ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.1380 (03/2023)

SERIES X: Data networks, open system communications and security

Secure applications and services (2) – Intelligent transportation system (ITS) security

---

Security guidelines for cloud-based event data recorders in automotive environments

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security (1)	X.1140–X.1149
Application Security (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1350–X.1369
Intelligent transportation system (ITS) security	**X.1370–X.1399**
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
Cyber Defence	X.1590–X.1599
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1380

Security guidelines for cloud-based event data recorders in automotive environments

Summary

Event data recorders (EDRs) are one of the most important components installed in automotive road vehicles to record vehicle status, vehicle movements and user inputs during crashes. By analysing the event data, the cause of a crash can be understood and eventually, used to improve safety in automotive environments. A data storage system for automated driving is also an important component to record data that will give a clear picture of the interactions between the driver and the automated driving system. Conventional event data recorders, however, record and manage the whole data locally and in this way, the data could come under threat of loss and destruction.

Cloud computing is being considered as an enabler of network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. Industries such as the aviation industry are already attempting to apply cloud services to event data recording systems to increase safety in the aviation environment. According to the current trend of connectivity among vehicles, EDRs and the data storage systems for automated driving will be implemented to increase their overall safety. However, they have various vulnerabilities in the process of collecting, transferring, storing, managing, and using the recorded data according to the distinctive characteristics of the automotive environment. Therefore, it is necessary to study these vulnerabilities, security requirements, and use cases for cloud-based data recorders in automotive environments.

Recommendation ITU-T X.1380 provides security guidelines for cloud-based data recorders in automotive environments. It describes threats, vulnerabilities, security requirements, and use cases for cloud-based data recorders in automotive environments.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1380	2023-03-03	17	11.1002/1000/15106

Keywords

Cloud, cloud-based DSSAD, cloud-based event data recorder (EDR), data recorders, DSSAD, EDR, security requirements, security threats.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1380

Security guidelines for cloud-based event data recorders in automotive environments

1 Scope

This Recommendation provides security guidelines for cloud-based data recorders such as an event data recorder (EDR) and a data storage system for automated driving (DSSAD) in automotive environments. This Recommendation includes technical considerations of data recording systems, EDR and DSSAD. In addition, this draft Recommendation also provides security requirements and use cases.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1371] Recommendation ITU-T X.1371 (2020), *Security threats to connected vehicles.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-ITU-T X.1252]: Formalized process of verification that, if successful, results in an authenticated identity for an entity.

3.1.2 automated lane keeping system [b-UN R157]: The system that is activated by the driver and which keeps the vehicle within its lane.

3.1.3 authorization [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.4 availability [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.5 authenticity [b-ITU-T X.641]: Protection for mutual authentication and data origin authentication.

3.1.6 accountability [b-ITU-T X.800]: The property that ensures that the actions of an entity may be traced uniquely to the entity.

3.1.7 confidentiality [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.8 data storage system for automated driving (DSSAD) [b-UN R157]: The system that enables the determination of interactions between the automated lane keeping systems (ALKS) and the human driver.

3.1.9 event data recorder (EDR) [b-UN R160]: a device or function in a vehicle that records the vehicle's dynamic, time-series data during the time period just prior to an event (e.g., vehicle speed vs. time) or during a crash event (e.g., delta-V vs. time), intended for retrieval after the crash event. For the purposes of this definition, the event data does not include audio and video data.

3.1.10 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.11 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 cloud interface: A gateway of the cloud system, which is an interface for communications between a cloud system and vehicles, users, third parties.

3.2.2 general manager: The component of a cloud system that governs the basic procedures of storing, and retrieving event data recorder (EDR)/data storage system for automated driving (DSSAD) data, and verifies basic requirements of request from a user, third party, or vehicle.

3.2.3 neutral server: The independent server from the vehicle manufacturers that can provide anonymized or vehicle identifiable information (VII) or VII-removed event data recorder (EDR)/data storage system for automated driving (DSSAD) data.

