بيانات الأحداث الإجراء المتمثل في التعامل "حسب أولوية الدخول" (FIFO). وإذا كانت جميع مخازن مسجل بيانات الأحداث قد امتلأت بالفعل بأحداث سابقة، تُكتب بيانات الأحداث الجديدة فوق البيانات الأقدم. ولكن، تتطلب بعض الظروف المسبّبة المحدَّدة مسبقاً التي يولدها حدث ما، مثل نشر الوسادة الهوائية الأمامية، إحكام تخزين البيانات بعد كتابة البيانات المسجلة بحيث يتعذّر الكتابة فوق البيانات المخزّنة. ويبين الشكل 5 مثالاً لإجراءات التسجيل التي يتبعها مسجل بيانات الأحداث، مع وجود مخزنين. ويبيّن الشكل 5 (أ) عملية تخزين بيانات الأحداث اللاحقة دون أن يكون هناك إحكام للبيانات، ويُظهر أن الحدث 3 يُسجل في المخزن فوق بيانات الأحداث الأقدم عهداً. ومن ناحية أخرى، يبيّن الشكلان (ب) و(ج) عملية تخزين بيانات الأحداث اللاحقة مع وجود إحكام للبيانات، ويُظهر أن الحدث التالي لا يمكن الكتابة فوقه في المخزن في حالة إحكام البيانات. ولا يمكن حفظ الحدث 3 في أي مخزن كان، خصوصاً في إطار العملية (ج)، لأن أجهزة التخزين مملوءة ومحكمة ببيانات الأحداث السابقة أي الحدث 1 والحدث 2. ولذلك، يلزم أن تقوم السياسة بتحديد الأولوية التي تُحكم بها إلى البيانات في أجهزة التخزين.



الشكل 5 – مثال على التسجيل في مسجل بيانات الأحداث باستخدام مخزنين:
(أ) دون إحكام للبيانات، و(ب) مع إحكام البيانات للحدث 1 فقط، و(ج) مع إحكام البيانات للحدث 1 والحدث 2

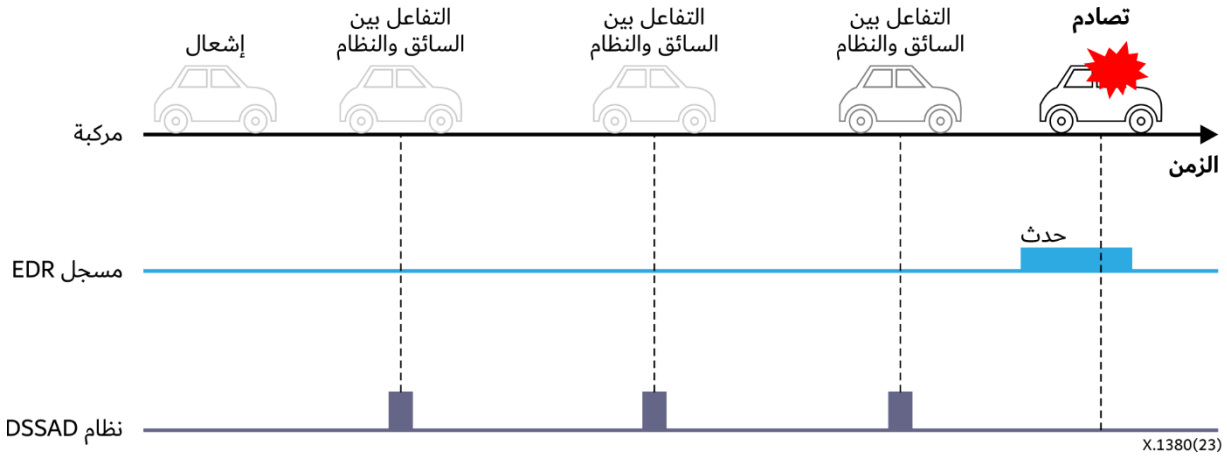
3.1.7 توسيع نطاق مجموعات البيانات

عادة ما تنظم الإدارات الوطنية أو الشركات المصنعة للمركبات مجموعة بيانات مسجل بيانات الأحداث التقليدي. ويتعين توسيع نطاق مجموعة بيانات مسجل بيانات الأحداث التقليدي لمواكبة تطوّر المركبات الموصولة وذاتية القيادة. فعلى سبيل المثال، قد تكون البيانات الواردة من أجهزة الاستشعار، مثل الرادارات وأجهزة كشف الأهداف وتحديد المدى ضوئياً، التي تُستخدم في المركبات ذاتية القيادة مهمة جداً للتحقيق في حادث سير. وعلاوة على ذلك، قد تكون الشهادات المخزنة المستعملة في الاتصالات من مركبة إلى كل شيء (V2X)، أثناء الحدث، ضرورية لبيئة المركبة الموصولة. وبالإضافة إلى ذلك، تكتسي السجلات المخزَّنة في نظام كشف الاقتحام (IDS)، فيما يتعلق بحالات الخلل وبالتوقيعات المستخدمة في الاقتحام، أهمية حاسمة لتوضيح ما إذا كان الحدث قد وقع نتيجة هجمات سيبرانية.

2.7 إدارة بيانات النظام DSSAD

1.2.7 وقت التسجيل في النظام DSSAD

يبيّن الشكل 6 الفَرق في وقت تسجيل البيانات بين المسجل EDR والنظام DSSAD. ويسجّل النظام DSSAD جميع التفاعلات المحدَّدة مسبقاً بين النظام الآلي والسائق، في حين يسجّل المسجل EDR خلال إطار زمني محدد مسبقاً عند وقوع الأحداث المسبّبة. وبالتالي، فإن البيانات المسجلة في المسجل EDR والنظام DSSAD مفيدة لتحديد الجهة التي كانت تتحكم في المركبة وقتَ الاصطدام.



الشكل 6 – وقت تسجيل البيانات فيما يخص المسجل EDR والنظام DSSAD

ينبغي أن يرسل النظام DSSAD القائم على الحوسبة السحابية البيانات إلى النظام السحابي وفقاً لسياسة محددة مسبقاً. وعندما تصل سعة تخزين النظام DSSAD في المركبة إلى الحد الأقصى، يمكن أن تُكتب البيانات الأحدث فوق البيانات السابقة باتباع مبدأ التعامل "حسب أولوية الدخول".

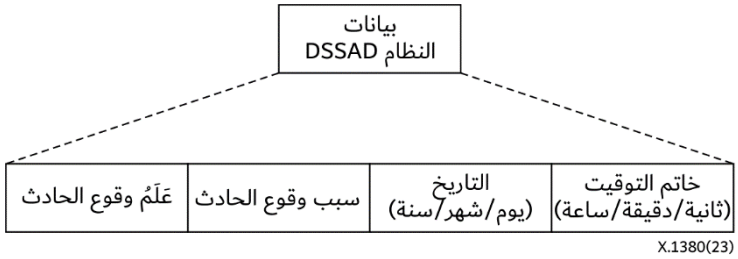
2.2.7 إحكام البيانات في وسط تخزين على متن المركبة

تَتَّبع أيضاً عمليةُ التخزين في النظام DSSAD مبدأ التعامل "حسب أولوية الدخول" مثل عملية التخزين التي يجريها المسجل EDR. وإذا كان مخزن النظام DSSAD ممتلئاً، تُكتب البيانات فوق البيانات القديمة. ولكن الظرف المحدَّد مسبقاً المسبّب لإحكام البيانات في مخزن المسجل EDR يتطلب إحكام مخزن بيانات النظام DSSAD بعد كتابة البيانات والقيام في الوقت نفسه برفض الكتابة فوق البيانات المخزَّنة. وتحدّد سياسة تخزين بيانات النظام DSSAD نسقَ البيانات المحكمة لهذا النظام. ويمكن أن يكون نسق البيانات المحكمة للنظام DSSAD مختلفاً عن النسق العادي لبيانات النظام DSSAD.

وبعد إحكام بيانات النظام DSSAD، يمكن إرسال البيانات المحكمة للنظام DSSAD إلى النظام السحابي. ويمكن أن يكون لإرسال البيانات المحكمة للنظام DSSAD الأولوية من بين البيانات المرسلة الأخرى، مثل البيانات العادية للنظام DSSAD وبيانات المسجل EDR المحكمة. وعندما يتم تأكيد انتهاء الإرسال، يمكن إزالة البيانات المرسلة من مخزن النظام DSSAD في المركبة.

3.2.7 نسق البيانات

في حين أن الغرض من مسجّل بيانات الأحداث هو تسجيل بيانات حدث ما، فإن الهدف من النظام DSSAD هو تحديد من يتحمّل عبء المسؤولية في لحظة معيَّنة (عادة لحظة وقوع الحادث).



الشكل 7 – نسق بيانات النظام DSSAD

تتضمن بيانات النظام DSSAD أربعة حقول، على نحو ما هو مبيَّن في الشكل 7 (يرجى العودة إلى اللائحة [b-UN R157]).

وعَلَمُ وقوع الحادث هو حقل يبيّن نوع التفاعل بين السائق والنظام، مثل طلبات الانتقال والمناورات التي تجرى في حالة طوارئ.

ويبيّن حقل سبب وقوع الحادث لم ظهر عَلَم وقوع الحادث. ويحتوي هذا الحقل على السبب المفصّل للانتقال. ويُدرج سبب وقوع الحادث في الفقرة 2.8 من اللائحة [b-UN R157].

وحقل التاريخ هو تاريخ استحداث عَلَم وقوع الحادث. وتَظهر البيانات في هذا المجال في الشكل التالي: يوم/شهر/سنة.

وحقل خاتم التوقيت هو لحظة إنتاج عَلَم وقوع الحادث. وترد البيانات في هذا الحقل في الشكل التالي: "ثانية/دقيقة/ساعة منطقة التوقيت". ونظراً لخصائص النظام DSSAD، ينبغي أن يكون خاتم التوقيت دقيقاً جداً. ويمكن استخدام خاتم توقيت واحد لبيانات أنظمة DSSAD متعددة مسجلة في آن واحد، ضمن الاستبانة الزمنية لبيانات معيَّنة من النظام DSSAD. وفي حال وقوع عدة أحداث في ثانية واحدة، يمكن أن يكون للأحداث المتعددة نفس خاتم التوقيت. وفي هذه الحالة، ينبغي أن تشير بيانات النظام DSSAD إلى الترتيب الزمني للأحداث.

3.7 المعلومات المحددة لهوية المركبة (VII)

عندما يقوم المسجل EDR/النظام DSSAD بتحميل بياناتهما في الأنظمة السحابية، ينبغي النظر في المعلومات المحدّدة لهوية المركبة. ويمكن أن تكون هذه المعلومات عبارة عن رقم لوحة المركبة أو شهادة المركبة أو الرقم المحدّد لهوية المركبة أو أي شيء يمكن استعماله للتعرف على هوية المركبة. ويمكن أن تُعتبر المعلومات المحدّدة لهوية المركبة معلومات محددة لهوية الأشخاص (PII).

وفيما يتعلق ببيئات المركبات المستقبلية، ينبغي أن نأخذ في الاعتبار الحالات التي يتشارك فيها مستعملون متعددون مركبة واحدة، مثل الاستخدام المشترك للسيارات. وفي الحالات التي يرغب فيها كل مستعمل في استعمال الأنظمة DSSAD/EDR القائمة على الحوسبة السحابية أثناء القيادة، ينبغي أن تكون المركبة التي يتم تشاركها قادرة على التمييز بين كل مستعمل أثناء القيادة. ولكن يصعب تحديد هوية كل مستعمل بسبب عدم وجود إجراء إلزامي تقوم المركبة بموجبه بجمع المعلومات المتعلقة بمستعمل ما (مثل هوية المستعمل). ويمكن الحصول على المعلومات المتعلقة بالمستعملين باستخدام أنظمة شخصية مثل المفتاح الرقمي للهواتف الذكية الذي يعتمد على عملية استيقان تستخدم شهادة المستعمل الفريدة. وهكذا يمكن جمع المعلومات المتعلقة بالمستعمل وإرسالها كجزء من المعلومات المحددة لهوية المركبة.

