国际电信联盟
电信标准化部门

建议书

ITU-T X.1380 (03/2023)

X系列: 数据网络、开放系统通信和安全

安全应用和服务（2） – 智能交通系统（ITS）安全

汽车环境中基于云的事件数据记录器的安全指南

ITU-T X 系列建议书

数据网络、开放系统通信和安全

公用数据网	X.1 – X.199
开放系统互连	X.200 – X.299
网间互通	X.300 – X.399
消息处理系统	X.400 – X.499
号码簿	X.500 – X.599
OSI组网和系统概貌	X.600 – X.699
OSI管理	X.700 – X.799
安全	X.800 – X.849
OSI应用	X.850 – X.899
开放分布式处理	X.900 – X.999
信息和网络安全	
一般安全问题	X.1000 – X.1029
网络安全	X.1030 – X.1049
安全管理	X.1050 – X.1069
生物测定	X.1080 – X.1099
安全应用和服务（1）	
组播安全	X.1100 – X.1109
家庭网络安全	X.1110 – X.1119
移动安全	X.1120 – X.1139
网页安全	X.1140 – X.1149
安全协议（1）	X.1150 – X.1159
对等网络安全	X.1160 – X.1169
网络身份安全	X.1170 – X.1179
IPTV安全	X.1180 – X.1199
网络空间安全	
网络安全	X.1200 – X.1229
反垃圾信息	X.1230 – X.1249
身份管理	X.1250 – X.1279
安全应用和服务（2）	
应急通信	X.1300 – X.1309
泛在传感器网络安全	X.1310 – X.1319
智能电网安全	X.1330 – X.1339
验证邮件	X.1340 – X.1349
物联网（IoT）安全	X.1360 – X.1369
智能交通系统（ITS）安全	**X.1370 – X.1389**
分布式账簿技术安全	X.1400 – X.1429
分布式账簿技术安全	X.1430 – X.1449
安全协议（2）	X.1450 – X.1459
网络安全信息交换	
网络安全概述	X.1500 – X.1519
漏洞/状态信息交换	X.1520 – X.1539
事件/事故/启发式信息交换	X.1540 – X.1549
策略的交换	X.1550 – X.1559
启发式和信息请求	X.1560 – X.1569
标识和发现	X.1570 – X.1579
确保交换	X.1580 – X.1589
云计算安全	
云计算安全概述	X.1600 – X.1601
云计算安全设计	X.1602 – X.1639
云计算安全最佳做法和指导原则	X.1640 – X.1659
云计算安全实施方案	X.1660 – X.1679
其他云计算安全	X.1680 – X.1699
量子通信	
术语	X.1700 – X.1701
量子随机数发生器	X.1702 – X.1709
QKDN安全框架	X.1710 – X.1711
QKDN安全设计	X.1712 – X.1719
QKDN安全技术	X.1720 – X.1729
数据安全	
大数据安全	X.1750 – X.1759
5G 安全	X.1800 – X.1819

欲了解更详细信息，请查阅 ITU-T 建议书目录。

ITU-T X.1380 建议书

汽车环境中基于云的事件数据记录器的安全指南

摘要

事件数据记录器（EDR）是安装在汽车道路车辆中的最重要组成部分之一，用于在碰撞期间记录车辆状态、车辆运动和用户输入。通过分析事件数据，可以了解碰撞的原因，并最终用于提高汽车环境的安全性。用于自动驾驶的数据存储系统也是记录数据的一个重要组成部分，这些数据将给出驾驶者与自动驾驶系统之间交互的清晰画面。然而，传统的事件数据记录器在本地记录和管理全部数据，这样，数据可能受到丢失和破坏的威胁。

云计算被认为是自我服务供应和按需管理情况下促成网络获取一系列可伸缩且富有弹性、可共享物理或虚拟资源的重要手段。航空业等行业已经在尝试将云服务应用于事件数据记录系统，以提高航空环境的安全性。根据车辆之间连接的当前趋势，将实施用于自动驾驶的EDR和数据存储系统，以提高其整体安全性。然而，根据汽车环境的独特特性，它们在采集、传输、存储、管理和使用所记录数据的过程中具有各种漏洞。因此，有必要研究汽车环境中基于云的数据记录器的这些漏洞、安全要求和用例。

ITU-T X.1380建议书为汽车环境中基于云的数据记录器提供了安全指南。它描述了汽车环境中基于云的数据记录器的威胁、漏洞、安全要求和用例。

历史沿革

版本	建议书	批准时间	研究组	唯一 ID*
1.0	ITU-T X.1380	2023-03-03	17	11.1002/1000/15106

关键词

云，基于云的自动驾驶数据存储系统（DSSAD），基于云的事件数据记录器（EDR），数据记录器，DSSAD，EDR，安全要求，安全威胁。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一ID，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联已收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

© 国际电联 2023

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

ITU-T X.1380 建议书

汽车环境中基于云的事件数据记录器的安全指南

1 范围

本建议书为基于云的数据记录器提供了安全指南，例如，汽车环境中的事件数据记录器（EDR）和自动驾驶数据存储系统（DSSAD）。本建议书包括有关数据记录系统、EDR和DSSAD的技术方面考虑。此外，本建议书草案还提供了安全要求和用例。

2 参考文件

下列ITU-T建议书和其他参考文件的条款，通过在本文本中的引用而构成当前建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文件均面临修订；因此鼓励本建议书的使用者探讨使用下列建议书和其他参考文件最新版本的可能性。当前有效的ITT-T建议书清单定期出版。

在本建议书中引用某个独立文件时，并未给予该文件建议书的地位。

[ITU-T X.1371] ITU-T X.1371 (2020)建议书，联网车辆面临的安全威胁。

3 定义

3.1 他处定义的术语

本建议书使用了下列他处定义的术语：

3.1.1 认证（authentication）[b-ITU-T X.1252]：验证的正式过程，如果成功，将为某实体产生一个经认证的身份。

3.1.2 自动车道保持系统（automated lane keeping system）[b-UN R157]：由驾驶者启动并使车辆保持在其车道内的系统。

3.1.3 授权（authorization）[b-ITU-T X.800]：授予权限，包括授予基于访问权限进行访问的权限。

3.1.4 可用性（availability）[b-ITU-T X.800]：经授权实体一旦需要即可访问和使用的特性。

3.1.5 真实性（authenticity）[b-ITU-T X.641]：保护相互认证和数据来源认证。

3.1.6 可核查性（accountability）[b-ITU-T X.800]：确保实体的行动可被唯一地追溯至该实体的特性。

3.1.7 机密性（confidentiality）[b-ITU-T X.800]：使信息不泄漏给未经授权个人、实体或过程或者不使信息为其利用的特性。

3.1.8 自动驾驶数据存储系统（DSSAD）[b-UN R157]：能够确定自动车道保持系统（ALKS）与人类驾驶者之间交互的系统。

3.1.9 事件数据记录器（EDR）[b-UN R160]：车辆中的一种设备或功能，负责记录事件发生前一段时间内（如车速与时间）或碰撞事件期间（如加速度与时间）的车辆动态、时序数据，以供碰撞事件后检索。就本定义而言，事件数据不包括音频和视频数据。

3.1.10 数据完整性（data integrity）[b-ITU-T X.800]：数据未被以未授权方式修改或破坏的特性。

3.1.11 威胁（threat）[b-ISO/IEC 27000]：可能对某个系统或组织造成伤害的有害事件的潜在起因。

3.2 本建议书中定义的术语

本建议书定义了下列术语：

3.2.1 云接口（cloud interface）：云系统的一个网关，是云系统与车辆、用户、第三方之间的通信接口。

3.2.2 通用管理器（general manager）：云系统的一个组成部分，负责管理存储和检索事件数据记录器（EDR）/自动驾驶数据存储系统（DSSAD）数据的基本程序，并负责验证来自用户、第三方或车辆之请求的基本要求。

3.2.3 中立服务器（neutral server）：来自车辆制造商的独立服务器，可以提供匿名或车辆可识别信息（VII）或VII删去的事件数据记录器（EDR）/自动驾驶数据存储系统（DSSAD）数据。

3.2.4 规则/策略管理器（rule/policy manager）：云系统的一个组成部分，负责更新规则/策略，是通用管理器的一部分。

3.2.5 存储协调器（storage coordinator）：云系统的一个组成部分，负责将事件数据记录器（EDR）/自动驾驶数据存储系统（DSSAD）数据和车辆可识别信息（VII）数据分开，按照预先确定的策略在云存储中存储和检索数据。

4 缩写词和首字母缩略语

本建议书使用了下列缩写词和首字母缩略语：

ALKS 自动车道保持系统
API 应用程序编程接口
CAN 控制器局域网
DoS 拒绝服务
DSSAD 自动驾驶数据存储系统
ECU 电子控制单元
EDR 事件数据记录器
FIFO 先进先出
GDPR 通用数据保护条例
IVN 车载网络
JTAG 联合测试行动小组
MAC 消息认证代码
MRM 最低风险策略
OBD 车载诊断
OTA 无线传送
PII 个人可识别信息

TLS 传输层安全性

UDS 统一诊断服务

V2X 车辆对一切

VII 车辆可识别信息

VIN 车辆识别号

5 惯例

本建议书使用下列惯例：

关键词**“要求”**表示一项必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与该要求有任何偏差。

关键词**“建议”**表示一项建议的、并非需要绝对遵守的要求，因此，声称遵守本建议书并不需要存在本要求。

6 基于云的数据记录器系统

6.1 基于云的事件数据记录器系统

基于云的EDR是一种连接到云系统（后端服务器）的EDR，用于提高联网和自动驾驶汽车环境中EDR数据的可及性和安全性。

EDR是一种安装在当今大多数汽车中的设备，用于记录与车辆碰撞或事故相关的信息，以提高车辆环境中的安全性和生活质量。

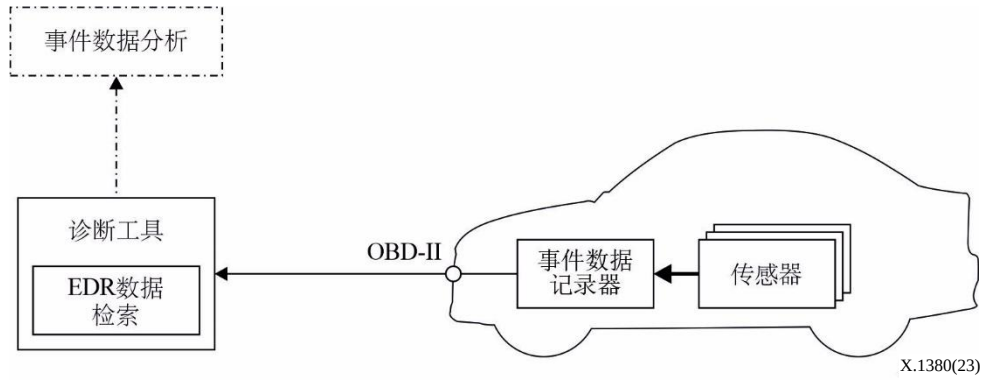

图1 – 传统的汽车EDR

如图1所示，当出现车辆状态满足特定条件的事件时，例如，正面气囊爆开、超过加速/减速阈值、翻车等，传统的EDR被触发。当EDR被触发时，EDR从传感器采集预先确定的数据集，然后将数据存储在其具有非易失性存储器的内部存储器中。数据实际上是从触发时间的−5秒（通常称为T0）到触发时间的+500毫秒记录的。“−5秒”和“+500毫秒”因国家法规或车辆制造商而异。

通常，EDR能够在车辆上存储多个事件。当存储器被过去的事件数据填满时，最旧的数据被新近更新的数据覆盖。在气囊爆开等特殊事件中，传统的EDR会存储采集到的数据，并锁定数据存储以防止数据被操纵或覆盖。

所存储数据由诊断工具或指定的检索工具通过车载诊断（OBD）-II端口来检索，并用于分析碰撞或事故。收集的最小数据集由国家车辆法规或车辆制造商的设计决定。此外，所记