3.2.4 rule/policy manager: The component of a cloud system that updates the rule/policy, which is a part of a general manager.

3.2.5 storage coordinator: The component of a cloud system that separates event data recorder (EDR)/data storage system for automated driving (DSSAD) data and vehicle identifiable information (VII) to store and retrieve the data in the cloud storage with a predetermined policy.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ALKS	Automated Lane Keeping Systems
API	Application Programming Interface
CAN	Controller Area Network
DoS	Denial of Service
DSSAD	Data Storage System for Automated Driving
ECU	Electronic Control Unit
EDR	Event Data Recorder
FIFO	First-in-first-out
GDPR	General Data Protection Regulation
IVN	In-Vehicle Network
JTAG	Joint Test Action Group
MAC	Message Authentication Code
MRM	Minimum Risk Manoeuvre
OBD	On-Board Diagnostic
OTA	Over-the-air

PII	Personally Identifiable Information
TLS	Transport Layer Security
UDS	Unified Diagnostic Services
V2X	Vehicle-to-everything
VII	Vehicle Identifiable Information
VIN	Vehicle Identification Number

5 Conventions

This Recommendation uses the following conventions:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

6 Cloud-based data recorder systems

6.1 Cloud-based event data recorder system

Cloud-based EDR is an EDR connecting to cloud systems (backend server) to increase accessibility and the security of EDR data in connected and autonomous vehicle environments.

An EDR is a device installed in most automobiles today to record information related to vehicle crashes or accidents to improve the safety and quality of life in the vehicle environment.

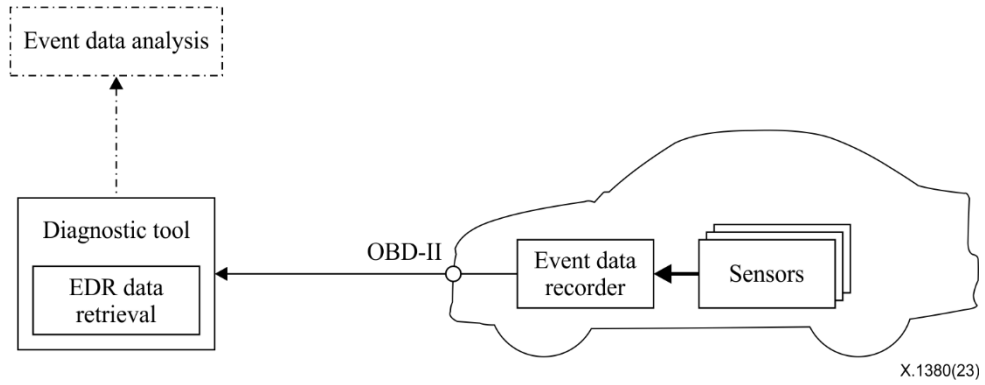

Figure 1 – Conventional automotive EDR

The conventional EDR, as shown in Figure 1, is triggered when there is an event in which the vehicle status meets certain conditions, such as frontal airbag deployment, exceeding the acceleration/deceleration threshold, rollover, etc. When the EDR is triggered, the EDR collects a predetermined dataset from sensors and then stores the data in its internal storage with non-volatile memory. The data is practically recorded from −5 seconds of trigger time (usually referred to as T0) to +500 milliseconds of trigger time. "−5 seconds" and "+500 milliseconds" are diverse by national regulations or vehicle manufacturers.

Generally, the EDR has the capacity to store more than one event on the vehicle. When the storage is filled with past event data, the oldest data is overwritten by newly updated data. In special events such as airbag deployment, the conventional EDR stores the collected data and locks the data storage to prevent it from being manipulated or overwritten.