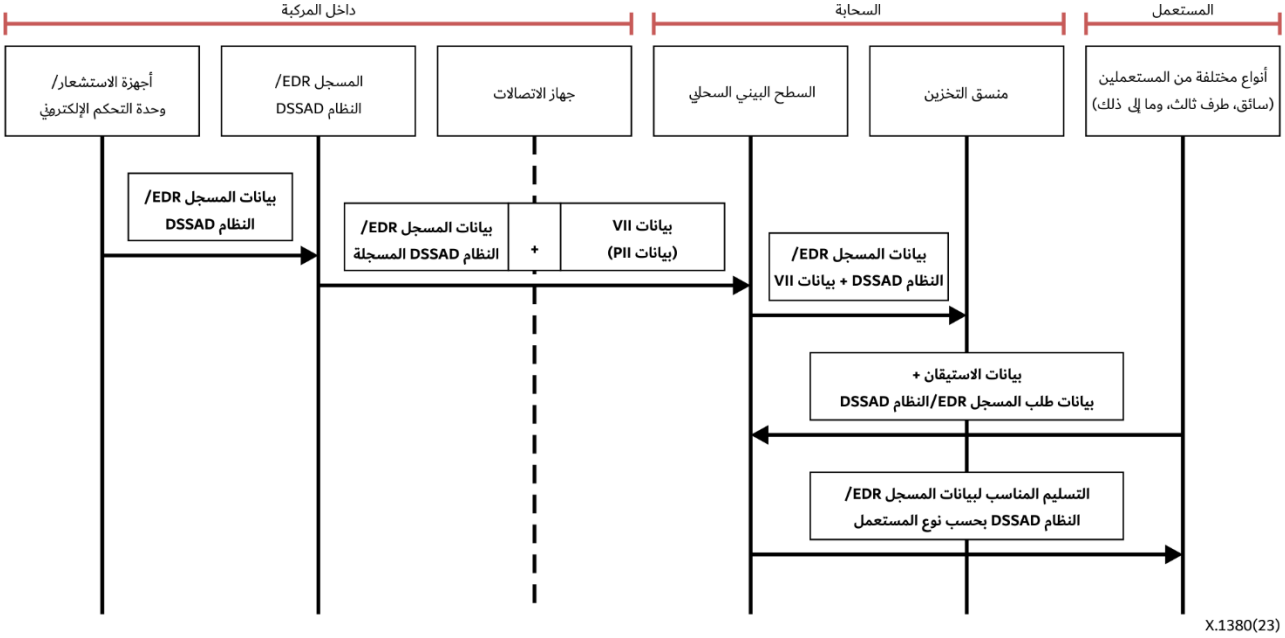
وعلى نحو ما ورد وصفه في الفقرة 1.6، تُجمع بيانات المسجل EDR عندما تواجه المركبة أحداثاً مسببة محددة مسبقاً، بينما تُجمع بيانات النظام DSSAD عندما يكون هناك تفاعل بين المركبة والسائق. وبما أن المسجل EDR والنظام DSSAD مرتبطان بمركبة وأن البيانات يتم جمعها لكل مركبة، يُعتبر تحديد هوية كل مركبة مَهمّة أساسية للنظام DSSAD/EDR القائم على الحوسبة السحابية. وبالتالي، تتألف المعلومات المحددة لهوية المركبة من العناصر التالية:

- **معلومات عن المركبة** (إلزامية): معلومات تحدد هوية مركبة معينة مثل الرقم المحدّد لهوية المركبة (VIN).
- **معلومات عن المستعمل** (اختيارية): بيانات تعرف هوية المستعمل أو السائق.

ويبين الشكل 8 عملية إرسال للمسجل EDR/النظام DSSAD للبيانات من المركبة إلى السحابة.

ويجمع المسجل EDR/النظام DSSAD البيانات من كل جهاز استشعار ووحدة تحكم إلكتروني في الشبكة المدمجة داخل المركبة وفقاً لقواعد محددة مسبقاً، ثم تُرسل إلى جهاز الاتصالات. ويضيف جهاز الاتصالات المعلومات المحددة لهوية المركبة إلى بيانات المسجل EDR/النظام DSSAD المجمعة، ويرسلها إلى النظام السحابي. وتُنقل بيانات المسجل EDR/النظام DSSAD والمعلومات المحددة لهوية المركبة، الواردة من السطح البيني السحابي، إلى منسق التخزين، ثم يتم تخزينها وفقاً لسياسة النظام السحابي.

ولا يُمنح الحقّ في النفاذ إلى بيانات المسجل EDR/النظام DSSAD المخزّنة في النظام السحابي إلا للمستعملين المخولين. ولذلك، ينبغي للمستعملين الذين يرغبون في الحصول على معلومات من النظام السحابي أن يرسلوا معلومات الاستيقان لإثبات هويتهم. ويوفر النظام السحابي بيانات المسجل EDR/النظام DSSAD للمستعملين الذين تم الاستيقان من هويتهم.



الشكل 8 – تدفق بيانات المسجل EDR/النظام DSSAD القائمين على الحوسبة السحابية

4.7 الأنظمة السحابية للمسجل EDR والنظام DSSAD

1.4.7 زيادة إمكانية النفاذ إلى البيانات المسجلة

لدى مسجل بيانات الأحداث التقليدي نقطة نفاذ على المنفذ OBD-II ولا يمكن استخراج بيانات المسجل EDR واستخدامها إلا عن طريق المنفذ OBD-II وأداة تشخيص المركبة. ولهذا السبب، لا يستخدم مالكو المركبات بيانات المسجل EDR إلا نادراً على الرغم من امتلاكهم للبيانات.

ومن ناحية أخرى، فإن المسجل EDR/النظام DSSAD القائمين على الحوسبة السحابية يوفران للمستعملين زيادة إمكانية النفاذ إلى بيانات DSSAD/EDR بتحميل بيانات DSSAD/EDR في البيئات السحابية. ويمكن للمستعملين أو لطرف ثالث استعمال المعلومات المحددة لهوية المركبة أو معلومات تحديد الهوية المحددة مسبقاً لتحميل بيانات DSSAD/EDR الخاصة بهم لمواصلة استخدامها. ويمكن أن يؤدي ذلك إلى توسيع نطاق بيانات DSSAD/EDR القابلة للزيادة، وأن يقود إلى تحسّن السلامة على الطرق.

2.4.7 تحديث القواعد/السياسات

يحدد نظام DSSAD/EDR القائم على الحوسبة السحابية وظيفة تحديث القواعد/السياسات. وتحدد القاعدة كيفية التعامل مع البيانات في مركبة ما، وتحدد السياسة كيفية التعامل مع البيانات في السحابة. وتتألف القاعدة من ظروف الحادث، ونمط تسجيل البيانات، ووقت تسجيل نوع معيَّن من البيانات، وإجراء التحميل في المركبة. وتتألف السياسة في سياق نظام DSSAD/EDR

القائم على الحوسبة السحابية من السلطة الممنوحة للأطراف للنفاذ إلى البيانات. ويتولى هذه السياسة منسق التخزين في الأنظمة السحابية لتخزين بيانات DSSAD/EDR.

وتتيح أنظمة DSSAD/EDR القائمة على الحوسبة السحابية وظيفة تحديث القواعد/السياسات. وبوجهٍ عام، تحدد إدارات التنظيم الوطنية مجموعة البيانات الإلزامية الخاصة بالأحداث وشروطها. وإثر التحديثات التنظيمية التي تجريها السلطات بناء على طلب شرعي من المستعمل/الطرف الثالث، يقوم نظام DSSAD/EDR القائم على الحوسبة السحابية بتنفيذ التحديثات التي أجريت فيما يخص القواعد/السياسات على المركبة والسحابة.

8 تحليل التهديدات الأمنية

1.8 الأصول الأمنية والأهداف الأمنية ذات الصلة

تعني الأصول الأمنية أي غرض للبيانات أو وظيفة أو مورد ينبغي حمايته. وبالنظر إلى الأنظمة DSSAD/EDR القائمة على الحوسبة السحابية، ترد الأصول والأهداف الأمنية ذات الصلة التالية في الجدول 2.

الجدول 2 – الأصول الأمنية والأهداف الأمنية ذات الصلة

الأصول الأمنية	الوصف	الأهداف الأمنية ذات الصلة
بيانات DSSAD/EDR المخزنة في مركبة	بيانات DSSAD/EDR المجمعة في المركبة	السلامة
قواعد DSSAD/EDR المخزنة في مركبة	قواعد DSSAD/EDR التي يمكن تحديثها بموجب سياسات الحوسبة السحابية	السلامة
برمجيات DSSAD/EDR الثابتة	البرمجيات الثابتة لجهاز DSSAD/EDR	السلامة
الرزمة عبر الأثير (OTA)	الرزمة عبر الأثير المستخدمة لتحديث قواعد DSSAD/EDR	السرية والسلامة
حركة نواقل البيانات	حركة نواقل البيانات المرسلة في الشبكة داخل المركبة (IVN)	السرية والسلامة
سجل DSSAD/EDR	سجل التدقيق في جهاز DSSAD/EDR	السلامة والمساءلة
الاتصالات مع وسائل التصحيح/التشخيص	الاتصال بين جهاز DSSAD/EDR وأدوات التصحيح أو أدوات التشخيص	السرية والاستيقان
الاتصالات مع الطرف الخلفي	الاتصال بين الطرف الخلفي والمركبات أو المستعملين/الأطراف الثالثة	السرية والاستيقان والتيسّر
سياسات الخدمات السحابية	سياسة الخدمات السحابية	السلامة
المعلومات المحدّدة لهوية المركبة	البيانات الخاصة المستخدمة لتحديد هوية المستعملين/المركبات	السرية
سجل الخدمات السحابية	يمكن أن تؤثر سجلات التدقيق المتعلقة بسياسات الخدمات السحابية، وطلبات المستعملين/الأطراف الثالثة، والسلوكيات الأخرى، على أمن الخدمات السحابية	السلامة والمساءلة
بيانات DSSAD/EDR المخزنة في الحوسبة السحابية	بيانات DSSAD/EDR الواردة من المركبات	السلامة

2.8 التهديدات الأمنية

تصف هذه الفقرة التهديدات الأمنية في أنظمة مسجلات البيانات القائمة على الحوسبة السحابية. ويرد في التوصية [ITU-T X.1371] وصف لمجمل التهديدات التي تم التعرّف عليها في المركبات الموصولة.

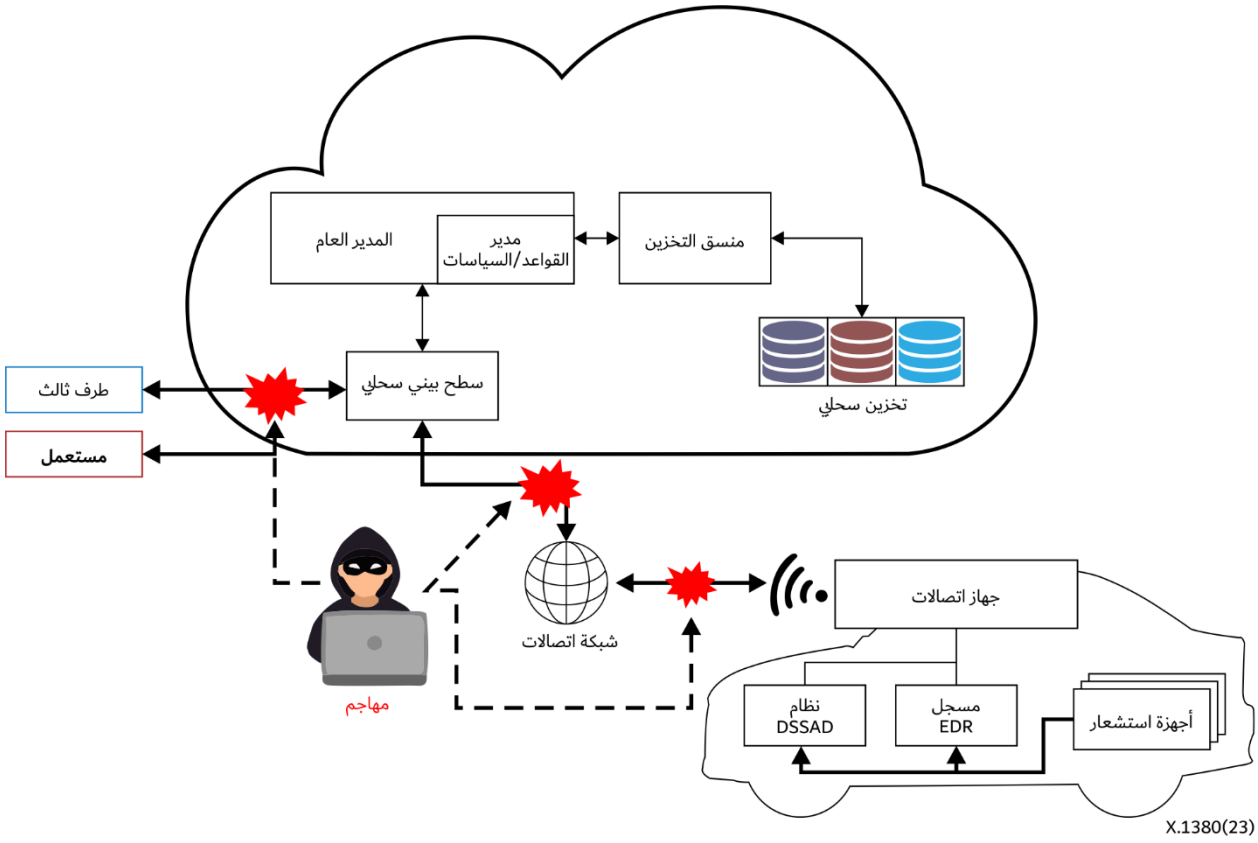
1.2.8 التهديدات المتعلقة بالسرية

إن البيانات التي تقدَّم داخل أنظمة مسجلات البيانات القائمة على الحوسبة السحابية هي بوجه عام البيانات الخاصة المتعلقة بالمستعملين. وقد تكون ملكية البيانات ونطاق جمعها مختلفين عما ورد في اللوائح التي ترتبط بها المركبة؛ ولكن عادة ما تُعتبر بيانات نظام مسجل البيانات معلومات محدّدة لهوية المركبة. ويمكن اعتبار الإخفاق في الحفاظ على سرية البيانات في أنظمة مسجلات

البيانات القائمة على الحوسبة السحابية انتهاكاً لسرية البيانات الخاصة بالمستعملين. وقد يكون التنصت بشكل عام والتنصت على الشبكة مثلاً من التهديدات النمطية للسرية.