录事件数据的数据格式通常因每个车辆制造商而异，并且通常因车辆型号而异。因此，当检索和分析事件数据时，需要专门的检索软件。

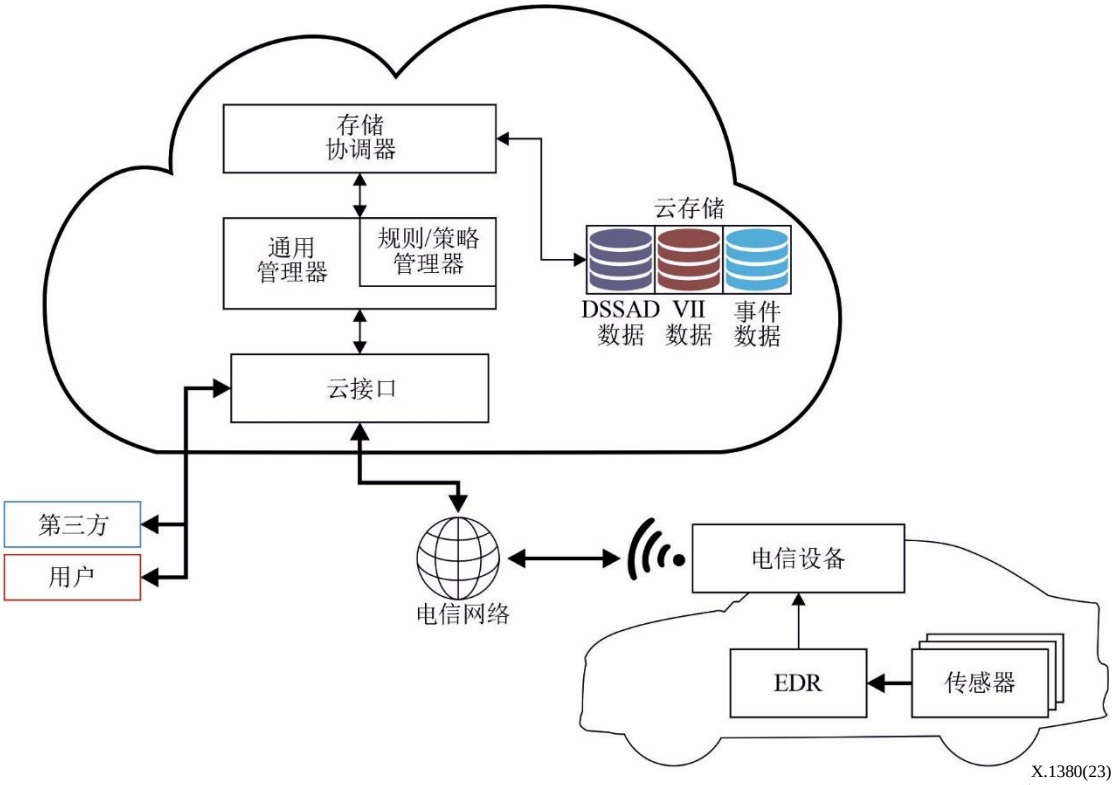

图2 – 基于云的EDR

图2中描述的基于云的EDR通过连接到EDR的一个电信设备来将事件数据存储于云系统上。

由于传统的EDR与基于云的EDR之间在系统和环境方面的差异，记录数据集可能不同于传统的EDR数据集。此外，可添加来自用于管理自动驾驶的电子控制单元（ECU）的新型数据，因为这是有助于分析自动驾驶车辆事故的关键数据。

与传统的EDR将新事件数据覆盖于未锁定的事件数据上不同，基于云的EDR可以在云存储上记录事件数据，而不覆盖数据。因此，基于云的EDR可以具有车辆的完整记录数据而不被删除。这是基于云的EDR的最大好处之一，使用完整的EDR数据极大地帮助了道路安全研究。

如果任何一方通过适当过程和授权来请求EDR数据，那么云服务中采集和存储的EDR数据应可供用户或第三方使用。在向各方传送所请求的EDR数据时，应该有一个认证过程来验证请求的有效性。

除了存储和提供EDR数据的功能之外，基于云的EDR还在系统上提供规则/策略更新。任何用户或第三方都可以请求更新车辆中EDR设备的规则/策略以及云系统上的相关策略。该请求将需要比任何普通的存储和检索程序更高的权限和安全性验证。

在图2中基于云的EDR系统中，云系统内的各实体被定义为在基于云的EDR的功能之上运行。云接口是云系统的一个网关，保存指定访问的日志。通用管理器负责管理存储和检索EDR数据的基本程序。它验证来自用户/第三方或车辆的请求的基本要求，还在规则/策略嵌入式管理器的帮助下执行规则/策略更新。存储协调器使用预先确定的策略来存储和检索事

件数据。该策略可能包括因请求者的权限而屏蔽从云存储器处检索的EDR数据。它还可能包括有关在云存储器上存储和检索EDR数据的过程的方法。

6.2 用于自动驾驶的基于云的数据存储系统

自动驾驶数据存储系统（DSSAD）是一个旨在通过存储一组数据来揭示谁请求驾驶和谁正在驾驶（可以有所不同，尤其是在转换程序期间）的系统，这些数据提供了驾驶者与自动驾驶系统之间交互的清晰画面。DSSAD已在[b-UN R157]中得到认可。该法规认可DSSAD是自动驾驶车辆的一项要求。

DSSAD存储诸如自动驾驶系统激活、停用、转换要求、紧急操作等信息。当自动系统的状态被停用或需要转换时，状态改变的原因被存储在DSSAD中。利益攸关方可以通过分析记录自动系统与驾驶者之间交互情况的DSSAD数据，来明确是谁请求驾驶以及是谁负责实际驾驶。

图3中描述的基于云的DSSAD通过连接到DSSAD的一个通信设备来将DSSAD数据存储于云系统上。将DSSAD数据传送到云系统的过程与有关基于云的EDR的过程相同。不同之处在于发送的是DSSAD数据，而不是EDR数据。DSSAD定期将DSSAD数据传输到云系统。因此，DSSAD可以灵活地应对因DSSAD存储器的局限性而导致的问题。

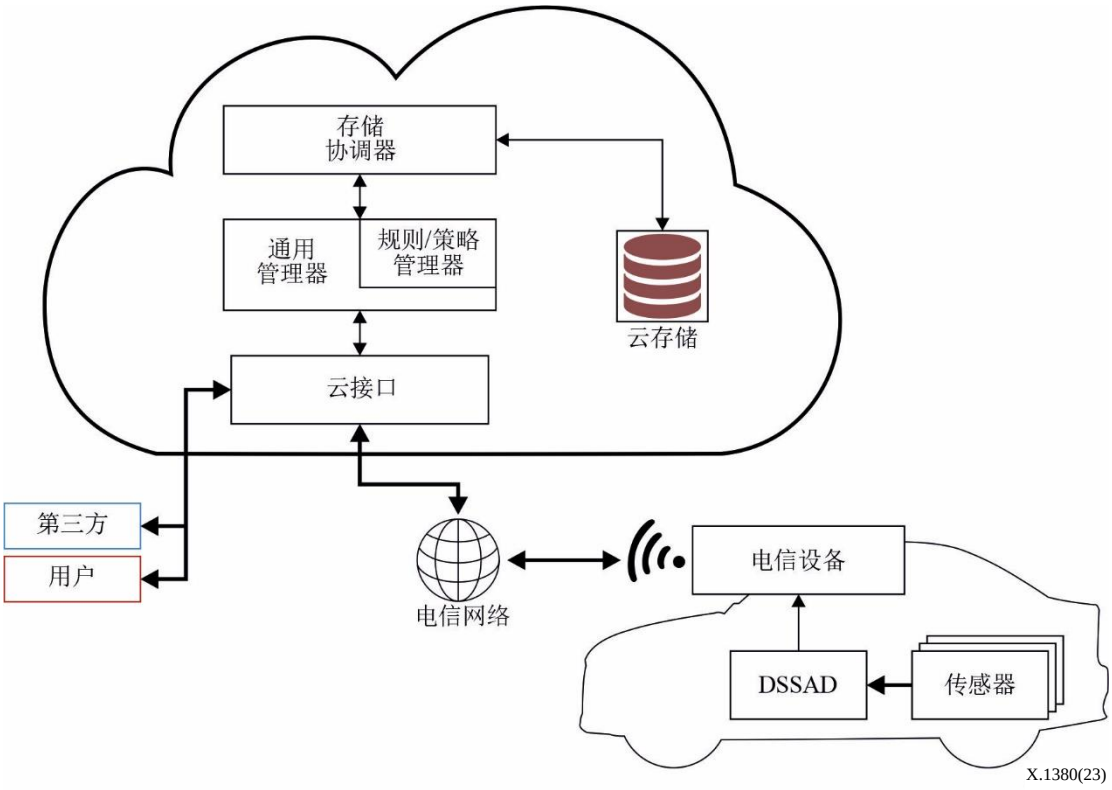

图3 – 基于云的DSSAD

6.3 EDR与DSSAD的比较

EDR与DSSAD之间的比较如表1所示。

表1 – EDR和DSSAD的比较

	EDR	DSSAD
目的	事故分析和重建	澄清车辆在特定时间的责任；请求谁开车，以及谁负责开车
触发条件	事件（如碰撞）：导致达到触发阈值的物理事件	交互：改变系统运行状态，或者要求改变系统运行状态
采集的数据	与碰撞分析相关的预先确定的数据集	与车辆控制和责任相关的预先确定的数据集
存储时间	触发时（瞬间）记录数据	在整个驾驶过程中记录数据
上载时机	每次存储时，点火开/关	

7 基于云的数据记录器系统设计

7.1 EDR的数据管理

EDR的目的是存储有关特定事件的车辆信息，如安全气囊爆开。EDR中记录的数据用于碰撞分析和事件重建。因此，EDR记录事件发生的时间和事件发生时的车辆状态。

7.1.1 事件数据的记录时间

图4描述了EDR如何记录事件。当EDR检测到某特定事件时，EDR将事件发生时间设为特定于已发生事件的T_0，然后在预先确定的记录时间段（预先定义的持续时间）采集指定的数据。T_0^n表示第n个事件的发生时间。由于每种类型的事件具有不同的触发条件，因此根据事件的类型，记录时间段可能不同。T_{pre}表示特定事件之前的时间。T_{post}表示特定事件之后的时间。时间段可以描述为$[(T_0 - T_{pre}) \sim (T_0 + T_{post})]$。

在多个事件相继发生的情况下，如图4所示，EDR记录EDR数据，而不考虑重叠的时间段。图4 (a)显示了有关非重叠事件的记录时间段。图4(b)显示了有关重叠事件的记录时间段。

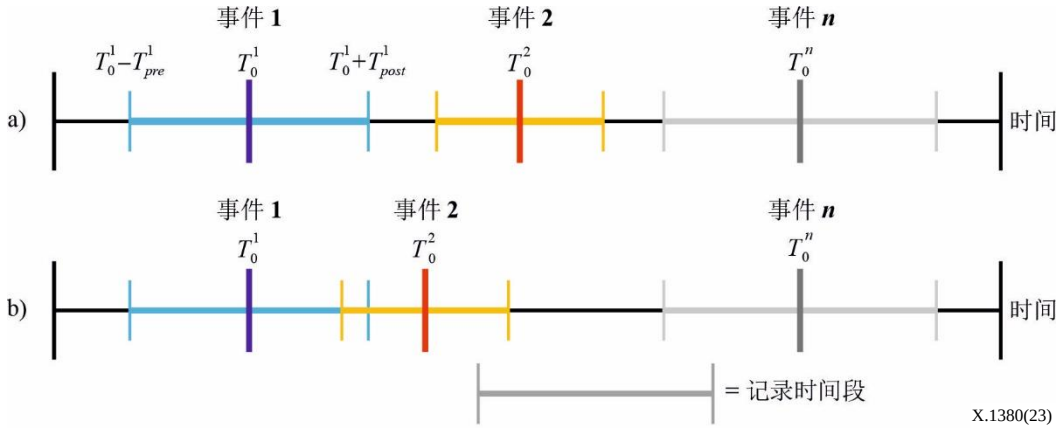

图4 – 记录EDR的时间段：（a）非重叠事件；（b）重叠事件

7.1.2 车辆存储器中的数据锁定

对EDR数据有几种车载存储设备。由于预先确定的条件是多样的，因此可以有多个事件相继发生。EDR的存储过程遵循先进先出（FIFO）程序。如果所有的EDR存储器已被先前的事件填满，那么新的事件数据会覆盖最旧的事件数据。然而，一些预先确定的事件触发条

件，如正面气囊爆开，需要在写入所记录的数据之后锁定数据存储器，从而使所存储的数据不能被覆盖。图5显示了拥有两个存储器的EDR记录程序的例子。图5（a）显示了无数据锁定条件下后续事件的数据存储过程，显示事件3覆盖带有最旧事件数据的存储器。另一方面，图（b）和图（c）显示了有数据锁定条件下后续事件的数据存储过程，显示后续事件不能覆盖有数据锁定的存储器。特别是在过程（c）中，事件3不能被保存在任何存储器上，原因是两个存储器设备都被先前的事件数据（即事件1和事件2）填充和锁定了。因此，需要策略设定存储设备中数据应被锁定的优先级。