Stored data is retrieved through the on-board diagnostic (OBD)-II port by the diagnostic tool or designated retrieval tool and is used to analyse the crash or the accident. The minimum of the dataset collected is determined by the national vehicle regulations or vehicle manufacturer's designs. Also, the data formats of recorded event data are usually different by each vehicle manufacturer and are often different by vehicle model. Thus, when retrieving and analysing the event data, specialized retrieval software is required.

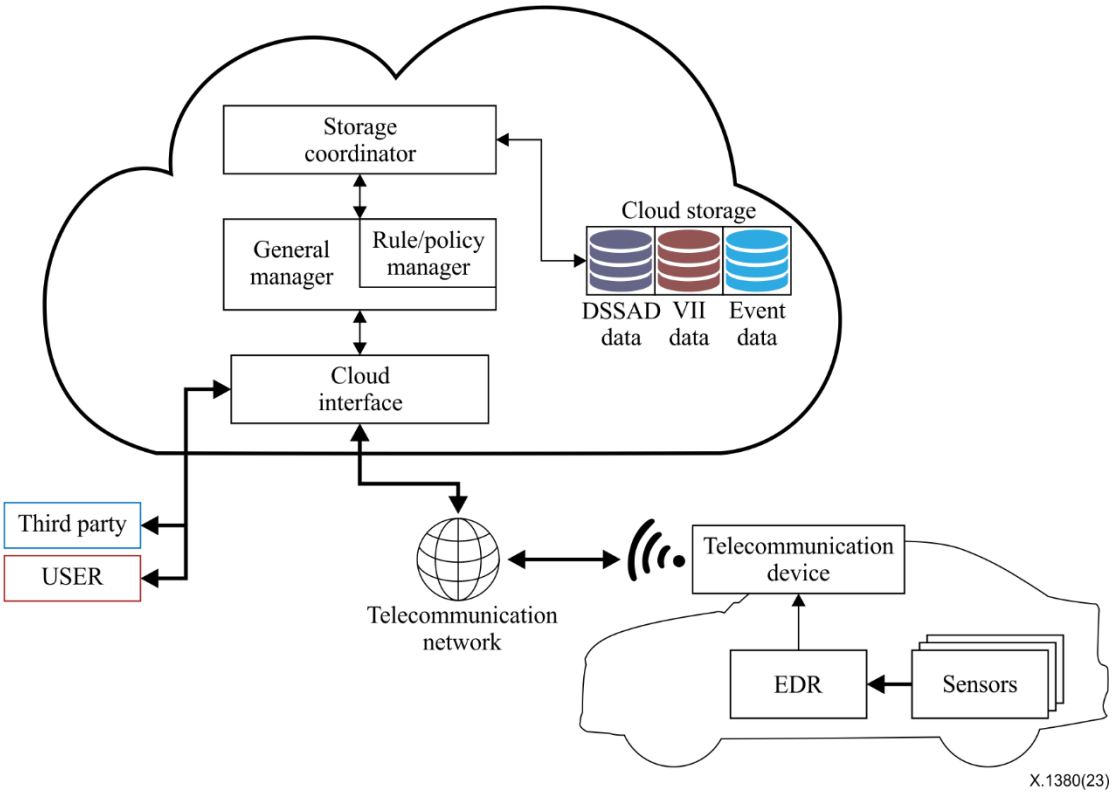

Figure 2 – Cloud-based EDR

A cloud-based EDR, described in Figure 2, stores the event data on the cloud systems through a telecommunication device connected to the EDR.

The recording data set may be different from conventional EDR data sets due to the systematic and environmental differences between conventional EDRs and cloud-based EDRs. Also, a new type of data from the electronic control unit (ECU) governing autonomous driving could be added because it is the critical data which helps in analysing autonomous vehicle accidents.

Different from conventional EDR, which overwrites new event data over unlocked event data, the cloud-based EDR can record event data on the cloud storage without overwriting data. Thus, the cloud-based EDR can have full recorded data for a vehicle without deletion. This is one of the biggest benefits the cloud-based EDR has, dramatically aiding road safety research using the full EDR data.