- **التنصت**: في الشبكات اللاسلكية، مثل الخدمة القائمة على الحوسبة السحابية، يُعدّ الاستماع إلى وسائل الإعلام هجوماً محتملاً من السهل تنفيذه. ويمكن للمهاجم أن يتجسس على رسائل تشمل المعلومات المحدّدة لهوية المركبة، في أنظمة مسجلات البيانات القائمة على الحوسبة السحابية بطريقتين. أولاً، يمكن أن يحدث ذلك بين المركبة والمخدم السحابي. وفي هذه الحالة، يمكن أن تتسرب بيانات الحدث من المركبات، والبيانات المتعلقة بتحديث القواعد/السياسات من المخدم السحابي.

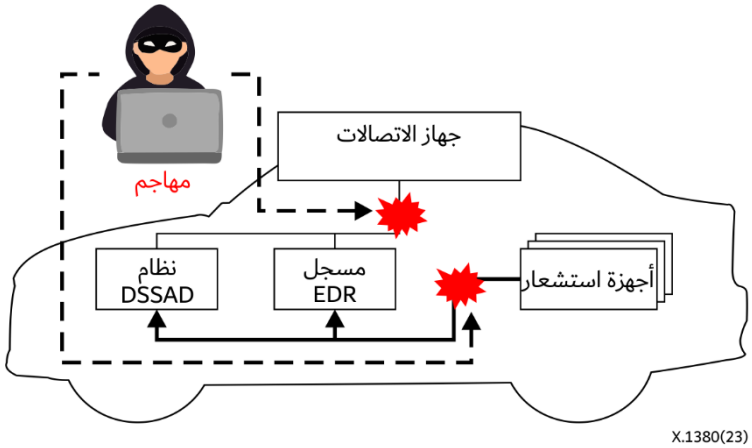
وثانياً، يمكن أن يحدث الهجوم بين المستخدم/الطرف الثالث والأنظمة السحابية. وفي هذه الحالة، يمكن أن تتسرب بيانات الحدث المستمدة من النظام السحابي وطلبات تحديث القواعد/السياسات التي يقوم بها المستخدم/الطرف الثالث ثالث.



الشكل 9 – التنصت على أنظمة مسجلات البيانات القائمة على الحوسبة السحابية

ثالثاً، يمكن لمهاجم أن يقوم بالتقاط وتحليل الرزمة عبر الأثير المرسلة لتحديث قواعد مسجل بيانات الأحداث (EDR). وبناءً على ذلك، قد يرسل مهاجم قواعد مزوّرة لتقويض التدابير الأمنية.

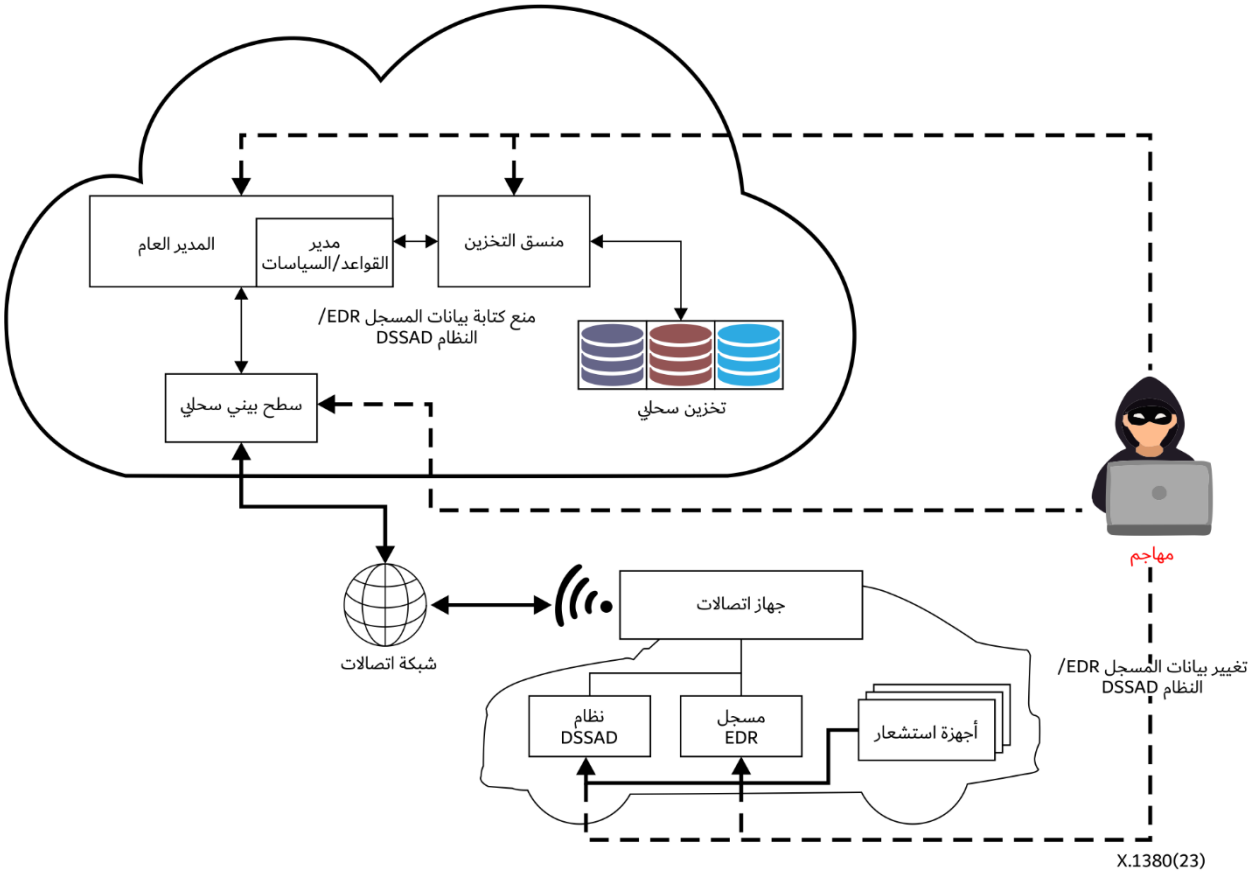
- **التجسس من خلال التنصّت**: يمكن التنصّت بشكل مباشر على شبكة داخل المركبة، وهذا يُعتبر من الهجمات المادية. وتملك المركبات الحديثة نواقل بيانات متعددة لشبكة منطقة وحدة التحكم (CAN)؛ وتقوم بوابة أمنية حصراً (أو حائط حماية داخل المركبة) بالتحكم في النفاذ إلى أي ناقل بيانات. ولا يمكن مراقبة إجمالي حركة جميع ناقلات بيانات شبكة منطقة وحدة التحكم إذا لم يكتسب المهاجمون امتياز البوابة الأمنية. وبالتالي، يمكن أن يحاول المهاجمون النفاذ مادياً إلى المركبة المستهدفة عن طريق التنصت بواسطة الأسلاك للتجسس على كامل حركة ناقلات بيانات شبكة منطقة وحدة التحكم بما فيها بيانات المسجل EDR/النظام DSSAD.



الشكل 10 – التنصت على أنظمة مسجلات البيانات القائمة على الحوسبة السحابية

2.2.8 التهديدات المتعلقة بالسلامة

تُستخدم بيانات المسجل EDR في تحليل اصطدام المركبات أو الحوادث التي تتعرض لها، وتُستخدم بيانات النظام DSSAD لتحديد من يتحمل المسؤولية. ولذلك، ينبغي التأكد من أن البيانات لا يتم التلاعب بها أثناء عمليتي التخزين والنقل. والسلامة هي أحد أهم الأهداف الأمنية لسجلات التدقيق مثل بيانات المسجل EDR/النظام DSSAD. وما يريده المهاجمون هو انتهاك سلامة هذه البيانات باستخدام الأساليب المحددة أدناه.



الشكل 11 – التلاعب بتدفق التحكم في أنظمة مسجلات البيانات القائمة على الحوسبة السحابية

من خلال التلاعب بتدفق التحكم لنظام مسجل البيانات القائم على الحوسبة السحابية، قد يغير المهاجم بيانات DSSAD/EDR أو يمنع كتابة إدخالات بيانات DSSAD/EDR. فعلى سبيل المثال، يحدد المهاجم السطح البيني للتصحيح على لوحة الدارة المطبوعة (PCB) التابعة للمسجل EDR/النظام DSSAD والنفاذ إليه، ويستخدم هذا السطح البيني للتلاعب بالشفرة المنفذة. وعلاوة على

ذلك، يستطيع المهاجم التلاعب بالبرمجيات الثابتة أو قواعد DSSAD/EDR على نظامي DSSAD/EDR. ويمكن للمهاجم أيضاً تعديل حركة نواقل البيانات والتلاعب بسجل المسجل EDR/النظام DSSAD.

وفي حالة النظام السحابي، يستطيع المهاجم النفاذ إلى المخزن والتلاعب ببيانات المسجل EDR وسجلات التدقيق وسياسة الخدمات السحابية باستخدام برمجيات ضارة وسطوح بينية غير آمنة لبرمجة التطبيقات (API).

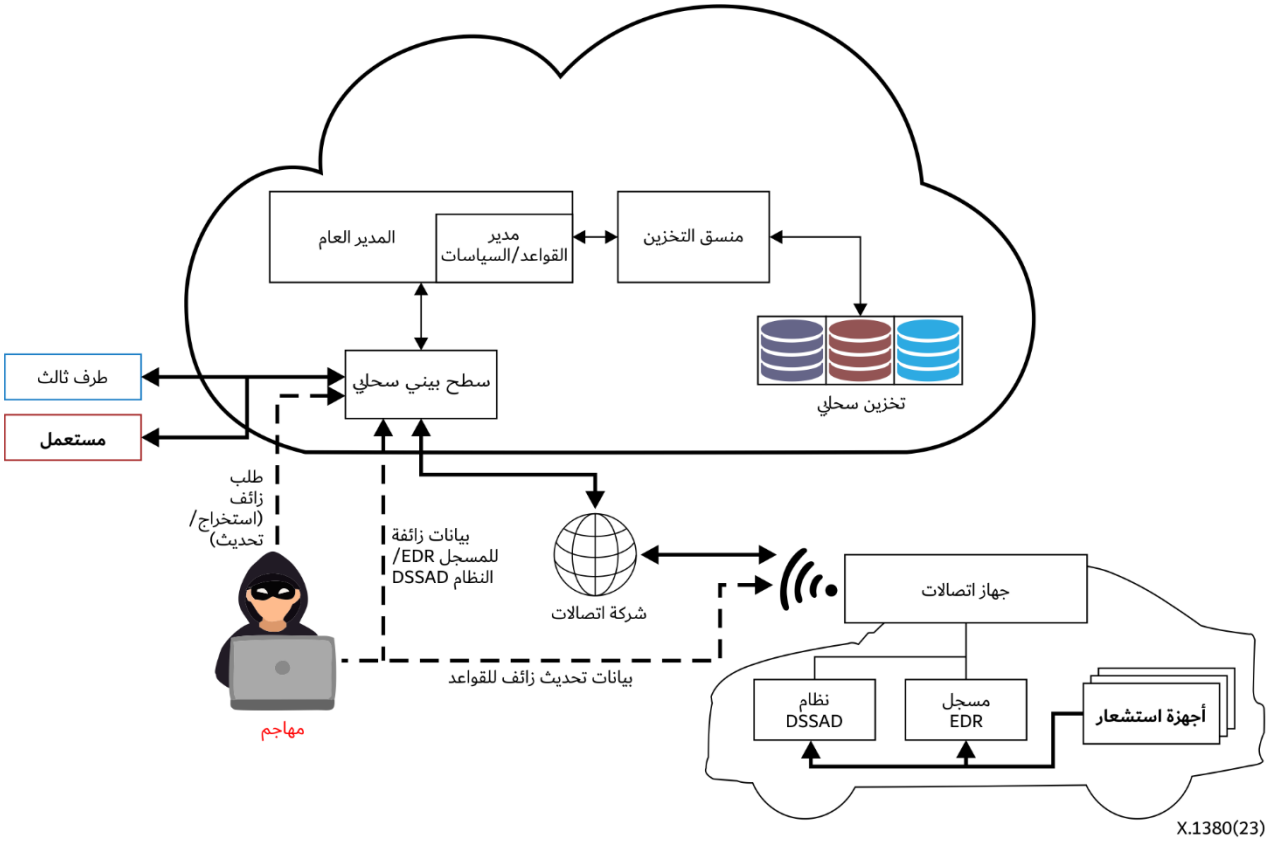
ويبين الشكل 11 الهجوم المتمثل في التلاعب بتدفق التحكم في نظام مسجل البيانات القائم على الحوسبة السحابية.