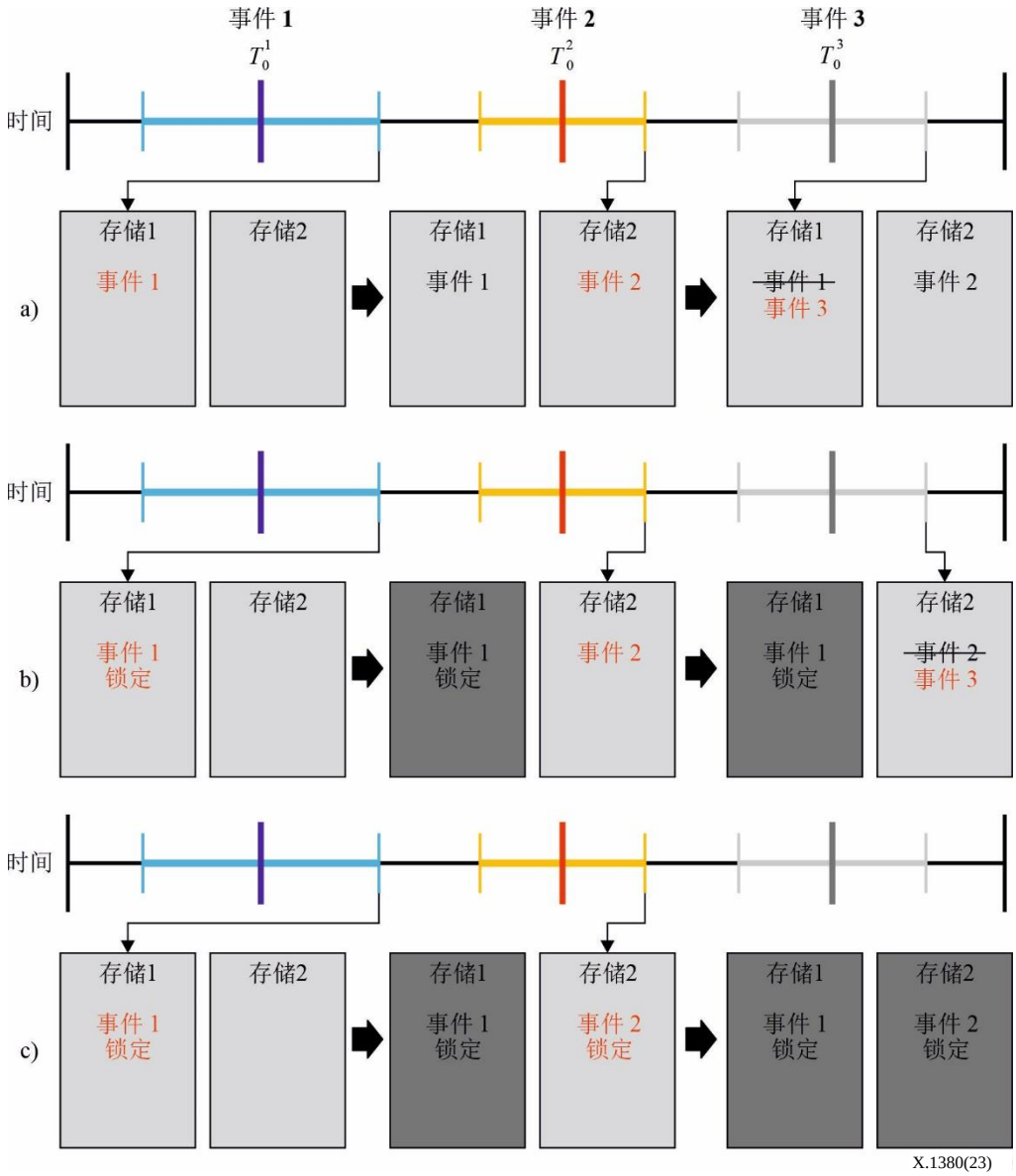

图5 – 两种存储的EDR记录示例：(a)无数据锁定；
(b)仅对事件1有数据锁定条件；(c)对事件1和事件2都有数据锁定条件

7.1.3 数据集的扩展

传统的EDR数据集通常由国家主管部门或车辆制造商管理。传统的EDR数据集需要做扩展，以应对联网和自动驾驶车辆。例如，来自自动驾驶车辆中使用的雷达和激光雷达等传感器的数据对车祸调查而言可能是至关重要的。此外，在事件期间存储的用于车辆对一切（V2X）通信的证书对联网车辆环境而言可能是至关重要的。此外，存储在入侵检测系统（IDS）中的关于异常和入侵特征的日志对澄清事件是否因网络攻击而发生而言是至关重要的。

7.2 DSSAD的数据管理

7.2.1 DSSAD的记录时间

图6显示了EDR与DSSAD之间数据记录时间的差异。DSSAD记录自动系统与驾驶者之间所有预先定义的交互，而EDR记录每当触发事件发生时预先确定的时间段。因此，EDR和DSSAD中所记录的数据有助于确定碰撞时谁在控制车辆。

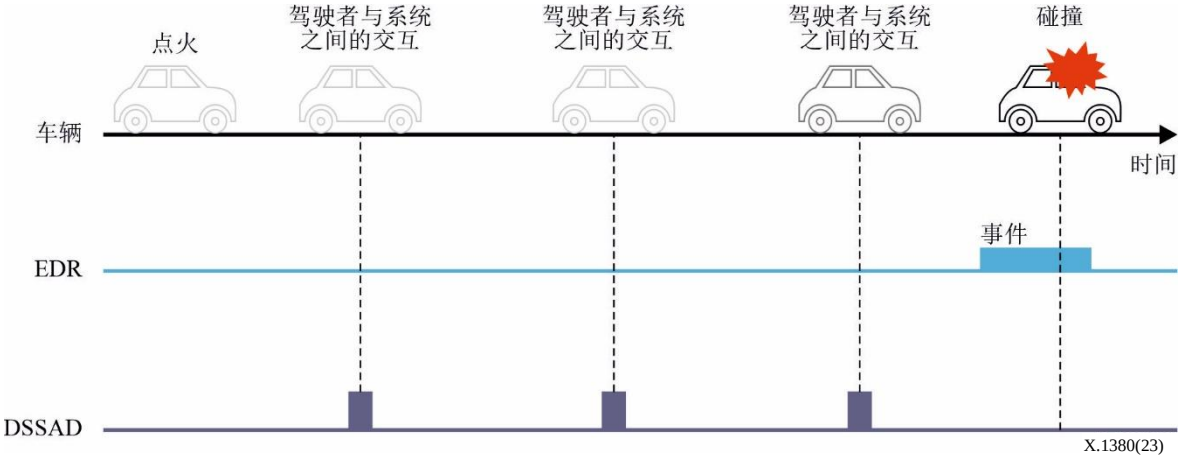

图6 – EDR和DSSAD的数据记录时间

基于云的DSSAD应该根据预先定义的策略将数据传输给云系统。当车辆中DSSAD存储器的容量达到极限时，最近的数据可以以FIFO程序的方式覆盖先前的数据。

7.2.2 车辆存储器中的数据锁定

DSSAD的存储过程也像EDR的存储过程一样，遵循先进先出（FIFO）程序。如果DSSAD存储器已满，那么数据将覆盖最旧的数据。然而，EDR存储器上有关数据锁定的预先确定的事件触发条件要求在写入数据之后锁定DSSAD数据存储器，同时拒绝覆盖已存储的数据。DSSAD已锁定数据的数据格式由DSSAD数据存储策略决定。DSSAD已锁定数据的数据格式可以不同于正常的DSSAD数据格式。

对DSSAD数据进行数据锁定后，DSSAD已锁定数据可以传输给云系统。对DSSAD已锁定数据的传输可以优先于其他数据传输，例如，正常的DSSAD数据和锁定的EDR数据。如果确认已传输，那么可以从车辆的DSSAD存储器中删去已传输的数据。

7.2.3 数据格式

EDR的目的是记录事件的数据，而DSSAD的目的是分清在某个时间点上（通常是事故发生的时间）由谁承担责任。

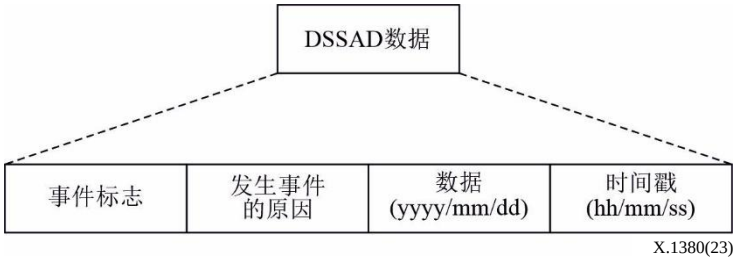

图7 – DSSAD的数据格式

DSSAD数据包括四个字段，如图7所示（参见[b-UN R157]）。

事件标志是用于指明驾驶者与系统之间交互类型的一个字段，例如，转换需求和紧急操作。

“事件原因”字段用于指明出现事件标志的原因。该字段包含转换的详细原因。事件原因列于[b-UN R157]的第8.2节。

日期字段指的是创建事件标志的日期。该字段中的数据采用年/月/日的形式。

时间戳字段指的是生成事件标志的时间。该字段中的数据采用“时/分/秒 时区”的形式。由于DSSAD的特性，要求时间戳具有高精度。对于在特定DSSAD数据的时间分辨率内同时记录的多个DSSAD数据，可以允许单个时间戳。如果一秒钟内发生多个事件，那么多个事件可能有相同的时间戳。在这种情况下，DSSAD数据应指明时间顺序。

7.3 车辆可识别信息（VII）

当EDR/DSSAD将其数据上载到云系统时，应考虑使用VII来识别数据。VII可以是车辆牌照号码、车辆证书、VIN或任何可用于识别车辆的信息。VII可被视为个人可识别信息（PII）。

关于未来的车辆环境，我们应该考虑多个用户共享一台车辆的情况，例如，共享小汽车。在每个用户都希望在驾驶时使用基于云的EDR/DSSAD系统的情况下，共享车辆应该能够在每个用户驾驶时将其区分开来。然而，很难识别每个用户，因为没有强制性的过程能让车辆采集用户的信息（例如：用户ID）。用户信息可使用个性化系统来获取，如智能手机数字密钥，它利用一个依托用户唯一证书进行的认证过程。因此，用户信息可作为VII的一部分来收集和发送。

如第6.1节中所述，当车辆遇到预先确定的触发事件时收集EDR数据，而每当车辆与驾驶者之间存在交互时收集DSSAD数据。由于EDR和DSSAD连接于一辆车上，并为每辆车收集数据，因此识别每辆车是基于云的EDR/DSSAD系统的一项基本任务。因此，VII由以下要素组成：

– **车辆信息**（强制的）：特定车辆的识别数据，如VIN
– **用户信息**（可选的）：用户或驾驶者的识别数据

图8显示了EDR/DSSAD从车辆到云的传输过程。

EDR/DSSAD根据预先定义的规则从车载网络中的每个传感器和ECU采集数据，然后将其发送给电信设备。电信设备将VII添加到所采集的EDR/DSSAD数据中，并将其发送给云系统。通过云接口接收的EDR/DSSAD数据和VII被传输给存储协调器，然后根据云系统策略进行存储。

存储在云系统中的EDR/DSSAD数据只能由经授权的用户来访问。因此，想从云系统中获取信息的用户应发送认证信息来证明自己。云系统向经过认证的用户提供EDR/DSSAD数据。

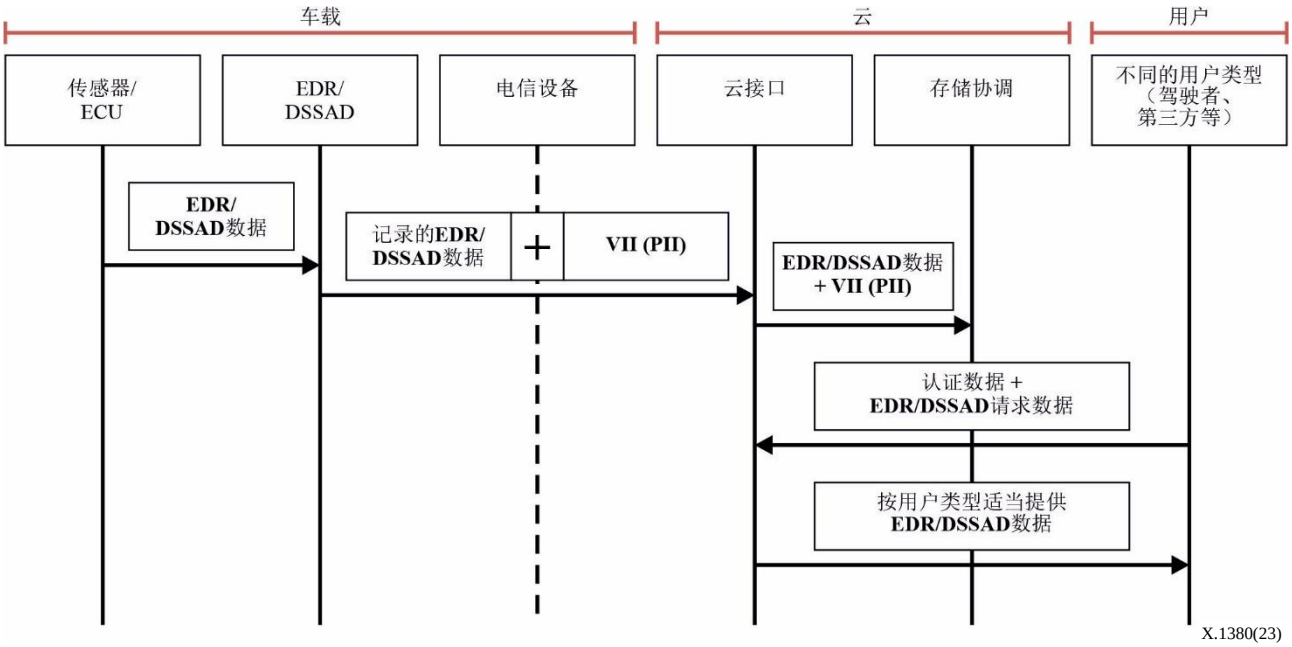

图8 – 基于云的EDR/DSSAD的数据流

7.4 EDR和DSSAD的云系统

7.4.1 增加所记录数据的可及性

传统的EDR在OBD-II端口上有一个接入点。只有通过OBD-II端口和车辆诊断工具，才能检索和利用EDR数据。这就是为什么EDR数据很少被车主使用的原因，尽管他们拥有这些数据。