The collected and stored EDR data in the cloud services should be available to users or third party if any party requests the EDR data with due process and authorization. On the delivery of requested EDR data to the parties, there should be an authentication process to verify the validity of the request.

In addition to the functions of storing and providing EDR data, the cloud-based EDR also provides rule/policy updates on the system. Any user or third party can request the rule/policy update for the EDR device in the vehicle and the related policy on the cloud system. The request would require higher authority and security verification than any ordinary storing and retrieving procedures.

In the cloud-based EDR system in Figure 2, entities within the cloud systems are defined to function above the functionalities of the cloud-based EDR. The cloud interface is a gateway of the cloud

system and keeps the log of the designated accesses. The general manager governs the basic procedures of storing and retrieving EDR data. It verifies basic requirements of request from the user/third party or vehicle, also executing rule/policy updates with the assistance of rule/policy embedded managers. Storage coordinator stores and retrieves the event data with a predetermined policy. The policy may include screening the EDR data retrieved from the cloud storage due to the authority of the requester. It may also include the methodology of storing and retrieving the process of the EDR data on the cloud storage.

6.2 Cloud-based data storage system for automated driving

Data storage system for automated driving (DSSAD) is a system that aims to shed light on who requested to drive and who was driving (it can be different, especially during transition procedures) by storing a set of data that provides a clear picture of the interactions between the driver and the automated driving system. DSSAD has been recognized in [b-UN R157]. The regulation recognizes the DSSAD as a requirement for automated driving vehicles.

DSSAD stores information such as the automated driving system activation, deactivation, transition demands emergency maneuvers, etc. When the state of the automated system is deactivated or transition demanded, the reason for the state change is stored in the DSSAD. Stakeholders can clarify who requested to drive and who was in charge of the actual driving by analysing the DSSAD data, which records the interaction between the automated system and the driver.

The cloud-based DSSAD, described in Figure 3, stores DSSAD data on the cloud systems through a communication device connected to the DSSAD. The process that DSSAD data is delivered to the cloud system is the same as for cloud-based EDR. The difference is that DSSAD data is sent instead of EDR data. DSSAD periodically transmits DSSAD data to the cloud system. Thus, DSSADs can flexibly respond to problems caused by the limitations of DSSAD storage.