3.2.8 التهديدات المتعلقة بالاستيقان

يمكن أن يشكل هجوم الاعتراض وهجوم انتحال الصفة وهجوم التكرار تهديدات نمطية لعملية الاستيقان.

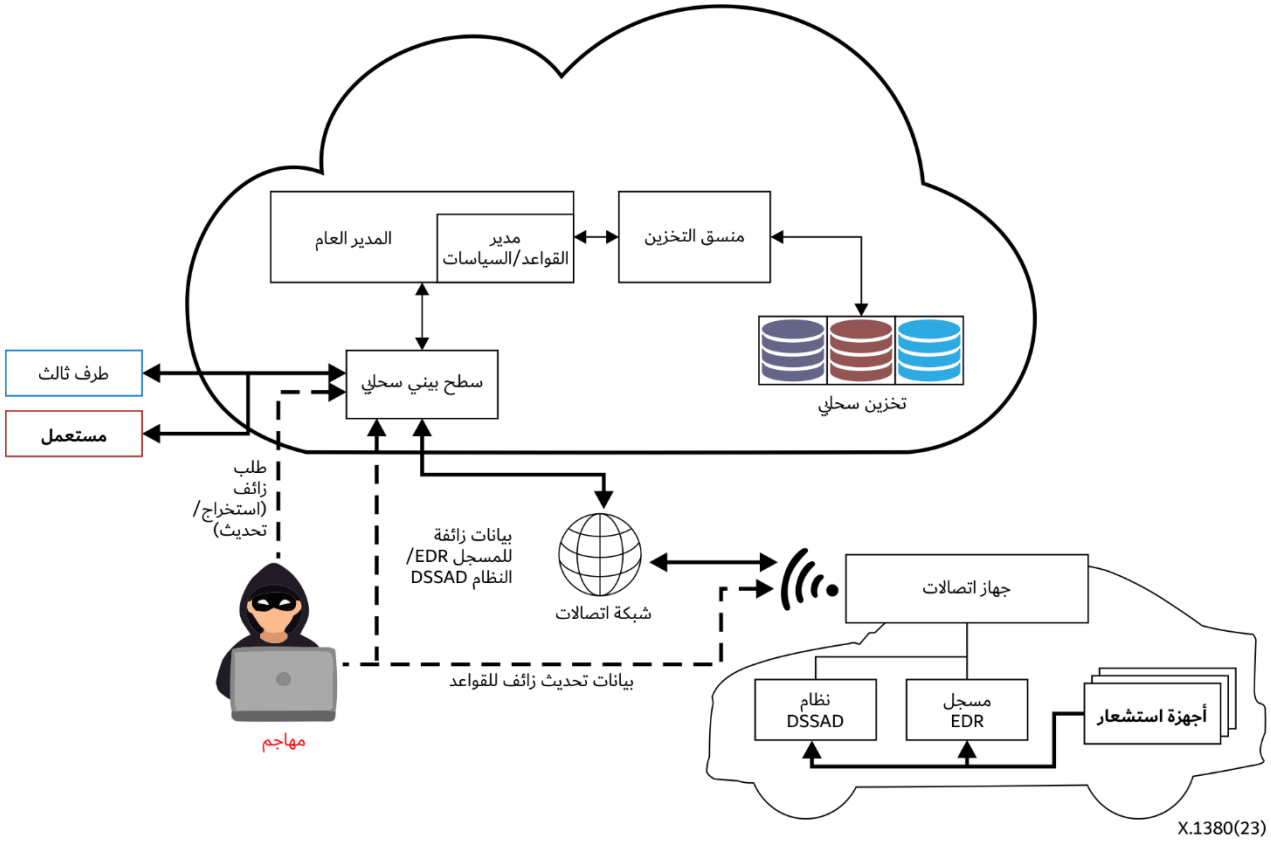
- **هجوم الاعتراض**: في نظام مسجل البيانات القائم على الحوسبة السحابية، يمكن للمهاجم اعتراض الرسائل التي تُرسَل بين مركبة وسحابة أو بين سحابة ومستعمل، ثم يقوم بإعادة إرسالها برسائل متلاعَب بها عشوائياً. ولا يدرك المرسِل أن المستقبِل مهاجم مجهول يحاول النفاذ إلى الرسالة أو تعديلها قبل إعادة إرسالها إلى المستقبل. وهكذا، يستطيع المهاجم التحكم في كامل عملية الاتصالات بينهما.
- **هجوم انتحال الصفة**: يمكن إجراؤه بأربعة أساليب في نظام مسجل البيانات القائم على الحوسبة السحابية:
  - طلب زائف لاستخراج بيانات المسجل EDR/النظام DSSAD إلى النظام السحابي
  - طلب زائف لتحديث القواعد من مركبة معيَّنة إلى النظام السحابي
  - طلب زائف لتخزين بيانات المسجل EDR/النظام DSSAD في النظام السحابي
  - تحديث زائف للقواعد لنظام DSSAD/EDR في المركبة

  ويمكن أن تتسبب هجمات انتحال الصفة في ضرر جسيم بسلامة كامل نظام مسجل البيانات القائم على الحوسبة السحابية لأنها قادرة على توليد بيانات أحداث زائفة أو تغيير قواعد/سياسات أحداث. ويمكن للمهاجم أيضاً تسريب البيانات الخاصة المخزنة في النظام السحابي من خلال هجوم انتحال الصفة.



الشكل 12 – هجوم انتحال الصفة على أنظمة مسجلات البيانات القائمة على الحوسبة السحابية

- **هجوم التكرار**: يمكن أن تَحدث من خلال هجوم التكرار ازدواجية في بيانات المسجل EDR/النظام DSSAD وتراجع غير مرغوب فيه في القواعد/السياسات.



الشكل 13 – هجوم التكرار على أنظمة مسجلات البيانات القائمة على الحوسبة السحابية

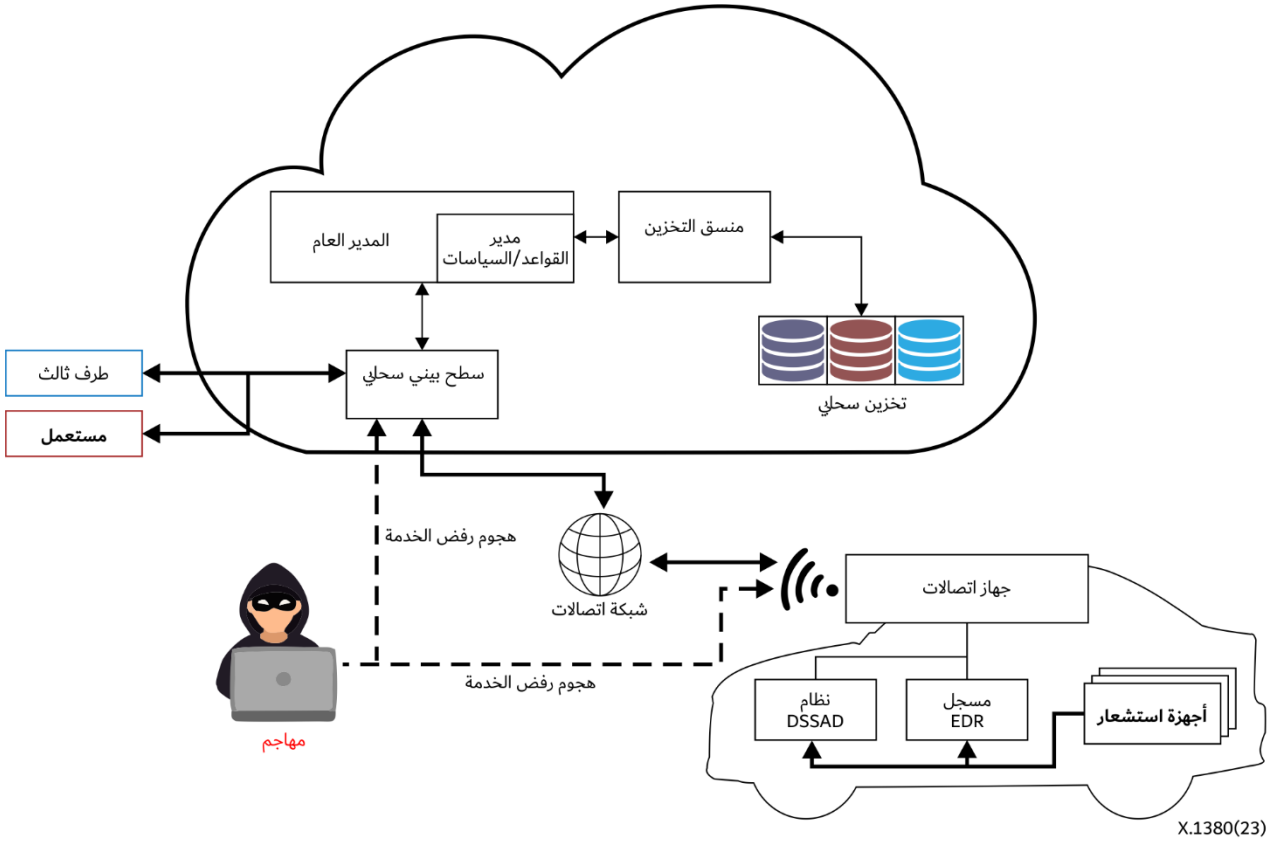
- **النفاذ المادي**: إذا تمكّن المهاجم من النفاذ إلى المركبة عبر منفذ التصحيح، يمكن أن يجري مجموعة أخرى من الهجمات. وفريق عمل الاختبار المشترك (JTAG) هو السطح البيني الأكثر شيوعاً الذي يُستخدم كمنفذ تصحيح. ويوفر النفاذ عبر فريق عمل الاختبار المشترك القدرةَ على قراءة وكتابة الذاكرة، مما يؤدي إلى التلاعب بالبرمجيات الثابتة وإضعاف التدابير الأمنية.

وعمليات التشخيص هي عبارة عن نفاذ مادي آخر إلى المركبة. ويمكن للمهاجم النفاذُ إلى المنفذ OBD-II باستخدام أدوات التشخيص، أو يمكنه النفاذُ مباشرةً إلى البوابة ذات وظائف التشخيص عن بُعد. وخدمة التشخيص الموحدة (UDS) هي بروتوكول قياسي لعمليات التشخيص يتيح مراقبة الشبكة ووحدات التحكم الإلكتروني داخل المركبة والتلاعب بها.

4.2.8 التهديدات المتعلقة بالتيسّر

التيسّر عامل حاسم في نظام مسجل البيانات القائم على الحوسبة السحابية نظراً إلى إمكانية تخزين معلومات مفيدة عن حوادث السير أو حوادث الاصطدام في أي وقت. وهجوم رفض الخدمة (DoS) هو التهديد الأكثر شيوعاً لعملية التيسر.

- **هجوم رفض الخدمة**: يمكن لهجوم رفض الخدمة أن تكون له تبعات خطيرة على أنظمة مسجلات البيانات القائمة على الحوسبة السحابية لأن المهاجم يحاول أن يحجب وسائل الاتصالات/التخزين/الإدارة الأساسية لبيانات DSSAD/EDR، مما يؤدي إلى جعل نظام مسجل البيانات القائم على الحوسبة السحابية غير ذي جدوى فيما يخص تحليل الحادث. وكمثال على هجوم رفض الخدمة، يمكن أن يؤدي إغراق قناة الشبكة بكم كبير من الرسائل التي يولدها المهاجم، إلى شلّ عُقد الشبكة أو الأنظمة السحابية بأكملها. ولن تكون عُقد الشبكة (في المركبة أو النظام السحابي) قادرة على التعامل مع الكمية الهائلة من البيانات الواردة، وتتسبب في خلل في تخزين بيانات DSSAD/EDR في الأنظمة السحابية أو في تحديث القواعد/السياسات في المركبة والأنظمة السحابية.



الشكل 14 – هجمات رفض الخدمة في أنظمة مسجلات البيانات القائمة على الحوسبة السحابي

5.2.8 التهديدات المتعلقة بالمساءلة

– **فقدان إمكانية اقتفاء أثر الأحداث:** تعمل مكونات من قبيل مدير القواعد/السياسات ومنسق التخزين الموجودين في النظام السحابي وفقاً لمجموعة القواعد/السياسات التي يقوم بتثبيتها المستعمل المخوّل. وبالتالي، تُعَد إدارة سجل التغييرات المدخلة على القواعد/السياسات ذات أهمية كبيرة في مجال المساءلة. ويمكن للمهاجم أن يُحدث بلبلة من خلال تلاعبه بسجل الأحداث أو حذفه.