另一方面，基于云的EDR/DSSAD通过在云环境中上载EDR/DSSAD数据，使用户更容易获得EDR/DSSAD数据。用户或第三方可以使用其VII或预先确定的标识来加载他们的EDR/DSSAD数据，以供进一步使用。这可以带来EDR/DSSAD数据的可伸缩性扩展，并促进道路安全。

7.4.2 规则/策略更新

基于云的EDR/DSSAD系统提供规则/策略更新功能。规则定义如何处置车辆中的数据，策略定义如何处置云中的数据。规则由事件条件、记录数据类型、某一数据类型的记录时间和车辆中的上载程序组成。基于云的EDR/DSSAD环境下的策略包括授予各方的数据访问权限。策略由存储EDR/DSSAD数据的云系统中的存储协调器来处置。

基于云的EDR/DSSAD系统提供规则/策略更新功能。通常，国家监管部门定义强制性事件数据集及其条件。在主管部门根据用户/第三方的正当请求进行监管更新之后，基于云的EDR/DSSAD系统在车辆和云上执行规则/策略更新。

8 安全威胁分析

8.1 安全资产和相关的安全目标

安全资产是指应该受到保护的任何数据对象、功能或资源。考虑到基于云的EDR/DSSAD系统，表2显示了以下资产和相关的安全目标。

表2 – 安全资产和相关的安全目标

安全资产	描述	相关的安全目标
存储于车辆的EDR/DSSAD数据	车辆中收集的EDR/DSSAD数据	完整性
存储于车辆的EDR/DSSAD规则	可以通过云策略更新的EDR/DSSAD规则	完整性
EDR/DSSAD固件	EDR/DSSAD设备的固件	完整性
无线传送（OTA）数据包	用于更新EDR/DSSAD规则的OTA数据包	机密性、完整性
总线流量	通过车载网络（IVN）传输的总线流量	机密性、完整性
EDR/DSSAD日志	EDR/DSSAD设备的审计日志	完整性、可核查性
与调试/诊断的通信	EDR/DSSAD设备与调试工具或诊断工具之间的通信	机密性、真实性
与后端的通信	后端与车辆或用户/第三方之间的通信	机密性、真实性、可用性
云策略	云策略	完整性
VII	用于识别用户/车辆的私有数据	机密性
云日志	云策略的审计日志、来自用户/第三方的请求以及其他行为都可影响云的安全性	完整性、可核查性
存储于云的EDR/DSSAD数据	从车辆处接收的EDR/DSSAD数据	完整性

8.2 安全威胁

本节描述了基于云的数据记录器系统中的安全威胁。[ITU-T X.1371]中描述了联网车辆中所有已识别的威胁。

8.2.1 对机密性的威胁

在基于云的数据记录器系统内传送的数据通常是用户的私有数据。数据采集的所有权和范围可能因车辆所在地法规而异；然而，数据记录器系统的数据一般被认为是VII。未能保持基于云的数据记录器系统中数据的机密性可被视为对用户数据私密性的侵犯。例如，网络上的窃听和线路窃听可能是对机密性的典型威胁。

– **窃听：**在如基于云的服务等无线网络中，监听媒质是一种容易实施的潜在攻击。攻击者可以以两种方式在基于云的数据记录器系统中嗅探包括VII在内的消息。首先，它可以发生在车辆与云服务器之间。在这种情况下，来自车辆的事件数据和来自云服务器的规则/策略更新数据可被泄露。

  其次，攻击可以发生在用户/第三方与云系统之间。在这种情况下，来自云系统的事件数据和来自用户/第三方的规则/策略更新请求可被泄露。

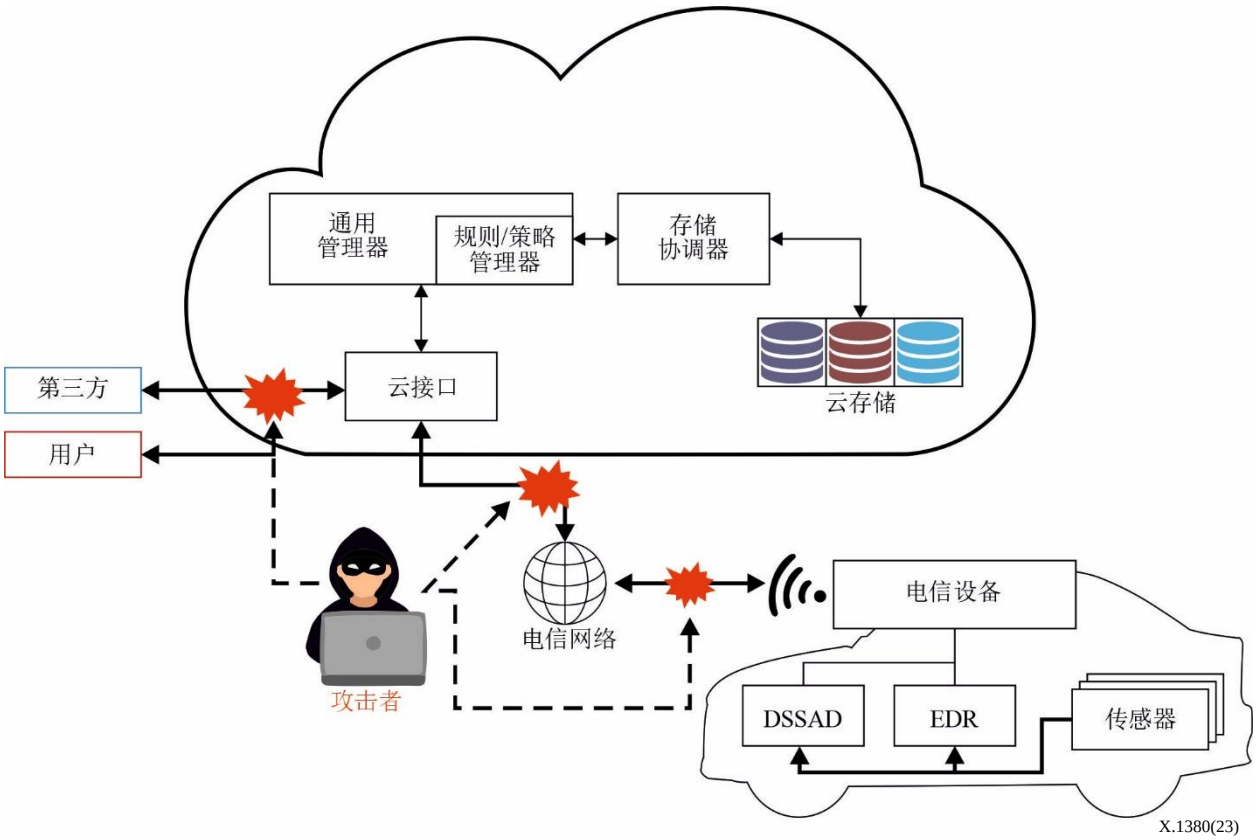

图9 – 窃听基于云的数据记录器系统

第三，攻击者可以采集并分析所传输的OTA数据包，以更新EDR规则。基于此，攻击者可能会发送虚假规则来破坏安全措施。

– **通过线路窃听的嗅探：**作为物理攻击的一种，对车载网络的直接窃听是可以发生的。现代车辆拥有多个控制器局域网（CAN）总线；对任何总线的访问都受到安全网关（或车载防火墙）的严格控制。如果攻击者没有获得安全网关的特权，那么就不可能监测所有CAN总线的全部流量。因此，攻击者可以通过线路窃听嗅探CAN总线的所有流量（包括EDR/DSSAD数据），来尝试物理访问目标车辆。

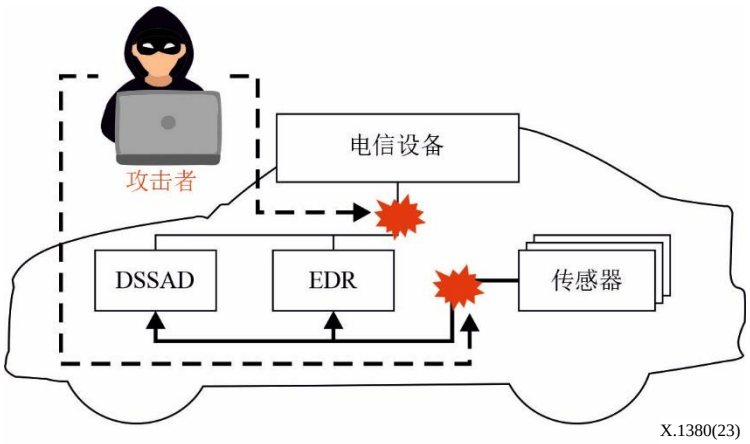

图10 – 线路窃听基于云的数据记录器系统

8.2.2 对完整性的威胁

EDR数据用于车辆碰撞或事故分析，DSSAD数据用于区分谁承担责任。因此，应确保数据在存储和传输过程中不会被更改。完整性是审计日志（如EDR/DSSAD数据）最重要的安全目标之一。攻击者想要通过使用下面给出的方法来破坏EDR/DSSAD数据的完整性。

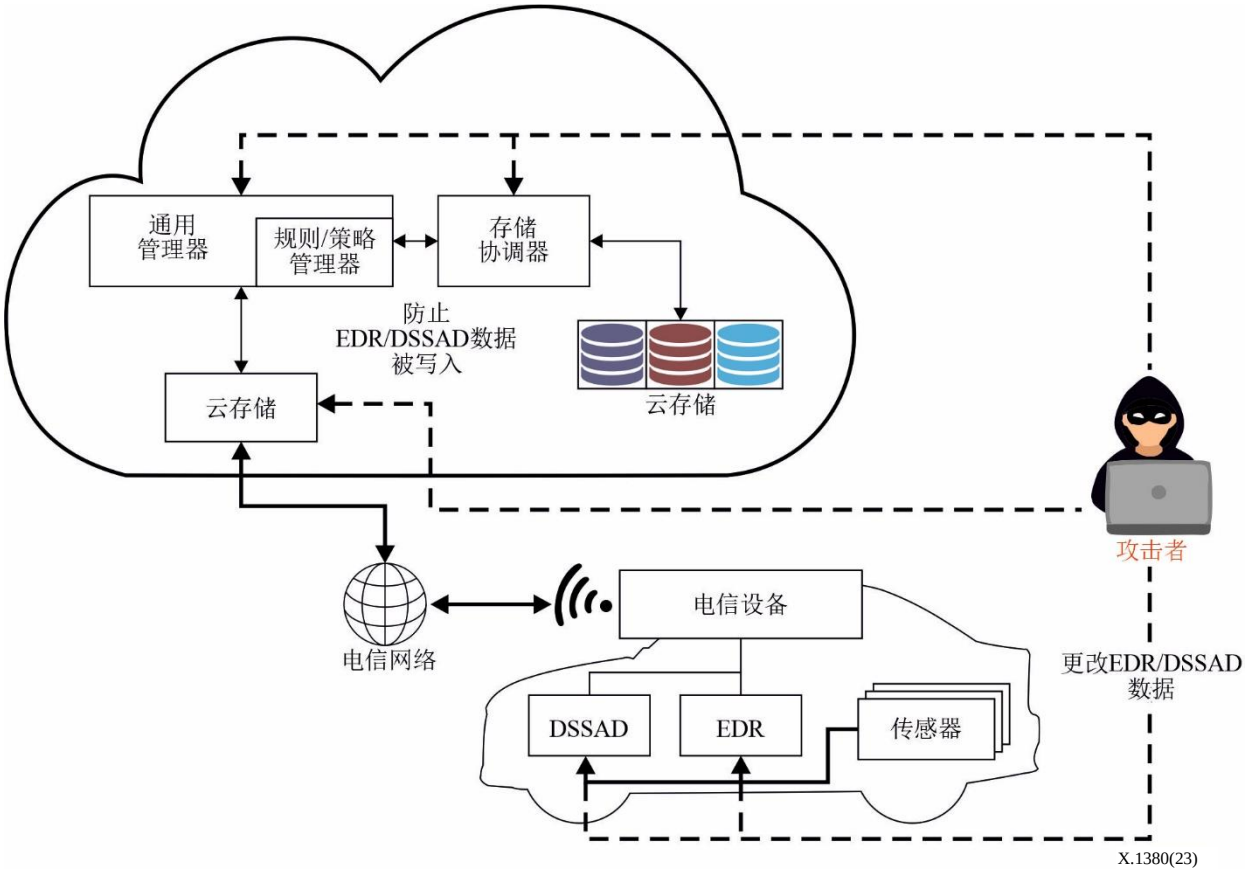

图11 – 操纵基于云的数据记录器系统的控制流

通过操纵基于云的数据记录器系统的控制流，攻击者可以更改EDR/DSSAD数据或者阻止EDR/DSSAD数据条目被写入。例如，攻击者识别并访问EDR/DSSAD印刷电路板（PCB）上的调试接口，并使用该接口操纵所执行的代码。此外，攻击者可以操纵EDR/DSSAD上的固件或EDR/DSSAD规则。攻击者还可以修改总线流量并操纵EDR/DSSAD日志。