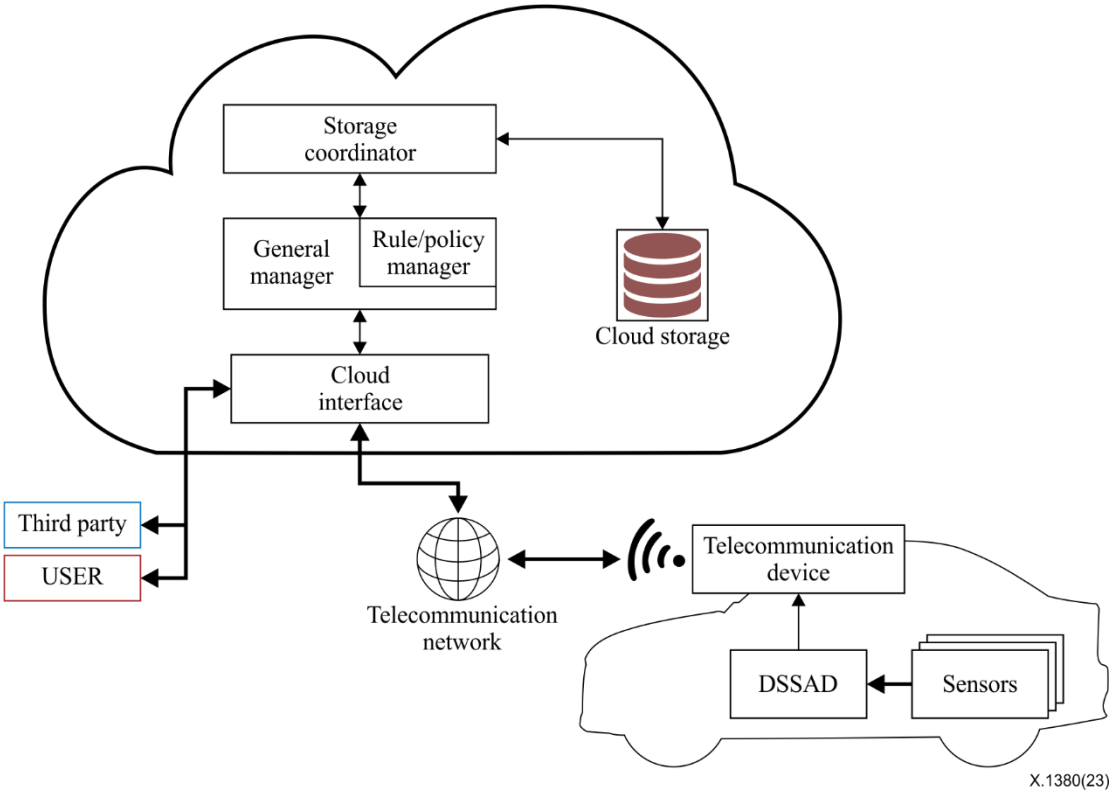

Figure 3 – Cloud-based DSSAD

6.3 Comparison of EDR and DSSAD

The comparison between EDR and DSSAD is shown in Table 1.

Table 1 – Comparison of EDR and DSSAD

	EDR	DSSAD
Purpose	Accident analysis and reconstruction	Clarifying liability of the vehicle at specific times; who was requested to drive and who was in charge of driving
Triggering condition	Event (e.g., crash): a physical occurrence that causes the trigger threshold to be met	Interaction: change in the system operation status, or demand for a change in the system operation status
Collected data	Predetermined dataset relevant to crash analysis	Predetermined data set relevant to vehicle control and liability
Storing time	Record data when triggered (momentaneous)	Record data over the entire driving
Upload timing	Every storing time, ignition on/off	

7 Cloud-based data recorder system design

7.1 Data management of EDR

The purpose of EDR is to store vehicle information on specific events such as an airbag deployment. The recorded data in the EDR is used for crash analysis and reconstruction. Therefore, EDR records the time of an event and the vehicle status of when the event happened.

7.1.1 Recording time for event data

Figure 4 describes how EDR records an event. When the EDR detects a specific event, EDR sets the event occurrence time as T_0 specific to the occurred event, then collects the designated data on a predetermined recording timeframe, which is a pre-defined time duration. T_0^n denotes the occurrence time of the n-th event. The recording timeframe may be different according to the types of events because each type of event has different triggering conditions. T_{pre} denotes the time before the specific event. T_{post} denotes the time after the specific event. The timeframe can be described as $[(T_0 - T_{pre}) \sim (T_0 + T_{post})]$.

In the case of multiple events occurring subsequently, as described in Figure 4, EDR records the EDR data regardless of the overlapping timeframe. Figure 4 (a) shows the recorded time frames for non-overlapped events. Figure 4 (b) shows the recorded time frames for overlapped events.