9 متطلبات الأمن

1.9 بدء التشغيل الآمن

يوصَى بالتحقق من سلامة البرمجيات الثابتة المخزنة في ذاكرة أجهزة DSSAD/EDR قبل التنفيذ أو أثناءه. ويوصى أيضاً بالتحقق من سلامة قواعد المسجلات EDR/الأنظمة DSSAD والتشكيلات ذات الصلة وبيانات المعايرة.

وتتألف عملية حماية البرمجيات الثابتة والقواعد من خطوتين. أولاً، أثناء تثبيت البرمجيات الثابتة والقواعد، يتم اختبارها للتحقق من استيقانها قبل أن تُكتب في الذاكرة الداخلية ثم تشكَّل باعتبارها البرمجيات الثابتة والقواعد المعمول بها. وثانياً، يتم، أثناء كل بدء تشغيل، التحقق من سلامة البرمجيات الثابتة والقواعد المعمول بها.

ويوصى بأن تَستخدم آلية بدء التشغيل الآمن وسائل تجفير تناظرية أو لا تناظرية للتحقق من سلامة البرمجيات الثابتة والقواعد من خلال تحلّيها بمستويات ملائمة من الأمن. ويوصى أيضاً بأن تَستعمل أجهزة EDR وDSSAD مصدر ثقة بالعتاد، مثل وحدة أمن العتاد (HSM)، لتخزين مفاتيح التجفير بشكل آمن والتعجيل بحساب خوارزميات التجفير.

2.9 السجل الآمن

ينبغي ضمان سلامة بيانات التسجيل باستخدام أساليب التجفير الآمنة. وبما أن بيانات المسجلات EDR/الأنظمة DSSAD هي أدلة على حالات معيّنة، ينبغي حماية هذه البيانات من حالات التلاعب غير المخوّل.

وفي حالة النظام السحابي، ينبغي للمدير العام أن يضع سجلات في كل حالة على النحو المحدّد أدناه:

- محاولات الاستيقان من المستعملين/الأطراف الثالثة؛
- تحديث السياسات.

ويوصَى بتخزين السجلات بشكل آمن. ويمكن إرفاق تدابير تجفير، مثل شفرة استيقان الرسائل (MAC)، بالسجلات و/أو تخزينها في مخزن آمن يتم التحكم بشكل مناسب في النفاذ إليه. وينبغي وضع حد أدنى لحفظ السجلات المخزَّنة، باتباع سياسة مورد الخدمة السحابية أو لوائح كل بلد.

3.9 الاتصالات الآمنة

لأنظمة مسجلات البيانات القائمة على الحوسبة السحابية عدة قنوات اتصالات على النحو المحدّد أدناه:

- الاتصالات بين الأنظمة السحابية والمركبات؛
- الاتصالات بين المستعملين/الأطراف الثالثة؛
- الاتصالات بين وحدات التحكم الإلكتروني وأجهزة الاستشعار والمفعِّلات في المركبات.

ويوصى بضمان سرية واستيقان الرسائل في الاتصالات بين النظام السحابي والمركبات أو المستعملين/الأطراف الثالثة. ويمكن تحقيق السرية والاستيقان باستخدام تدابير تجفير مثل بروتوكول أمن طبقة النقل (TLS).

ويوصى أيضاً بضمان التيسّر في الاتصالات بين النظام السحابي والمركبة. وهذا يعني أن كمية هائلة من بيانات المسجلات EDR والأنظمة DSSAD المستمدة من مركبات عديدة ينبغي تخزينها في المخزن السحابي بشكل مناسب.

ويوصى بضمان سلامة الرسائل والبيانات في الاتصالات بين وحدات التحكم الإلكتروني وأجهزة الاستشعار والمفعّلات في المركبات لإنتاج بيانات سليمة للمسجلات EDR/الأنظمة DSSAD، لأن البيانات الواردة من وحدات التحكم الإلكتروني وأجهزة الاستشعار مرتبطة بحوادث الاصطدام أو أنشطة القيادة.

4.9 النفاذ الآمن

يوصى بتعطيل السطوح البينية المستخدمة لتصحيح الأخطاء، مثل فريق عمل الاختبار المشترك (JTAG) على جهاز DSSAD/EDR، إذا لم تكن إلزامية للتشغيل الميداني، على ألا تتجاوز التشغيل الآمن. وتُصنَّف طرائق تعطيل السطوح البينية المتعلقة بالتصحيح على النحو التالي:

- حذفها بشكل دائم؛
- تعطيلها المشروط من خلال تطبيق التحكم في النفاذ.

وفي حالة إعادة تشغيل السطوح البينية المتعلقة بالتصحيح لأغراض تحليل الإعادة المضمونة، ينبغي ألا تكون السطوح البينية المتعلقة بالتصحيح متاحة إلا من جانب أطراف مخوَّلة ومستيقنة. ويوصَى بضرورة الحد من امتيازات التطبيقات التي تستقبل على السطوح البينية للعتاد والبرمجيات وفقاً لمبدأ "الامتياز الأدنى".

ويوصى بأن تُحمى الوظائف والبيانات الحساسة بالنسبة إلى الأمن، من خلال أوامر وطلبات تشخيص بواسطة آلية تجفير. وهذا يعني الاستيقان من الشخص الذي يرغب في النفاذ إلى جهاز DSSAD/EDR قبل إرسال الأوامر.

5.9 التحديث الآمن

يوصى بأن يضمن إجراء التحديث الخاص بالبرمجيات الثابتة والقواعد الاستيقان والسلامة، أي لا يُسمح إلا لرزم التحديث المستيقن منها وغير المعدلة بأن تُفعل. وإضافة إلى ذلك، يوصى بعدم تخفيض إصدار البرمجيات الثابتة والقواعد إلى النسخة السابقة لمنع استخدام الثغرات الأمنية السابقة بطريقة خبيثة. ويوصى أيضاً بإرسال الرزم عبر الأثير بواسطة قناة آمنة محمية بأساليب تجفير.

6.9 العلاقة بين التهديدات المحدَّدة ومتطلبات الأمن

يتضمن الجدول 3 التالي معلومات متعلقة بتقابل التهديدات المحددة في القسم 8 ومتطلبات الأمن.

الجدول 3 – العلاقة بين التهديدات المحدَّدة ومتطلبات الأمن

متطلبات الأمن	التهديدات	الأهداف الأمنية
بدء التشغيل الآمن	التلاعب بتدفق التحكم. – التلاعب بالبرمجيات الثابتة – التلاعب بقواعد المسجلات EDR/الأجهزة DSSAD	سلامة قواعد المسجلات EDR/الأجهزة DSSAD المخزنة في المركبات سلامة البرمجيات الثابتة للمسجلات EDR/الأجهزة DSSAD
السجل الآمن	التلاعب بتدفق التحكم. – التلاعب بالسجلات فقدان إمكانية اقتفاء أثر الحدث	سلامة بيانات المسجلات EDR/الأجهزة DSSAD في المركبات، سلامة السجل السحابي
الاتصالات المأمونة	التنصت التجسس من خلال التنصت التلاعب بتدفق التحكم هجوم الاعتراض هجوم انتحال الصفة هجوم التكرار هجوم رفض الخدمة	سرية و/أو سلامة حركة ناقلات البيانات سرية واستيقانية الاتصال مع الأنظمة الطرفية الخلفية تيسّر الأنظمة الطرفية الخلفية
النفاذ الآمن	النفاذ المادي	سرية و/أو استيقان الاتصالات مع وحدات التصحيح/التشخيص
التحديث الآمن	التنصت التلاعب بتدفق التحكم – التلاعب بقواعد المسجلات EDR/ الأجهزة DSSAD هجوم انتحال الصفة	سرية وسلامة الرزم المرسلة عبر الأثير

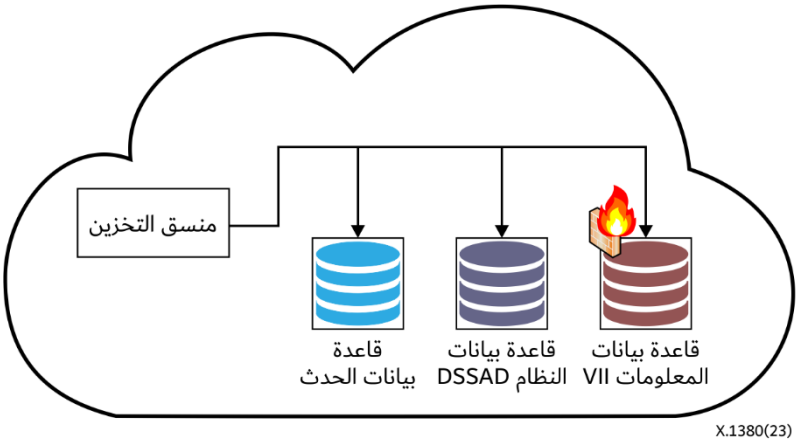
10 المبادئ التوجيهية لتنفيذ أنظمة مسجلات البيانات القائمة على الحوسبة السحابية

يجب أن تكون هناك حماية صارمة للبيانات عند استخدام وإدارة بيانات المسجلات EDR/الأنظمة DSSAD في أنظمة مسجلات البيانات القائمة على الحوسبة السحابية. كما تتضمن أنظمة مسجلات البيانات القائمة على الحوسبة السحابية وظيفة للبحث والتطوير كي تكون المركبات أكثر أماناً بفضل استخدام بيانات مسجلة لا تستطيع مسجلات البيانات التقليدية توفيرها. وتقدم هذه الفقرة المبادئ التوجيهية لتنفيذ نظام مسجل البيانات القائم على الحوسبة السحابية.

1.10 فصل أماكن التخزين السحابي

نظراً لضرورة وجود معلومات محدّدة لهوية المركبة في نظام DSSAD/EDR القائم على الحوسبة السحابية، يتعين توفير حماية آمنة لهذه المعلومات. ويلزم أن يكون هناك فصل مادي، في أنظمة DSSAD/EDR القائمة على الحوسبة السحابية، بين بيانات المسجلات EDR/الأنظمة DSSAD والمعلومات المحدّدة لهوية المركبة. وهذا لا يحقق فوائد أمنية فحسب، بل يتيح أيضاً وظائف إضافية مثل توفير بيانات المسجلات EDR/الأنظمة DSSAD لطرف ثالث دون أي انتهاك للخصوصية. وينبغي فصل التخزين مادياً، وإدارته

على نحو منفصل في أماكن تخزين مستقلة. ويتطلب تخزين المعلومات المحدّدة لهوية المركبة (ترد باسم "قاعدة بيانات المعلومات المحددة لهوية المركبة" في الشكل 15) مستوى أمن أعلى مما تتطلبه البيانات الأخرى نظراً لأهميتها النسبية.



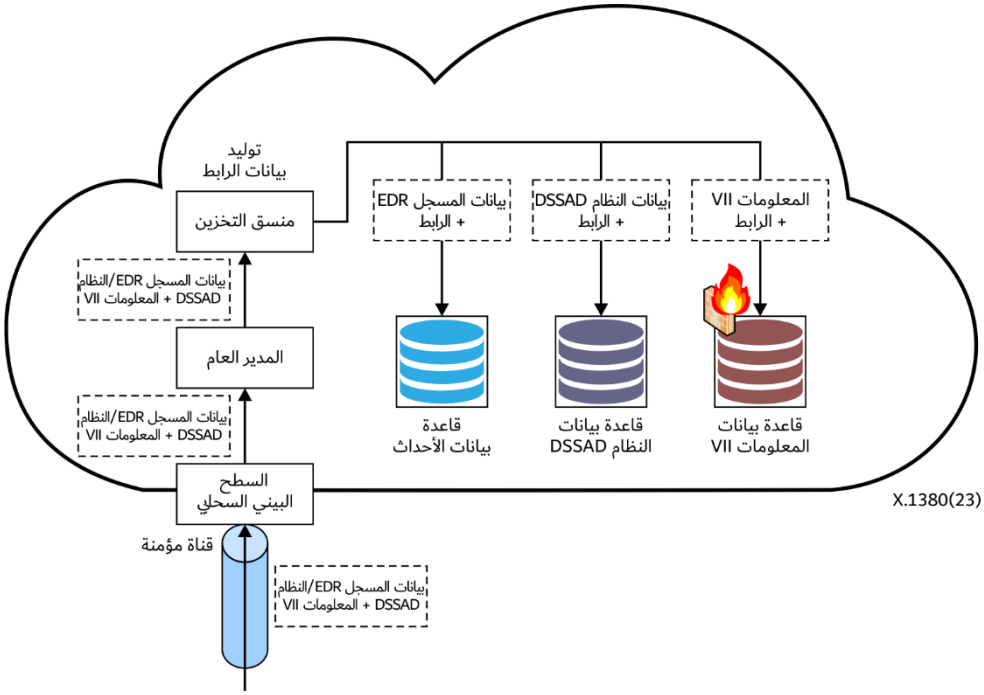
الشكل 15 – فضل أماكن التخزين

1.1.10 إجراء تخزين البيانات

لضمان سرية بيانات الاتصالات واستيقانيتها مع الطرف الخلفي، ينبغي إنشاء قناة آمنة مسبقاً قبل إرسال بيانات DSSAD/EDR من المركبة إلى النظام السحابي.