在云系统的情况下，攻击者可以通过使用恶意软件和不安全的应用程序编程接口（API）来访问存储器并操纵EDR数据、审计日志和云策略。

图11显示了在基于云的数据记录器系统上操纵控制流的攻击。

8.2.3 对真实性的威胁

中间人攻击、假冒攻击和重放攻击可能是对真实性的典型威胁。

– **中间人攻击：**在基于云的数据记录器系统中，攻击者可以拦截车辆与云之间或者云与用户之间传输的消息，然后用任意被操纵的消息重新传输给它们。发送方没有意识到接收方是一个未知的攻击者 - 试图在将消息重新传输给接收方之前访问或修改消息。因此，攻击者可以控制它们之间的整个通信。

– **假冒攻击：**在基于云的数据记录器系统中，模仿攻击可以通过以下四种方式来进行：

- 向云系统提出虚假的对EDR/DSSAD数据的检索请求
- 向云系统提出虚假的对指定车辆的规则更新请求
- 向云系统提出存储虚假EDR/DSSAD数据的请求
- 对车辆EDR/DSSAD系统做虚假的规则更新

假冒攻击可对整个基于云的数据记录器系统的完整性造成严重损害，因为它们可以生成伪造的事件数据或改变事件规则/策略。此外，攻击者可以通过假冒攻击泄露存储在云系统中的私有数据。

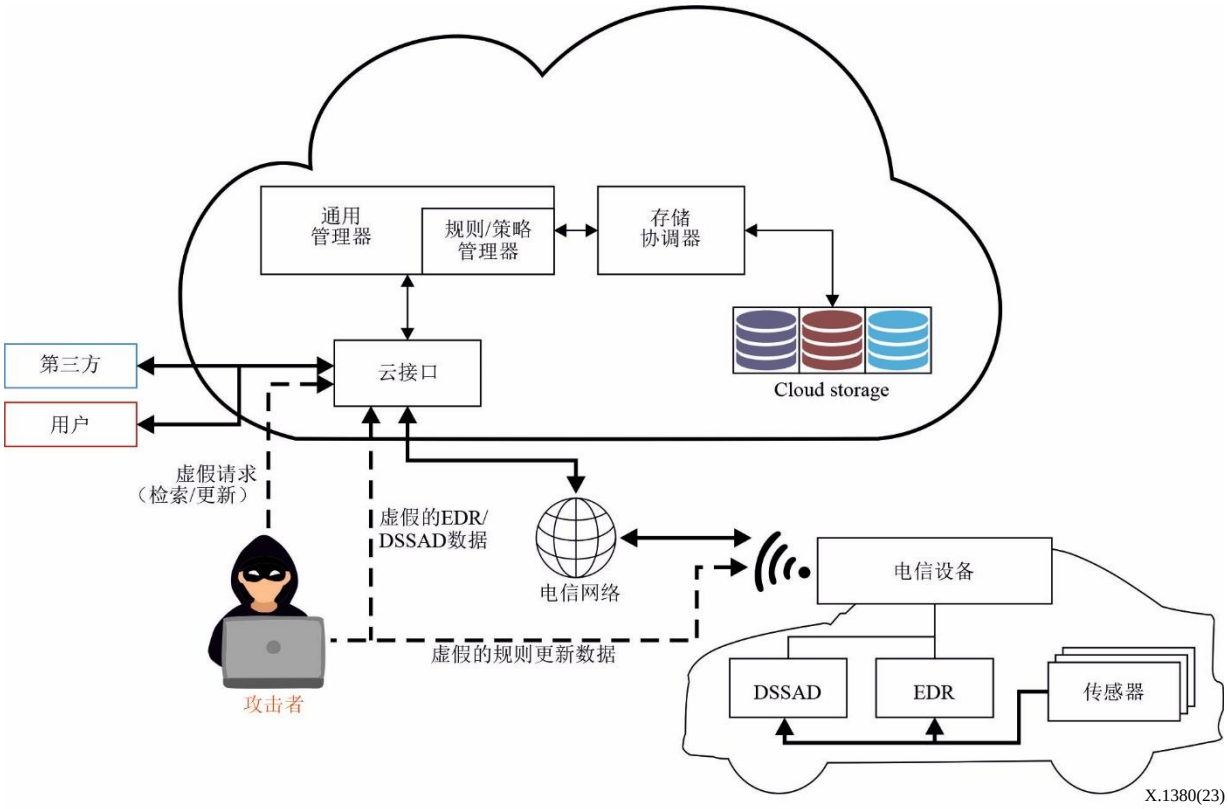

图12 – 对基于云的数据记录器系统的假冒攻击

– **重放攻击：**重放攻击可导致EDR/DSSAD数据复制和有害的规则/策略反转。

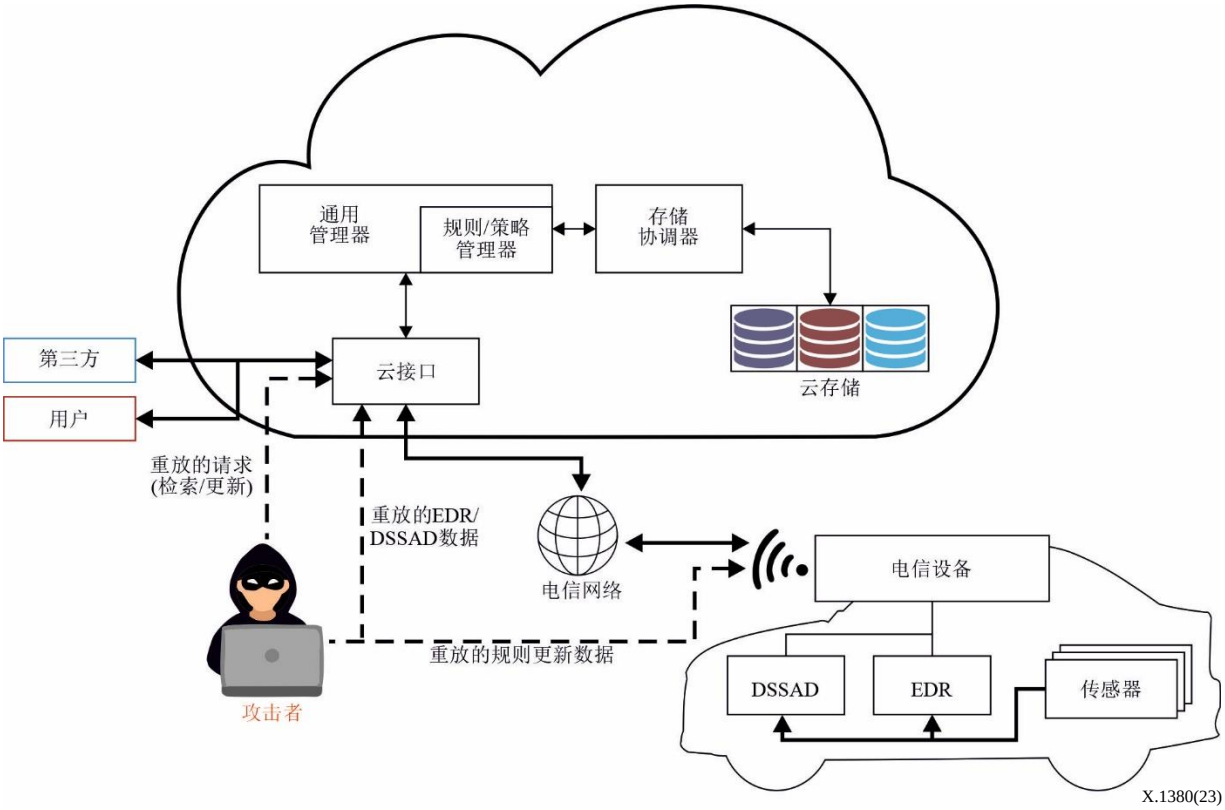

图13 – 对基于云的数据记录器系统的重放攻击

– **物理访问：**如果攻击者可以通过调试端口访问车辆，那么可以执行另一组攻击。联合测试行动小组（JTAG）是作为调试端口的最常见接口。经由JTAG的访问提供了读写内存的能力，这导致对固件的操纵和对安全措施的危害。

诊断是对车辆的另一种物理访问。攻击者可以使用诊断工具访问OBD-II端口，或者直接访问具有远程诊断功能的网关。统一诊断服务（UDS）是一种标准的诊断协议，允许对车载网络和车辆中的ECU进行监测和操纵。

8.2.4 对可用性的威胁

可用性是基于云的数据记录器系统的一个关键因素，因为可以随时存储关于事故或碰撞的有用信息。拒绝服务（DoS）攻击是对可用性最著名的威胁。

– **DoS攻击：**DoS攻击会对基于云的数据记录器系统造成严重后果，因为攻击者试图阻断有关EDR/DSSAD数据的主要的通信/存储/管理手段，这导致基于云的数据记录器系统在事故分析方面变得毫无意义。作为DoS攻击的一个例子，攻击者生成的大量消息淹没网络信道可以使网络节点或整个云系统瘫痪。（车辆或云系统中的）网络节点将无法处置大量接收的数据，并导致在将EDR/DSSAD数据存储到云系统或者更新车载和云系统规则/策略时出现故障。

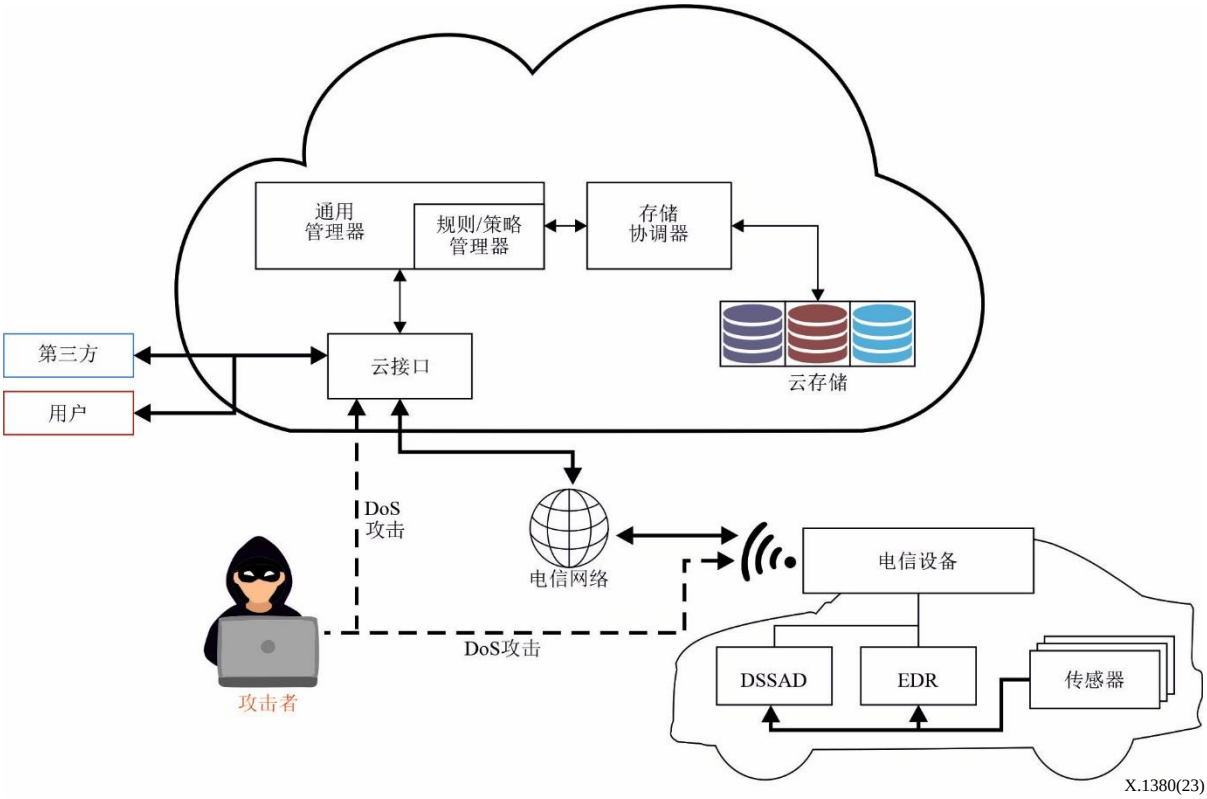

图14 – 对基于云的数据记录器系统的DoS攻击

8.2.5 对可核查性的威胁

– 丢失事件可追溯性：云系统中包含的规则/策略管理器和存储协调器等组成部分根据授权用户安装的规则/策略集开展工作。因此，管理规则/策略更改日志就可核查性而言是非常重要的。攻击者可以通过篡改或删除事件日志来制造混乱。