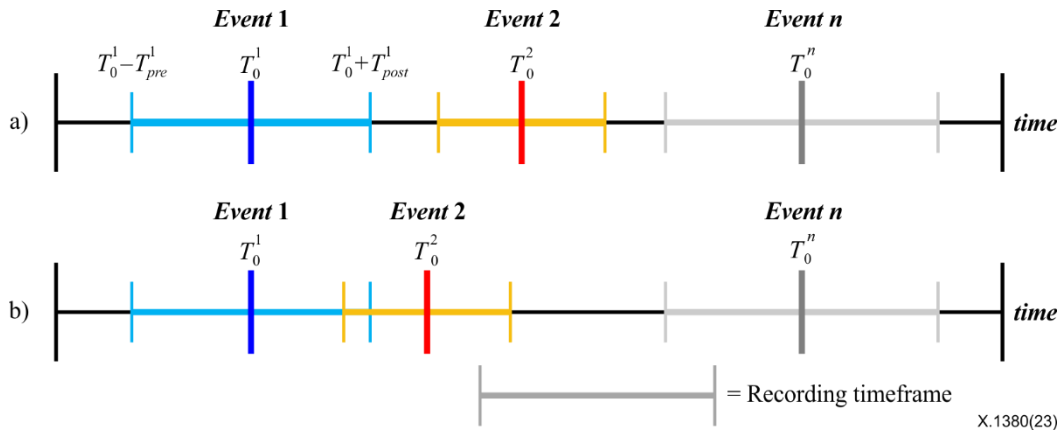

Figure 4 – Recording timeframe of EDR: (a) non-overlapped events (b) overlapped events

7.1.2 Data lock in storage in a vehicle

There are several in-vehicle storage devices for EDR data. Since the predetermined conditions are diverse, there can be multiple events occurring subsequently. Storing process of EDR follows the first-in-first-out (FIFO) procedure. If all EDR storages are already filled with the previous events, new event data overwrites the oldest one. However, some predetermined event trigger conditions, such as frontal airbag deployment, require the lock on data storage after writing the recorded data so that the stored data cannot be overwritten. Figure 5 shows an example of EDR recording procedures with two storages. Figure 5, (a) shows the data storing process for the subsequent events without data lock condition, showing that event 3 overwrites on the storage with the oldest event data. On the other hand, (b) and (c) shows the data storing process for the subsequent events with data lock condition, showing that the following event cannot be overwritten on the storage with data lock. Especially in process (c), event 3 cannot be saved on any storage because both storage devices are filled and locked with the previous event data, i.e., event 1 and event 2. Therefore, the policy is required to set the priority on which data should be locked in the storage devices.