وعند إرسال البيانات من المركبة إلى منسّق التخزين عن طريق سطح بيني سحابي، يقوم منسّق التخزين بفصل بيانات DSSAD/EDR والمعلومات المحددة لهوية المركبة. وبعد الفصل، يقوم منسق التخزين بتوليد بيانات الرابط لجعل بيانات DSSAD/EDR مترابطة مع المعلومات المحددة لهوية المركبة. ثم يتم تخزين مجموعتين من البيانات في مخازن مختلفة (قواعد بيانات). وكما هو موضَّح في الشكل 16، تخزَّن المعلومات المحدّدة لهوية المركبة وبيانات DSSAD/EDR مع بيانات الرابط في قاعدة بيانات المعلومات المحددة لهوية المركبة وفي قاعدة بيانات الأحداث/النظام DSSAD وفقاً لذلك. وبعد إجراء التخزين، ينبغي تسجيل نتيجة عملية التخزين، سواء نجاح أو فشل إجراء تخزين البيانات.

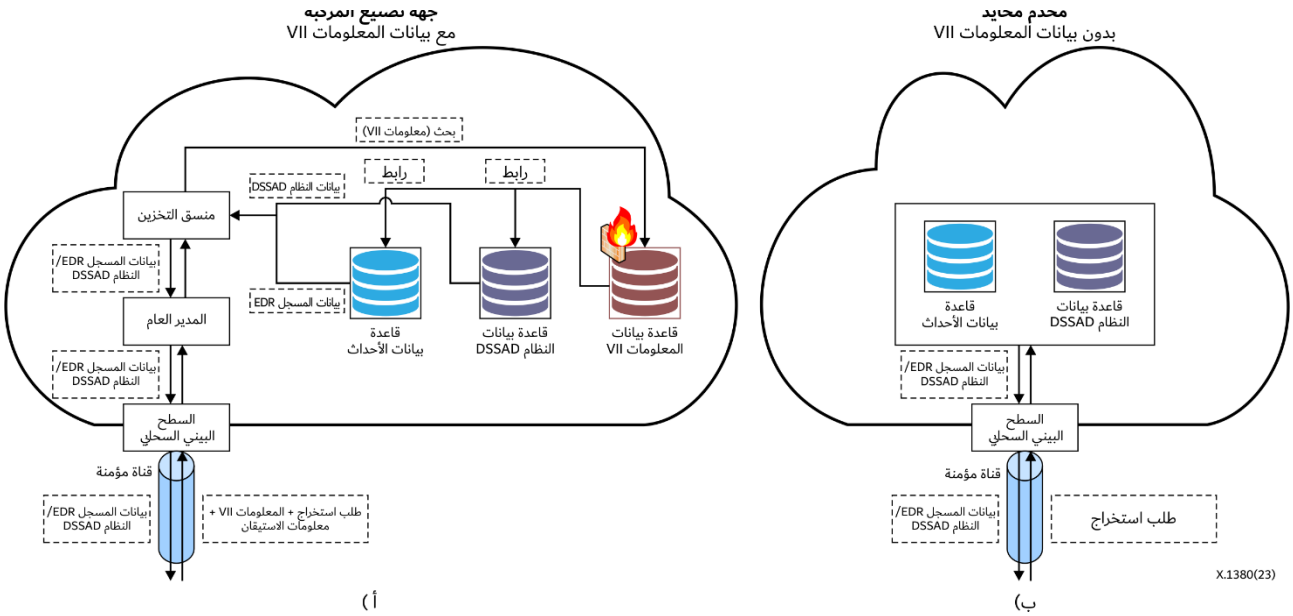
ومن أهم الأمور في إجراءات تخزين البيانات الامتثال للوائح ذات الصلة مثل اللائحة العامة لحماية البيانات (GDPR). ولذلك، يوصى بالحصول على موافقة صاحب البيانات قبل جمع أي بيانات من المركبة.



الشكل 16 – إجراء التخزين في إطار فصل أماكن التخزين

2.1.10 إجراء استخراج البيانات

يبدأ إجراء استخراج بيانات المسجلات EDR/الأنظمة DSSAD بطلب من المستعمل/الطرف الثالث لاستخراج بيانات المسجلات EDR/الأنظمة DSSAD. وعندما ينفذ المستعمل/الطرف الثالث إلى النظام السحابي، ينبغي أن يقوم السطحُ البيني السحابي بالاستيقان من هوية المستعمل/الطرف الثالث وأن يسجل جميع المحاولات. وإذا نجحت عملية الاستيقان، يستعمل منسقُ التخزين المعلومات المعروضة المحدّدة لهوية المركبة للعثور على بيانات الرابط في قاعدة بيانات المعلومات المحددة لهوية المركبة (راجع الشكل 17 (أ)). ويقوم منسق التخزين، بفضل بيانات الرابط التي عُثر عليها، بالبحث عن بيانات المسجلات EDR/الأنظمة DSSAD. وعند العثور على بيانات المسجلات EDR/الأنظمة DSSAD، يوفر منسق التخزين البيانات إلى الطرف الطالب بعد أن يتمايز إجراء التحكم في نفاذ المدير العام من حيث مستوى ترخيص الطرف الطالب. واستخراج بيانات المعلومات المحددة لهوية المركبة مسموح به على نحو مقيَّد ويتطلب سلطة عالية المستوى. ومن ناحية أخرى، فإن بيانات المسجلات EDR أو بيانات الأنظمة DSSAD التي لا تتضمن معلومات محددة لهوية المركبة يمكن أن يستخرجها الطرف الثالث. ويمكن استخراج بيانات المسجلات EDR أو بيانات الأنظمة DSSAD دون عملية البحث عن المعلومات المحددة لهوية المركبة، وذلك عندما تُحذف بيانات المعلومات المحددة لهوية المركبة وتُنقل إلى مخدم محايد منفصل (انظر الشكل 17 (ب)).

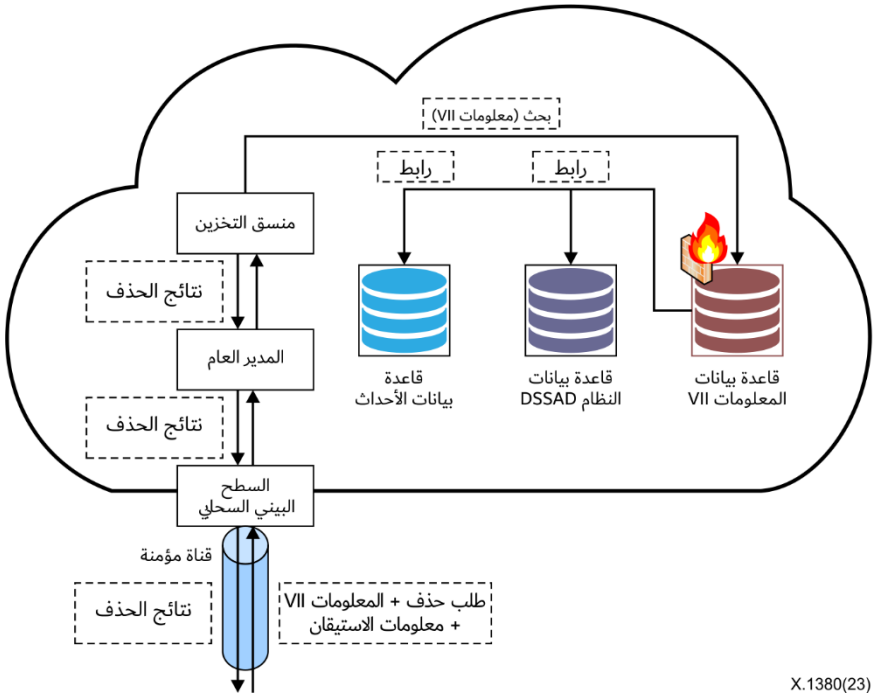


الشكل 17 – إجراء استخراج البيانات في إطار فصل أماكن التخزين

3.1.10 إجراء حذف البيانات

ينبغي أن يحصل النظام السحابي للمسجلات EDR/الأنظمة DSSAD على موافقة المستعمل بما في ذلك تاريخ انتهاء الصلاحية أو مدة البيانات المسجلة لبيانات المعلومات المجمعة المحددة لهوية المركبة. وعندما ينتهي تاريخ صلاحية البيانات المخزَّنة أو مدتها، ينبغي حذف البيانات المجمعة تلقائياً من النظام السحابي.

وعندما يطلب المستعملون حذف بياناتهم قبل تاريخ انتهاء الصلاحية، ينبغي للأنظمة السحابية أن تحذف البيانات بناء على طلبهم. وعندما يطلب المستعمل حذف البيانات، ينبغي أن يستيقن السطح البيني السحابي من هوية المستعمل ويسجل جميع المحاولات. وإذا نجحت عملية الاستيقان، ينبغي لمنسق التخزين أن يستعمل المعلومات المعروضة المحددة لهوية المركبة للعثور على بيانات الرابط التي جرى تخزينها في قاعدة بيانات المعلومات المحددة لهوية المركبة. وبواسطة بيانات الرابط التي تم العثور عليها، ينبغي لمنسق التخزين البحث عن بيانات المسجلات EDR/الأنظمة DSSAD وحذفها عند العثور عليها. وينبغي بعد ذلك أن يقوم منسق التخزين بتخزين السجل الخاص بنتيجة الحذف وبإبلاغ الطرف الطالب بالنتيجة.



الشكل 18 – إجراء الحذف في إطار فصل أماكن التخزين

2.10 تسجيل الخدمات السحابية

يبين الشكل 19 إجراء التسجيل الذي تتبعه مسجلات البيانات القائمة على الحوسبة السحابية في بيئات المركبات.

وبالإشارة إلى الشكل 19، إذا ورد طلب استيقان لتسجيل خدمة تسجيل لبيانات قائمة على الحوسبة السحابية، أي طلب استيقان مركبة، من مركبة في أسلوب تنفيذ خدمة في الخطوة 1، عندئذ ينبغي التحقق من معرّف هوية المركبة، وذلك مثلاً باستخدام خوارزمية توقيع رقمي لنظام تجفير مفتاح عمومي، في الخطوة 2. وهنا يمكن تنفيذ طلب الاستيقان من المركبة بإرسال رسالة موقعة بواسطة مفتاح خاص للمركبة إلى نظام خدمة تسجيل البيانات القائمة على الحوسبة السحابية. ونتيجة للتحقق في الخطوة 2، إذا تبين أن هوية المركبة غير صالحة، يقوم نظام خدمة تسجيل البيانات القائمة على الحوسبة السحابية بتوليد رد مقابل يفيد بفشل الاستيقان ويحيل هذا الردّ إلى المركبة كما هو مبيَّن في الخطوة 3.

ونتيجة للتحقق في الخطوة 2، إذا تبين أن هوية المركبة صالحة، يقوم نظام خدمة تسجيل البيانات القائمة على الحوسبة السحابية بتوليد رد استيقان للمركبة ويحيل هذا الردّ إلى المركبة كما هو مبيَّن في الخطوة 4.

وبعد ذلك، وعند استلام رد الاستيقان، أي أن استيقان المركبة قد تحقق، وبعد إدراج مدخلات المستخدم وتوليد معلومات تسجيل خدمة التسجيل القائمة على الحوسبة السحابية، بما في ذلك أنواع بيانات التسجيل وفترة الإبلاغ وغير ذلك، ترسل المركبة معلومات تسجيل خدمة تسجيل البيانات القائمة على الحوسبة السحابية إلى نظام خدمة تسجيل البيانات القائمة على الحوسبة السحابية، وبذلك تطلب تسجيل خدمة تسجيل البيانات القائمة على الحوسبة السحابية، كما هو مبيَّن في الخطوة 5.