9 安全要求

9.1 安全启动

建议在执行前或执行期间应检查存储在EDR/DSSAD设备内存中的固件的完整性。亦建议应检查EDR/DSSAD规则和相关配置以及校准数据的完整性。

固件和规则的保护过程分为两个步骤。首先，在固件和规则的安装过程中，在写入内存之前对其进行真实性测试，然后将其配置为当前的固件和规则。其次，在每次启动过程中，对当前固件和规则的完整性进行检查。

建议安全启动机制应采用对称或非对称加密手段，以足够的安全级别验证固件和规则的完整性。还建议EDR和DSSAD设备应使用硬件信任锚，如硬件安全模块（HSM），以安全存储加密密钥并加速加密算法的计算。

9.2 安全日志

要求应使用安全加密方法确保日志数据的完整性。由于EDR/DSSAD数据是特定情况下的证据，因此应保护EDR/DSSAD数据，防止未经授权的操纵。

对于云系统，通用管理器应在每个情况下记录日志，如下所述：

– 来自用户/第三方的认证尝试

– 策略更新

建议应安全地存储日志。信息验证码（MAC）等加密措施，可以附加到日志上和/或存储在有充分访问控制的安全存储系统中。应根据云服务提供商的策略或每个国家的法规来定义最低的日志存储保留期限。

9.3 安全通信

基于云的数据记录器系统有几个通信信道，如下所述：

– 云系统和车辆之间的通信

– 用户/第三方之间的通信

– 车辆中的ECU、传感器和执行器之间的通信

建议应确保云系统与车辆或用户/第三方之间通信中消息的机密性和真实性。机密性和真实性可以通过使用传输层安全（TLS）等加密措施来实现。

还建议云系统和车辆之间的通信应确保可用性。这意味着来自众多车辆的大量EDR和DSSAD数据应适当地存储在云存储中。

建议应确保车辆的ECU、传感器和执行器之间通信中的消息和数据的完整性，以生成正确的EDR/DSSAD数据，因为来自ECU和传感器的数据与碰撞事件或驾驶活动有关。

9.4 安全访问

建议禁用EDR/DSSAD设备上的调试接口，如JTAG，因为它们对于现场操作来说不是必须的，不应绕过安全启动。调试接口的禁用方法分类如下：

– 永久性地删除

– 通过应用访问控制有条件地禁用

如果要重新启用调试接口进行质保退货分析，调试接口只能由经过授权和认证的相关方访问。建议根据最小权限原则，对硬件和软件接口上接收应用程序的权限进行限制。

建议通过诊断命令和请求的安全关键功能和数据应得到加密机制的保护。这意味着想要访问EDR/DSSAD设备的主体在发送命令前应经过认证。

9.5 安全更新

建议固件和规则的更新程序应确保真实性和完整性，即只允许刷新经过认证和未经修改的更新包。此外，建议固件和规则不应降级到以前的版本，以防止恶意使用以前的安全漏洞。还建议OTA包应通过加密方法保护的安全通道传输。

9.6 已识别的威胁和安全要求之间的关系

下表3提供了第8条中已识别的威胁和安全要求之间的对照关系信息。

表3 – 已识别的威胁和安全要求之间的关系

安全要求	威胁	安全目标
安全启动	操纵控制流 – 操纵固件 – 操纵EDR/DSSAD规则	存储在车辆中的EDR/DSSAD规则的完整性 EDR/DSSAD固件的完整性
安全日志	操纵控制流 – 操纵日志	车辆中EDR/DSSAD数据的完整性 云日志的完整性

表3 – 已识别的威胁和安全要求之间的关系

安全要求	威胁	安全目标
	失去事件可核查性	
安全通信	窃听 通过线路窃听的嗅探 操纵控制流 中间人攻击 假冒攻击 重放攻击 DoS攻击	总线流量的机密性和/或完整性 与后端系统通信的机密性和真实性 后端系统的可用性
安全访问	物理访问	与调试/诊断通信的机密性和/或真实性
安全更新	窃听 操纵控制流 – 操纵EDR/DSSAD规则 假冒攻击	OTA包的机密性和完整性

10 基于云的数据记录器系统的实施指南

在基于云的数据记录器系统中使用和管理EDR/DSSAD数据时，要求对数据进行严格保护。基于云的数据记录器系统通过使用传统数据记录器无法提供的记录数据，为研发更安全的车辆提供进一步的功能。本条介绍了基于云的数据记录器系统的实施指南。

10.1 云存储隔离

由于基于云的EDR/DSSAD系统中VII的重要性，因此要求保护VII的安全。在基于云的EDR/DSSAD系统中，要求对EDR/DSSAD数据和其VII进行物理隔离。这不仅提供了安全方面的好处，而且还允许提供额外的功能，如在不侵犯任何隐私的情况下提供第三方EDR/DSSAD数据。存储应实现物理上的隔离，并在独立的存储系统中单独管理。由于VII的相对重要性，VII的存储系统（在图15中描述为VII数据库）要求比其他数据更高的安全级别。

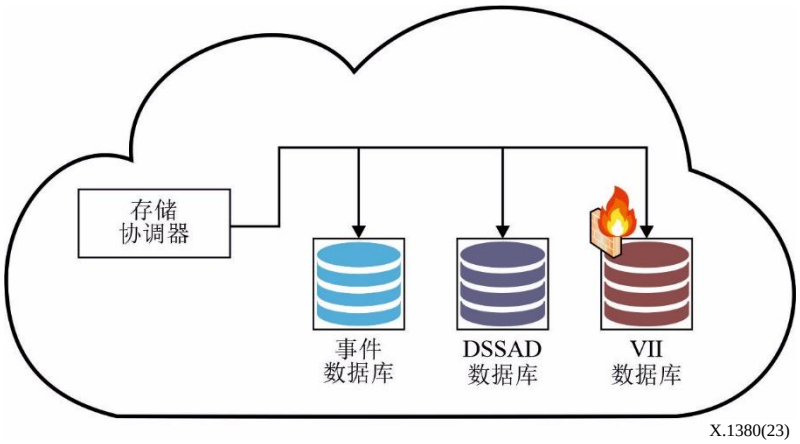

图15 – 存储隔离

10.1.1 数据存储程序

为确保与后端通信数据的机密性和真实性，在EDR/DSSAD数据从车辆发送到云系统之前，应事先建立安全通道。

当数据从车辆通过云接口发送到存储协调器时，存储协调器将EDR/DSSAD数据和VII隔离。隔离后，存储协调器生成链路数据，使EDR/DSSAD数据与VII数据联系在一起。然后，两个数据集被存储在不同的存储系统（数据库）。如图16所述，VII和EDR/DSSAD数据与链路数据被相应地存储在VII数据库和事件/DSSAD数据库中。在存储程序之后，应该记录存储过程的结果、数据存储程序的成功或失败。

数据存储程序中最重要的一个方面是遵守相关法规，如《通用数据保护条例》（GDPR）。因此，在收集车辆的任何数据之前，建议获得数据所有者的同意。

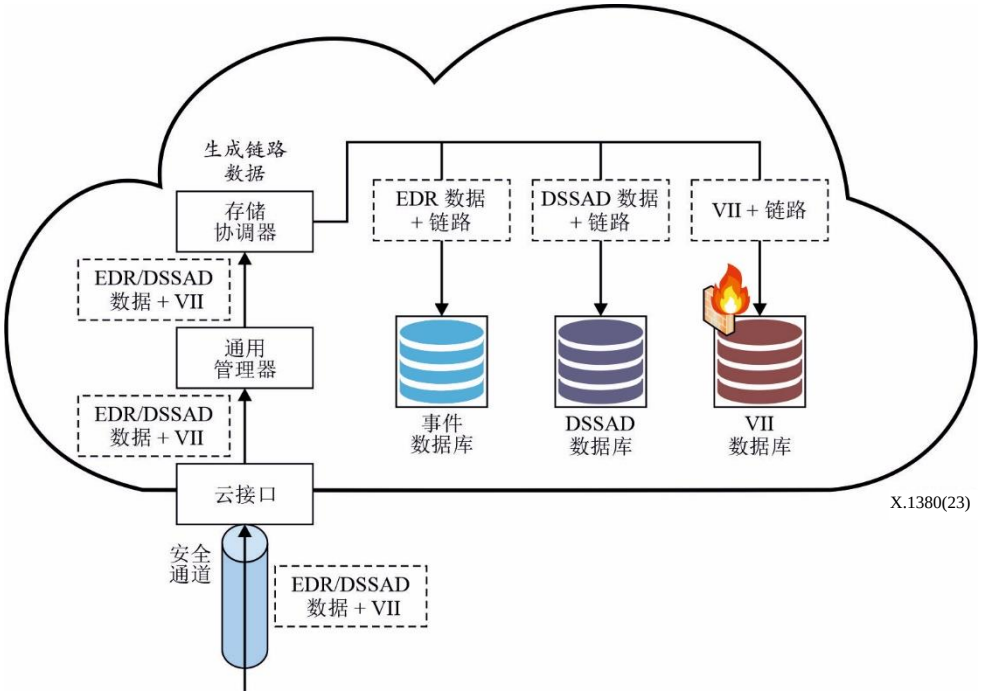

图16 – 存储隔离的存储程序

10.1.2 数据检索程序

检索EDR/DSSAD数据的程序始于用户/第三方发起的EDR/DSSAD数据检索请求。当用户/第三方访问云系统时，云接口应对用户/第三方进行认证并记录所有的尝试。如果认证成功，存储协调器使用所呈现的VII在VII数据库中找到链路数据（参阅图17(a)）。找到链路数据后，存储协调器就会搜索EDR/DSSAD数据。找到EDR/DSSAD数据时，存储协调器经过通用管理器的访问控制程序将数据提供给请求方，通用管理器的访问控制程序根据请求方的授权级别不同。检索VII数据是严格受限的，并且需要高等级的授权。另一方面，不包括VII的EDR数据或DSSAD数据可以由第三方检索。当VII数据被删除并传输到隔离的中立服务器时，EDR数据或DSSAD数据可以不经过VII搜索过程被检索（参考图17(b)）。

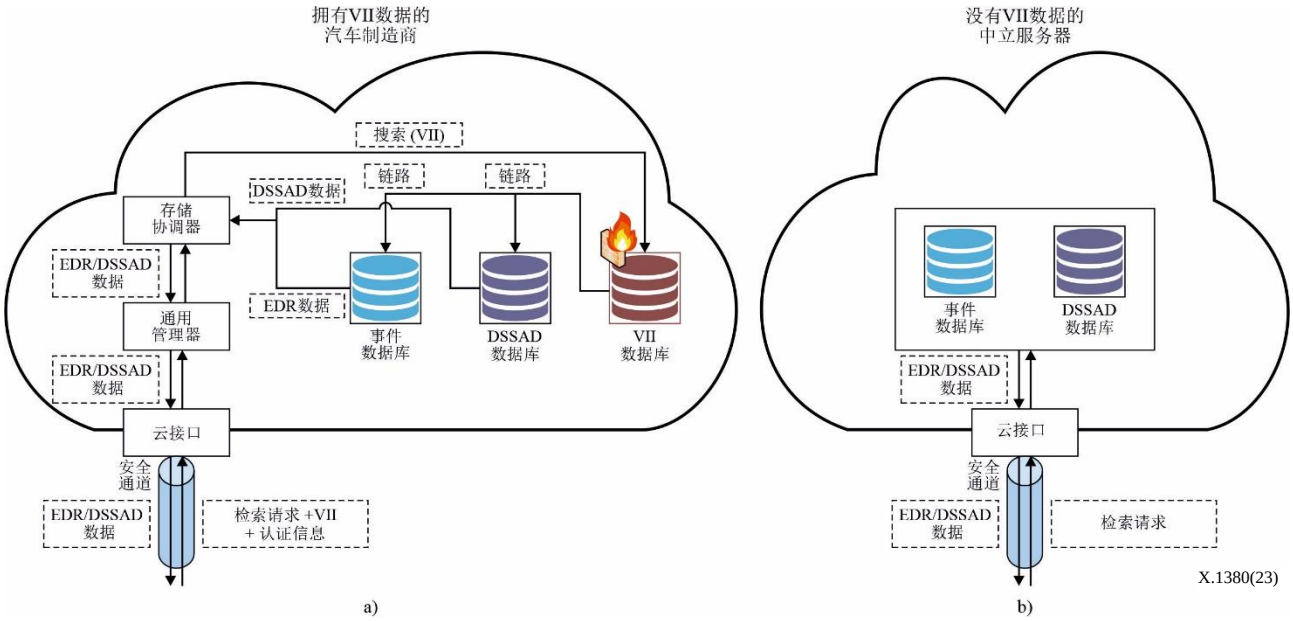

图17 – 存储隔离的检索程序

10.1.3 数据删除程序

EDR/DSSAD云系统应获得用户的同意，包括所收集的VII数据的到期日或记录数据的期限。当存储数据的到期日或给定期限到期时，应从云系统中自动删除收集的数据。

当用户请求在到期日之前删除其数据时，云系统应根据请求删除数据。当用户请求删除时，云接口应该对用户进行认证并记录所有的尝试。如果认证成功，存储协调器应使用所呈现的VII来寻找存储在VII数据库中的链路数据。利用找到的链路数据，存储协调器应搜索EDR/DSSAD数据，找到后将其删除。然后，存储协调器应存储关于删除结果的日志，并将结果报告给请求方。