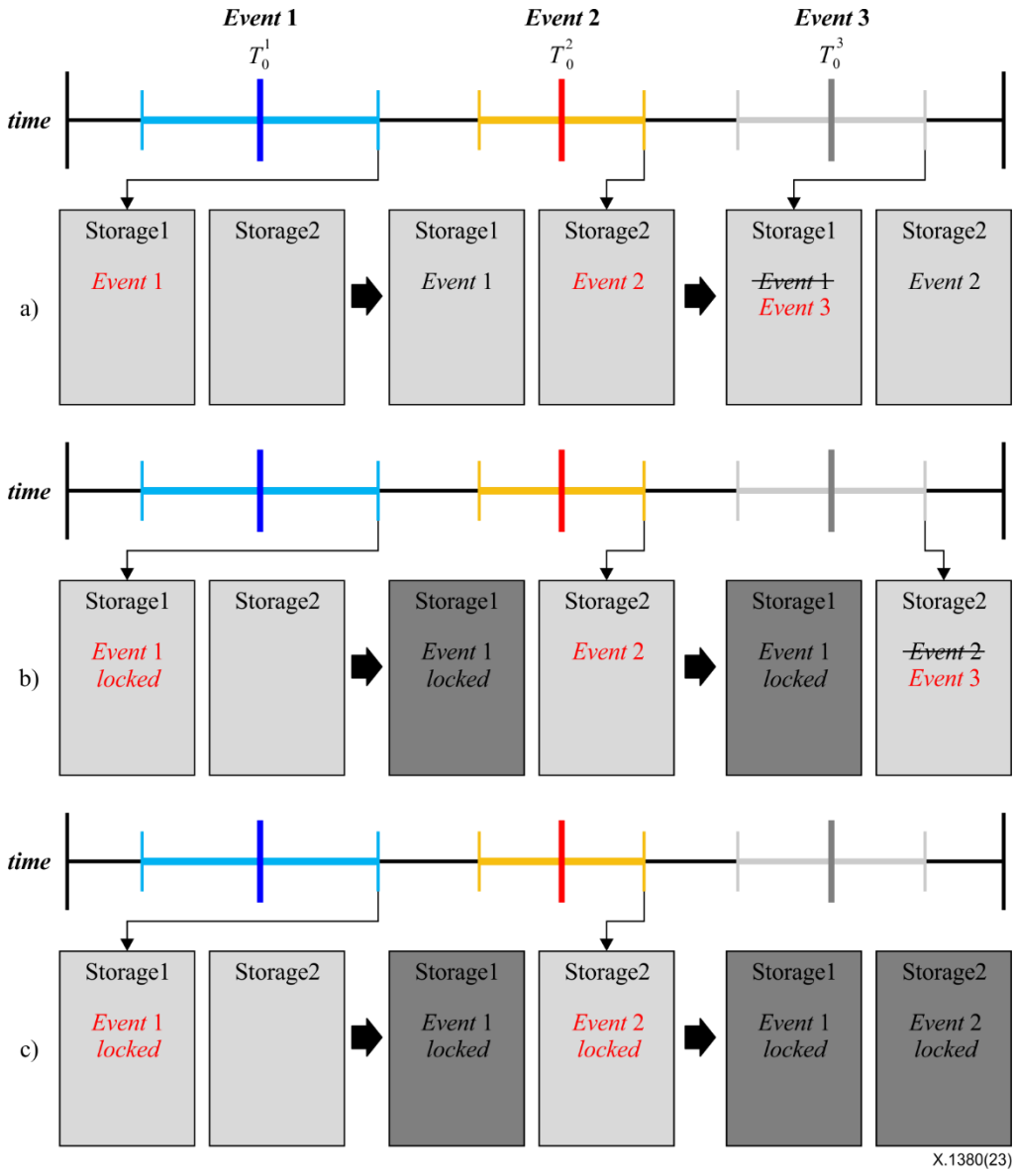

Figure 5 – Example of EDR recording with two storages: (a) without data lock, (b) with data lock condition only for Event 1, (c) with data lock condition both for Event 1 and Event 2

7.1.3 Extension of data set

Conventional EDR data set is generally regulated by national administrations or vehicle manufacturers. The conventional EDR dataset needs to be extended to cope with connected and autonomous vehicles. For example, the data from sensors such as radar and lidar used in the autonomous driving vehicle may be critical to investigate the car accident. In addition, certificates stored used in the vehicle-to-everything (V2X) communication during the event may be essential to the connected vehicle environment. In addition, logs stored in an intrusion detection system (IDS) regarding anomalies and intrusion signatures are crucial to clarify whether the event has occurred due to cyberattacks.

7.2 Data management of DSSAD

7.2.1 Recording time for DSSAD

Figure 6 shows the difference in data recording time between EDR and DSSAD. DSSAD records all of the predefined interactions between the automated system and the driver, while EDR records for a predetermined time frame whenever the triggering events occur. Therefore, the recorded data in EDR and DSSAD is useful to determine who was in control of the vehicle at the time of the crash.