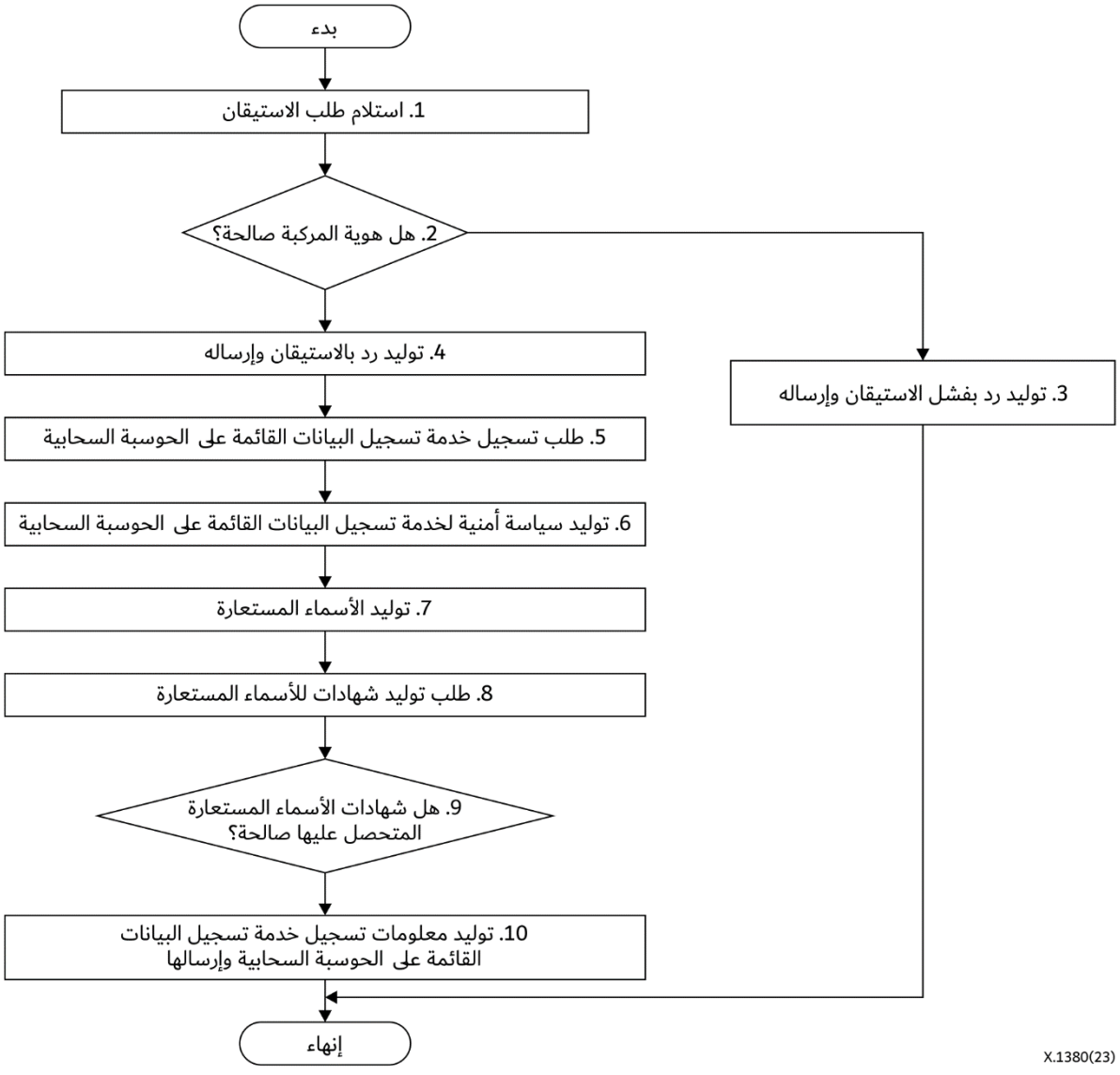
ومن ثم، إذا ورد طلب لتسجيل خدمة تسجيل البيانات القائمة على الحوسبة السحابية، يتضمن معلومات تسجيل خدمة تسجيل البيانات القائمة على الحوسبة السحابية، من المركبة، فإن نظام خدمة تسجيل البيانات القائمة على الحوسبة السحابية يولد سياسة أمنية باستخدام معلومات تسجيل خدمة تسجيل البيانات القائمة على الحوسبة السحابية، من قبيل أنواع بيانات التسجيل وفترة التسجيل، وهكذا، ثم يخزن/يسجل المعلومات كما هو مبيَّن في الخطوة 6.

وبعد ذلك، يخصص نظام خدمة تسجيل البيانات القائمة على الحوسبة السحابية اسماً مستعاراً لكل مركبة على النحو المبيَّن في الخطوة 7، ويقوم بتوليد رسالة طلب شهادة يطلب فيها توليد شهادة اسم مستعار للاسم المستعار المخصص لكل مركبة، ويرسل رسالة طلب الشهادة إلى مركز الاستيقان، كما هو مبيَّن في الخطوة 8.

ويراقب نظام خدمة تسجيل البيانات القائمة على الحوسبة السحابية ما إذا قد تم الحصول على شهادة اسم مستعار أم لا من مركز الاستيقان في الخطوة 9. ونتيجة لهذه المراقبة، إذا تم الحصول على شهادة الاسم المستعار، يعمد نظام خدمة تسجيل البيانات القائمة على الحوسبة السحابية إلى تخزين شهادة الاسم المستعار في قاعدة بيانات معلومات تسجيل البيانات القائمة على الحوسبة السحابية. وقد تكون شهادة الاسم المستعار رسالة موقعة رقمياً من مركز الاستيقان. ومن الممكن ضمان تبرير الاسم المستعار من خلال شهادة الاسم المستعار.

ومن الممكن تخصيص عدد كبير من الأسماء المستعارة لكل مركبة. وبما أن الاسم المستعار لا يحتوي على معلومات مرتبطة بمعرّف هوية كل مركبة، يمكن حماية المعلومات المحدِّدة لهوية الأشخاص لكل مركبة.

وإذا تم استلام الإخطار بذلك، يقوم نظام خدمة تسجيل البيانات القائمة على الحوسبة السحابية بتوليد معلومات تسجيل خدمة تسجيل البيانات القائمة على الحوسبة السحابية لكل مركبة، ويخزنها في قاعدة بيانات، ويرسلها إلى كل مركبة في الخطوة 10. وهنا قد تتضمن معلومات تسجيل خدمة تسجيل البيانات القائمة على الحوسبة السحابية الاسم المستعار المخصص لكل مركبة وشهادة الاسم المستعار وما إلى ذلك. ويمكن لكل مركبة، أي مستخدم المركبة، في خدمة تسجيل البيانات القائمة على الحوسبة السحابية التي جرى تسجيلها أن تقوم بتسجيل للبيانات قائم على الحوسبة السحابية بإجراء اتصالات بين المركز السحابي والمركبات باستخدام معلومات تسجيل خدمة تسجيل البيانات القائمة على الحوسبة السحابية الواردة من نظام خدمة تسجيل البيانات القائمة على الحوسبة السحابية.

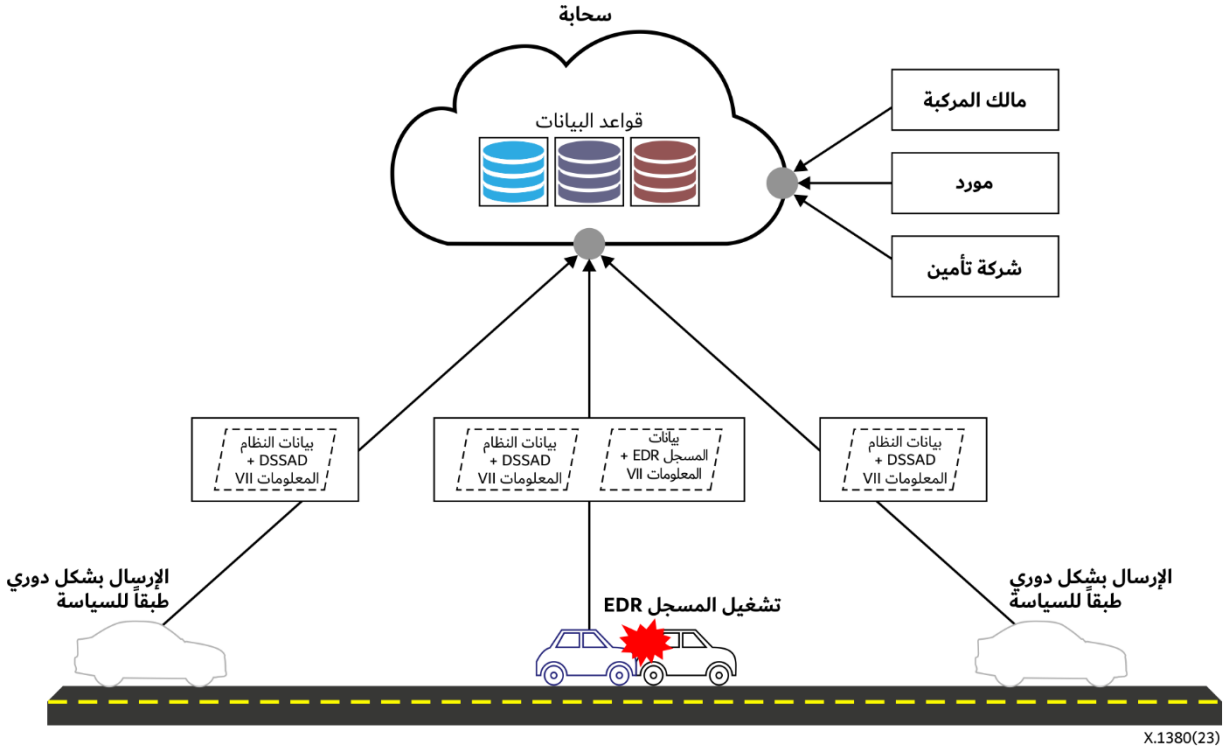


الشكل 19 – تسجيل خدمة تسجيل البيانات القائمة على الحوسبة السحابية

يمكن النظر في إجراء إلغاء تسجيل مسجلات البيانات القائمة على الحوسبة السحابية في حالات استعمال مثل تأجير السيارات والمركبات المستعملة، وما إلى ذلك، لأن مالكي السيارات المتغيرين لا يرغبون في تزويد النظام السحابي ببيانات المسجلات EDR/الأنظمة DSSAD.

11 حالات استعمال مسجلات البيانات القائمة على الحوسبة السحابية في بيئة السيارات

عندما يقع حادث سيارة، يمكن استخدام بيانات المسجلات EDR/الأنظمة DSSAD بشكل فعّال لتحليل سبب الحادث ولتحديد ما إذا كانت المركبة هي المسؤولة عن الحادث أو السائق. ويبين الشكل 20 تدفق بيانات المسجلات EDR/الأنظمة DSSAD. فتُنقل بيانات المسجلات EDR/الأنظمة DSSAD المتولدة في المركبة إلى السحابة من خلال الاتصالات اللاسلكية. ويمكن لصاحب مركبة أو مصنّع أو مورّد أو أي أطراف ثالثة مخوّلة (مثل شركات التأمين) استعمال بيانات المسجلات EDR/الأنظمة DSSAD المتوافرة في السحابة.



الشكل 20 – تدفق بيانات المسجلات EDR/الأنظمة DSSAD

يتمتّع نظام مسجلات البيانات القائمة على الحوسبة السحابية بالعديد من المزايا. أولاً، يَسْهل الحصول على بيانات المسجلات EDR/الأنظمة DSSAD، حتى في حالات المخاطر المحتملة (مثل حريق المركبة وغرقها). ثانياً، يمكن لمحللي الحوادث المخوّلين الحصول على بيانات من نظام الحوسبة السحابية بسهولة أكبر من الحصول عليها من وحدات التحكم الإلكتروني في السيارة مباشرة.