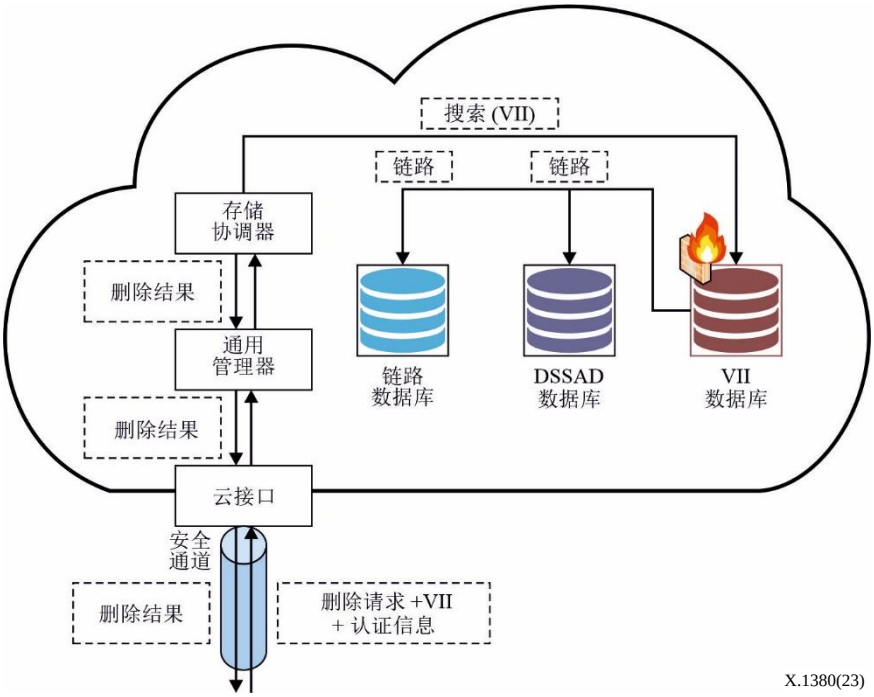

图18 – 存储隔离的删除程序

10.2 云服务注册

汽车环境中基于云的数据记录器的注册程序如图19所示。

参照图19，如果在步骤1的服务执行模式中从车辆接收到一个有关注册基于云的数据记录服务的认证请求，即车辆认证请求，步骤2应确认车辆的ID，如使用公钥密码系统的数字签名算法。在此，车辆认证请求可以以下方式来执行，即向基于云的数据记录服务系统发送利用车辆私钥签名的消息。作为步骤2中的确认结果，如果确定车辆的ID是无效的，基于云的数据记录服务系统生成相应的认证失败响应，并将该响应结果发送给车辆，如步骤3所示。

在步骤2中，作为验证结果，如果确定车辆的ID是有效的，基于云的数据记录服务系统为车辆生成认证响应，并将该响应传输给车辆，如步骤4所示。

之后，当接收到认证响应，即实现对车辆的认证时，在用户输入并生成基于云的记录服务注册信息（包括记录数据类型和记录期等）后，车辆将基于云的数据记录服务注册信息发送给基于云的数据记录服务系统，从而请求注册基于云的数据记录服务，如步骤5所示。

随后，如果从车辆输入基于云的数据记录服务注册请求（包括基于云的数据记录服务注册信息），则基于云的数据记录服务系统利用基于云的数据记录服务注册信息（例如记录数据类型和记录期等）生成安全策略，然后存储/注册信息，如步骤6所示。

此后，基于云的数据记录服务系统为每辆车指派一个化名，如步骤7所示，生成证书请求消息，用于请求为指派给每辆车的化名生成一个化名证书，并将证书请求消息发送给认证中心，如步骤8所示。

在步骤9中，基于云的数据记录服务系统监测是否从认证中心获得了化名证书。作为监测结果，如果确保获得了化名证书，则基于云的数据记录服务系统将化名证书存储在基于云的数据记录信息数据库中。化名证书可以是认证中心的数字签名消息。通过化名证书有可能保证化名的合理性。

可以为每辆车指派多个化名。由于化名不具有与每辆车的ID相关联的信息，所以有可能保护每辆车的PII。

如果收到通知，则在步骤10中，基于云的数据记录服务系统生成每辆车的基于云的数据记录服务注册信息，将其存储在信息数据库中，并将信息发送给每辆车。在此，基于云的数据记录服务注册信息可包括指派给每辆车的化名、有关化名的化名证书等。已注册的基于云数据记录服务中的每辆车（即车辆的用户），可利用从基于云的数据记录服务系统提供的基于云的数据记录服务注册信息，通过云中心和车辆之间的通信，来完成基于云的数据记录。

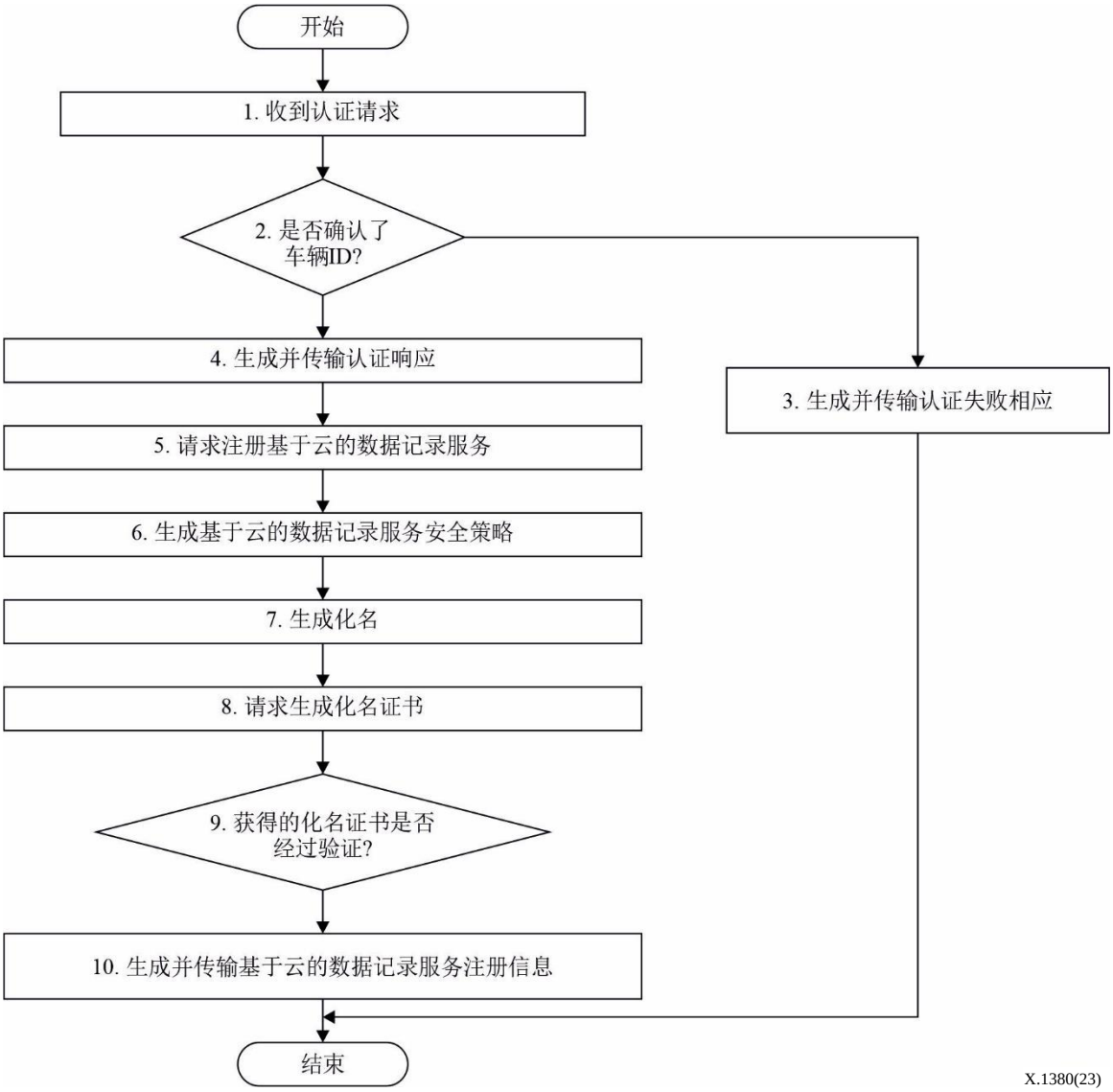

图19 – 基于云的数据记录器服务注册

基于云的数据记录器的注销程序可以考虑用于汽车租赁、二手车等用例，因为车辆所有人变更后不希望向云系统提供EDR/DSSAD数据。

11 基于云的数据记录器在汽车环境中的用例

如果汽车事故发生，EDR/DSSAD数据可以有意义地用于分析事故的原因，并确定车辆和司机是否负有责任。图20显示了EDR/DSSAD数据流。车辆中产生的EDR/DSSAD数据通过无线通信传输到云端。车主、制造商、供应商或授权第三方（如保险公司）可以利用云中的EDR/DSSAD数据。

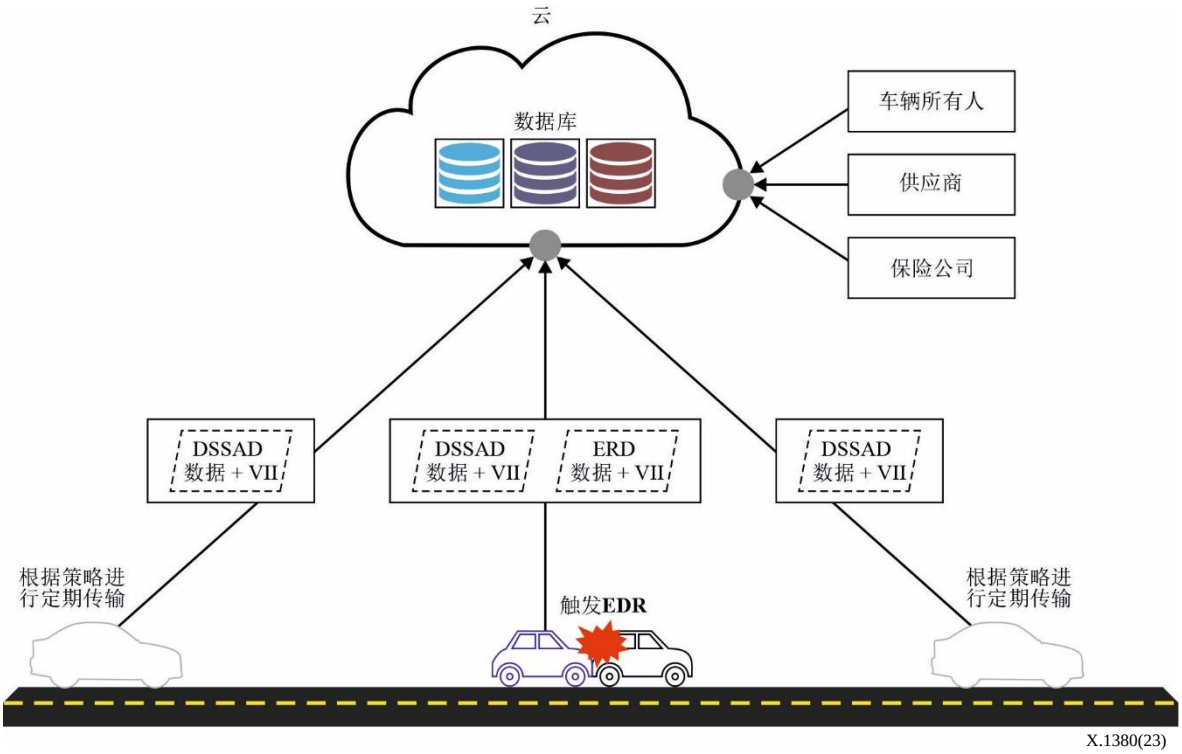

图20 – EDR/DSSAD数据流

基于云的数据记录器系统有许多优点。首先，很容易获得EDR/DSSAD数据，即使在潜在的风险情况下（如车辆起火、车辆淹水）。其次，经授权的事故分析人员可以比直接从车辆的ECU中更容易地从云系统中获得数据。