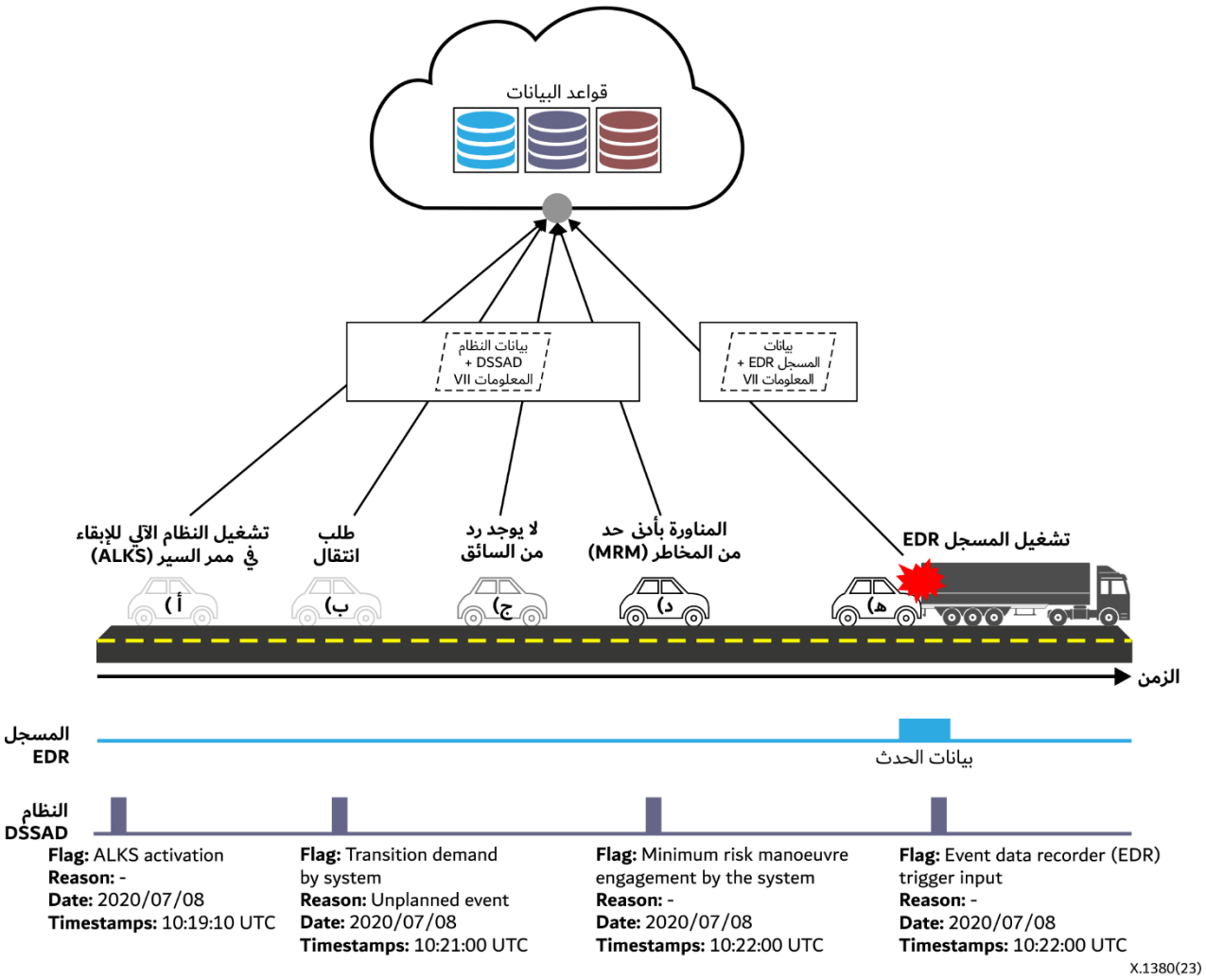
1.11 الحالة 1: حادث اصطدام بين مركبتين

يبيّن الشكل 21 سيناريو تُعرض أحداثه بترتيبها الزمني وتسير فيه على الطريق مركبة مجهَّزة بنظام آلي للإبقاء في ممر السير. ويقع حادث سيارة في اللحظة (هـ) ويُطلَق حدث لمسجل بيانات الأحداث (EDR). وتقوم السحابة بتخزين بيانات المسجلات EDR/الأنظمة DSSAD ابتداء من (أ) لحظة تشغيل النظام الآلي للإبقاء في ممر السير، حتى (هـ) لحظة وقوع الحادث. وتقدّم بيانات المسجلات EDR/الأنظمة DSSAD المخزَّنة المعلومات التالية:

نظراً إلى أن سائق المركبة هو الذي قام بتشغيل النظام الآلي للإبقاء في ممر السير عند الساعة 10:19:10، يتم تسليم النظام عملية التحكم في المركبة. وبعد دقيقة واحدة و50 ثانية، تسوء حالة الطقس ويطلب النظام الآلي للإبقاء في ممر السير من السائق نقل

التحكم في المركبة، ولكن السائق لا يجيب. ويجري بالتالي النظام الآلي للإبقاء في ممر السير، تلقائياً، مناورة بأدنى حد من المخاطر (MRM) عند الساعة 10:22:00. ثم يقع الاصطدام في الساعة 10:22:30.

ومن خلال تحليل بيانات المسجلات EDR/الأنظمة DSSAD، يمكن التحقق من فترة الحادث وظروفه. وتقوم أنظمة مسجلات البيانات القائمة على الحوسبة السحابية بتخزين بيانات المسجلات EDR/الأنظمة DSSAD في مخزن بالنظام السحابي بموجب سياسات محددة مسبقاً لنقل البيانات. وبالتالي، يخفّف ذلك من الجهود المبذولة لجمع المعلومات المتعلقة بحادث الاصطدام مقارنة بالاستخراج المباشر من مخزن مسجل بيانات الأحداث (EDR) في المركبة.



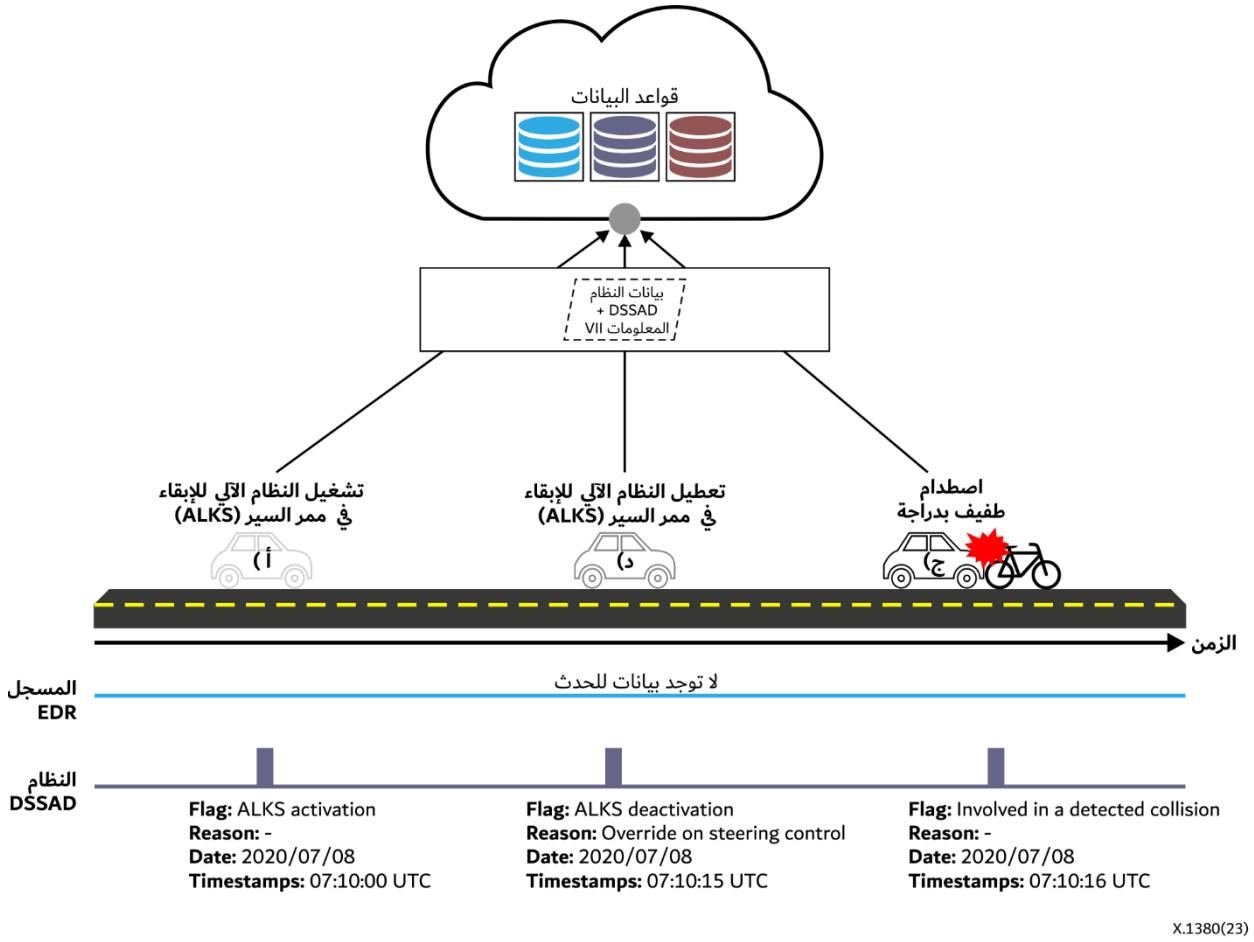
الشكل 21 – حادث اصطدام بين مركبات

2.11 الحالة 2: حادث اصطدام بين مركبة ودراجة

يبيّن الشكل 22 سيناريو تُعرض أحداثه بترتيبها الزمني وتسير فيه على الطريق مركبة مجهَّزة بنظام آلي للإبقاء في ممر السير. وتصطدم المركبة بشكل طفيف بدراجة في اللحظة (ج)، ولكن نظراً إلى خفّة الاصطدام لم يُشغل مسجل بيانات الأحداث (EDR). بيد أن جميع بيانات النظام DSSAD الحديثة تحمَّل على السحابة. وتقدّم بيانات المسجلات EDR/الأنظمة DSSAD المخزَّنة المعلومات التالية:

يقوم السائق بتشغيل النظام الآلي للإبقاء في ممر السير عند الساعة 10:19:10. وبعد 15 ثانية يشغّل السائق مباشرةً عجلة القيادة ثم يعطِّل النظام الآلي للإبقاء في ممر السير. ويقع الاصطدام بين المركبة والدراجة في الساعة 07:10:16.

وفي هذه الحالة، يكون الوقع على المركبة طفيفاً بحيث لا تُستوفى الشروط اللازمة لتشغيل مسجل بيانات الأحداث ولا يتم جمع أي بيانات للمسجل EDR. ومع ذلك، يمكن إجراء محاكاة لحالة الحادث بصورة مفصلة، وتحليلها بسهولة نظراً لوجود بيانات النظام DSSAD مخزَّنة في النظام السحابي.



الشكل 22 – حادث اصطدام بين مركبة ودراجة

التذييل I

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

مثال على مجموعة البيانات في مسجل بيانات الأحداث التقليدي

يُعدّ المثال على مجموعة البيانات هذه عنصراً أساسياً لازماً لمسجلات بيانات الأحداث التقليدية في الولايات المتحدة الأمريكية (USA)، التي تنظمها الإدارة الوطنية للسلامة على الطرق السريعة (NHTSA).

الجدول 1.I – عناصر البيانات الأساسية اللازمة في مسجل بيانات الأحداث التقليدي [b-NHTSA EDR]

رقم البند	عناصر البيانات	زمن التسجيل*	معدل الاعتيان	المدى	الدقة	الاستبانة
1	التغير في السرعة، طولياً	0 ms 250-0 أو إلى نهاية الحدث + 30 ms، أيهما أقصر	s/100	100– إلى 100 km/h	± 10%	1 km/h
2	التغير الأقصى في السرعة، طولياً	0 ms 300-0 أو إلى نهاية الحدث + 30 ms، أيهما أقصر	لا ينطبق	100– إلى 100 km/h	± 10%	1 km/h
3	الزمن، التغير الأقصى في السرعة، طولياً	0 ms 300-0 أو إلى نهاية الحدث + 30 ms، أيهما أقصر	لا ينطبق	0 ms 300-0 أو إلى نهاية الحدث + 30 ms، أيهما أقصر	± 3 ms	2,5 ms
4	السرعة، كما تبينها المركبة	0 s إلى 5,0–	s/2	0-200 km/h	± 1 km/h	1 km/h
5	كبح المحرك، نسبة مئوية من الكبح الكامل (دواسة الوقود، نسبة مئوية من الضغط الكامل)	0 s إلى 5,0–	s/2	0-100%	± 5%	1%
6	توقف الخدمة، تشغيل/إيقاف	0 s إلى 5,0–	s/2	تشغيل/إيقاف	لا ينطبق	تشغيل/إيقاف
7	دورة الاشتعال، اصطدام	0 s 1,0–	لا ينطبق	0-60 000	± 1 دورة	1 دورة
8	دورة الاشتعال، تنزيل	عند التنزيل	لا ينطبق	0-60 000	± 1 دورة	1 دورة
9	حالة حزام الأمان، السائق	0 s 1,0–	لا ينطبق	تشغيل/إيقاف	لا ينطبق	تشغيل/إيقاف
10	مصباح إنذار وسادة الأمان الأمامية	0 s 1,0–	لا ينطبق	تشغيل/إيقاف	لا ينطبق	تشغيل/إيقاف
11	زمن نشر وسادة الأمان الأمامية، السائق (المرحلة الأولي، في حالة وسائد الأمان متعددة المراحل)	حدث	لا ينطبق	0-250 ms	± 2 ms	1 ms
12	زمن نشر وسادة الأمان الأمامية، الراكب بجوار السائق (المرحلة الأولي، في حالة وسائد الأمان متعددة المراحل)	حدث	لا ينطبق	0-250 ms	± 2 ms	1 ms
13	تعدد الأحداث، عدد الأحداث (1 أو 2)	حدث	لا ينطبق	1، 2	لا ينطبق	1، 2
14	المدة بين الحدثين 1 و2	حسب المطلوب	لا ينطبق	0-5,0 s	0,1 s	0,1 s
15	تسجيل ملف كامل (نعم أم لا)	حسب البيانات الأخرى	لا ينطبق	نعم/لا	لا ينطبق	نعم/لا

بيبليوغرافيا

[b-ITU-T X.641] Recommendation ITU-T X.641 (1997), *Information technology – Quality of service: framework*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2021), *Baseline identity management terms and definitions*.

[b-ISO/IEC 27000] ISO/IEC 27000:2018(en), *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-UN R157] UN Regulation No. 157, *Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems*.

[b-UN R160] Addendum 159 – UN Regulation No. 160, *Uniform provisions concerning the approval of motor vehicles with regard to the Event Data Recorder*.

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

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2023