11.1 案例1：车辆间的碰撞

图21显示了一个按时间顺序排列的场景，当时一辆装有自动车道保持系统（ALKS）的车辆正在路上行驶。车祸发生在（e），并触发了EDR事件。云端存储了从（a）（ALKS被激活时）到（e）（事故发生时）的EDR/DSSAD数据。存储的EDR/DSSAD报告了以下信息：

由于ALKS在10:19:10被驾驶员激活，车辆控制权移交系统。1分50秒后，天气恶化，ALKS要求司机接收车辆控制权，但司机没有回应。然后ALKS在10:22:00自动启动了最低风险操作（MRM）。然后在10:22:30发生车祸。

通过对EDR/DSSAD数据的分析，可以检查出事故发生的时期和情况。基于云的数据记录器系统通过预定的数据传输策略将EDR/DSSAD数据存储在云系统的存储系统中。因此，与直接从车辆中的EDR存储系统中检索相比，减少了收集车祸信息的工作。

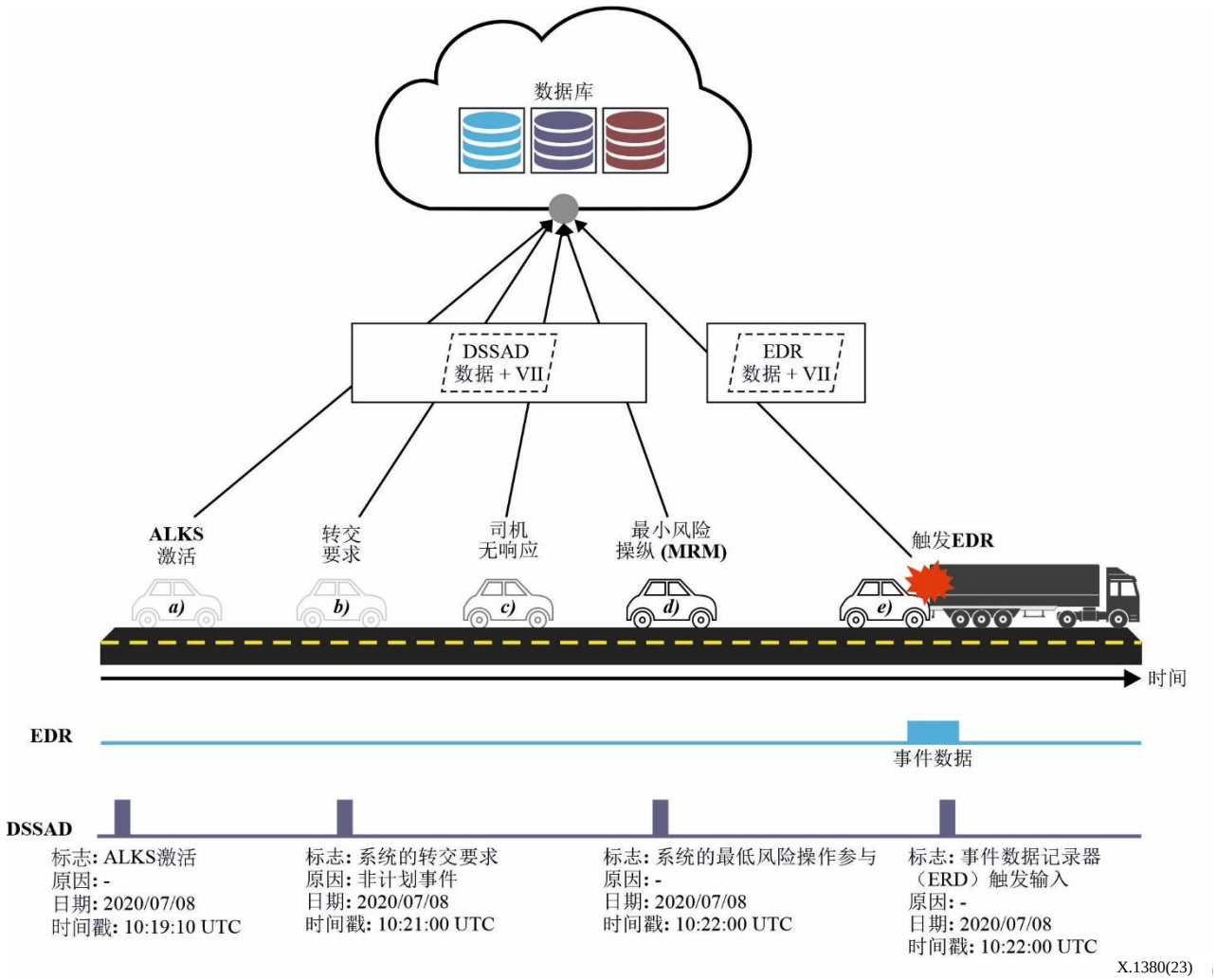

图21 – 车辆间的碰撞

11.2 案例2：车辆和自行车之间的碰撞

图22显示了一个按时间顺序排列的场景，当时一辆装有自动车道保持系统（ALKS）的车辆正在路上行驶。车辆在（c）与一辆自行车发生了软碰撞，但由于冲击力很弱，所以并未触发EDR。然而，所有最近的DSSAD数据均上传到云端。存储的EDR/DSSAD报告了以下信息：

> ALKS在10:19:10被司机激活。15秒后，司机直接操作方向盘，然后ALKS失效。车辆和自行车之间的碰撞发生在07:10:16。

在这个案例中，对车辆的撞击非常轻微，不符合EDR的触发条件，没有收集到EDR数据。尽管如此，由于DSSAD数据存储在云系统中，详细的事故情况可以很容易地被模拟和分析。

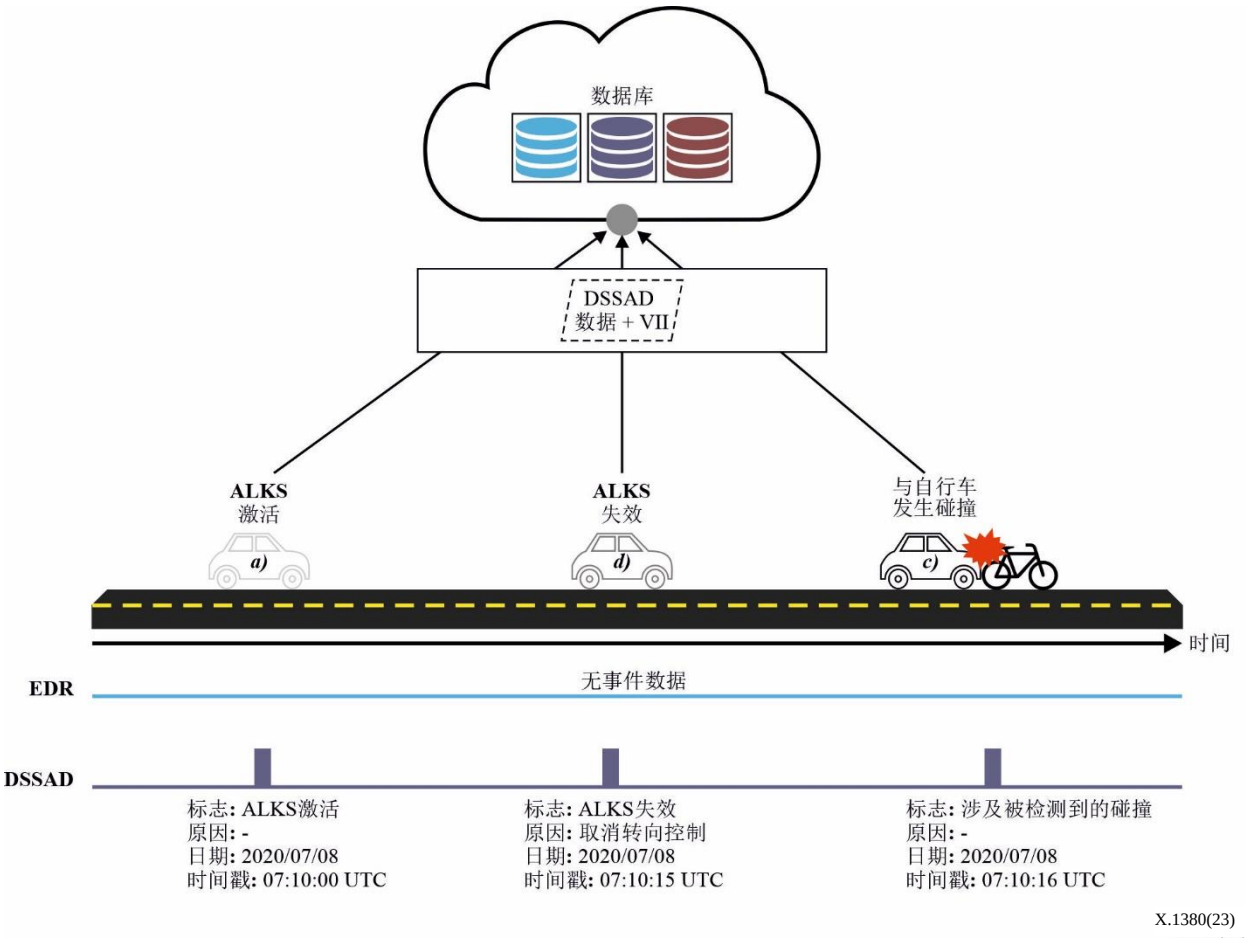

图22 – 车辆和自行车之间的碰撞

附录一

（此附录不构成本建议书不可分割的组成部分。）

常规EDR数据集示例

本示例数据集是美利坚合众国（USA）常规EDR的必要基本数据项，由美国国家公路交通安全管理局（NHTSA）监管。

表I.1 – 常规EDR的必要基本数据项[b-NHTSA EDR]

项目编号	数据项	记录时间*	采样率	范围	准确度	解析度
1	纵向Delta-V	取0-250 ms或0至事件结束加30 ms两者中的较低值	100/s	-100 至100 km/h	± 10%	1 km/h
2	最大纵向Delta-V	取0-300 ms或0至事件结束加30 ms两者中的较低值	不适用	-100 至100 km/h	± 10%	1 km/h
3	到达最大纵向Delta-V的时间	取0-300 ms或0至事件结束加30 ms两者中的较低值	不适用	取0-300 ms或0至事件结束加30 ms两者中的较低值	± 3 ms	2.5 ms
4	速度，指明车辆	-5.0至0 s	2/s	0-200 km.h	± 1 km/h	1 km/h
5	发动机节气门，%全开 加速器踏板，%全开	-5.0至0 s	2/s	0-100%	± 5%	1%
6	主刹车系统，开/关	-5.0至0 s	2/s	开/关	不适用	开/关
7	点火循环，碰撞	-1.0 s	不适用	0-60,000	± 1循环	1循环
8	点火循环，下载	下载时	不适用	0-60,000	± 1循环	1循环
9	安全带状态，司机	-1.0 s	不适用	开/关	不适用	开/关
10	前安全气囊警告灯	-1.0 s	不适用	开/关	不适用	开/关
11	前安全气囊部署时间，司机（第一阶段，多级安全气囊）	事件	不适用	0-250 ms	± 2 ms	1 ms
12	前安全气囊部署时间，RFP（第一阶段，多级安全气囊）	事件	不适用	0-250 ms	± 2 ms	1 ms
13	多个事件，事件数量（1或2）	事件	不适用	1, 2	不适用	1, 2
14	事件1到事件2的时间	根据需要	不适用	0-5.0 s	0.1 s	0.1 s
15	完整的文件记录（是或否）	遵循其他数据	不适用	是/否	不适用	是/否

参考文献

[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）*.

ITU-T 建议书系列

A 系列	ITU-T 工作的组织
D 系列	资费和结算原则以及国际电信/ICT 经济和政策问题
E 系列	综合网络运行、电话业务、业务运行和人为因素
F 系列	非话电信业务
G 系列	传输系统和媒质、数字系统和网络
H 系列	视听和多媒体系统
I 系列	综合业务数字网
J 系列	有线网和电视、声音节目及其他多媒体信号的传输
K 系列	干扰的防护
L 系列	环境和 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、 安装和保护
M 系列	电信管理，包括电信网管管理和网络维护
N 系列	维护：国际声音节目和电视传输电路
O 系列	测量设备技术规程
P 系列	电话传输质量、电话装置、本地线路网络
Q 系列	交换和信令以及相关的测量与测试
R 系列	电报传输
S 系列	电报业务终端设备
T 系列	远程信息处理业务的终端设备
U 系列	电报交换
V 系列	电话网上的数据通信
X 系列	**数据网络、开放系统通信和安全**
Y 系列	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
Z 系列	用于电信系统的语言和一般软件问题

瑞士印刷
2023年，日内瓦