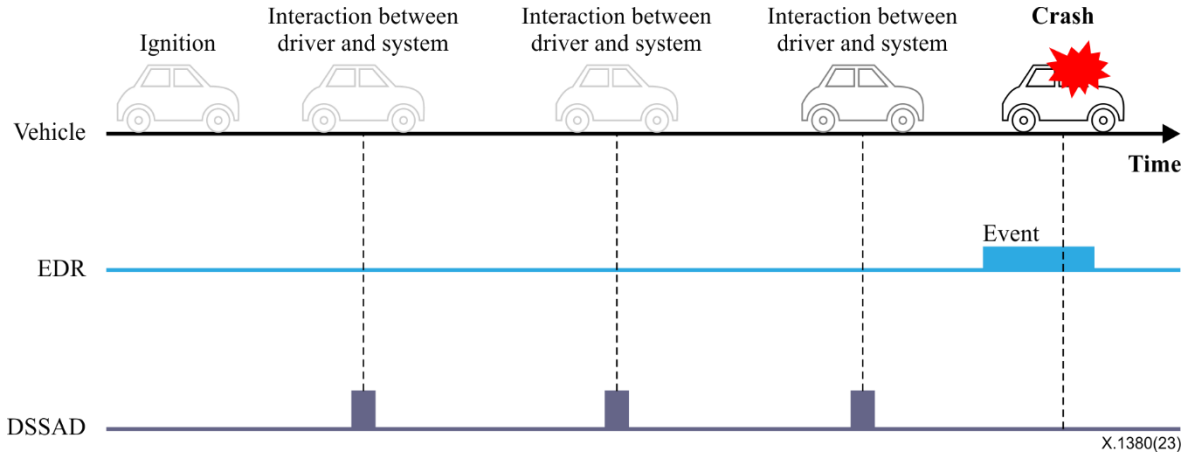

Figure 6 – Data recording time of EDR and DSSAD

The cloud-based DSSAD should transmit data to the cloud system according to a predefined policy. When the capacity of DSSAD storage in the vehicle reaches the limit, the recent data can overwrite the previous data in the way of the FIFO procedure.

7.2.2 Data lock in storage in a vehicle

Storing process of DSSAD also follows the first-in-first-out (FIFO) procedure like the storing process of EDR. If the DSSAD storage is full, the data overwrites the oldest one. However, the predetermined event trigger condition of data lock on EDR storage requires the lock on DSSAD data storage after writing the data while rejecting overwrites on the stored data. The data format of the locked data for DSSAD is determined by the policy of the DSSAD data storage. The data format of the locked data for DSSAD can be different from the normal DSSAD data format.

After data lock on DSSAD data, the locked data for DSSAD can be transmitted to the cloud system. Transmission of the locked data for DSSAD may have priority among other data transmissions such as normal DSSAD data and locked EDR data. If completion of transmission is confirmed, transmitted data can be eliminated in the DSSAD storage of the vehicle.

7.2.3 Data format

While the purpose of EDR is to record the data of an event, the objective of DSSAD is to distinguish who carries the burden of the liability at a certain point in time (usually the time of the accident).

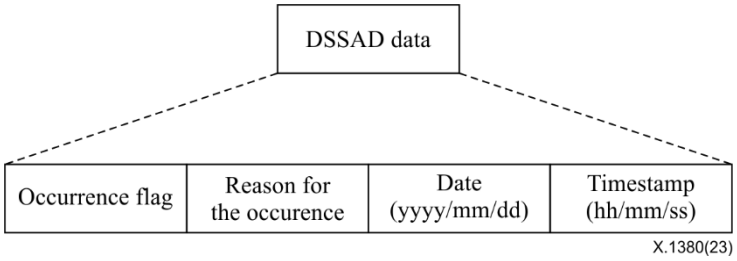

Figure 7 – The data format of DSSAD

DSSAD data includes four fields, as shown in Figure 7 (refer to [b-UN R157]).

The occurrence flag is a field that indicates the type of interaction between the driver and the system, such as transition demands and emergency maneuvers.

The reason for the occurrence field indicates why the occurrence flag occurred. This field contains the detailed reason for the transition. The reason for the occurrence is listed in clause 8.2 of [b-UN R157].

The date field is the date when the occurrence flag is created. The data in this field is in the form of a year/month/day.

The timestamp field is the time when the occurrence flag is generated. The data in this field is in the form of "hour/minute/second time zone". Due to the characteristics of DSSAD, high precision of the timestamp is required. A single timestamp can be allowed for multiple DSSAD data recorded simultaneously within the time resolution of a particular DSSAD data. If multiple events occur within one second, multiple events may have the same timestamp. In this case, DSSAD data should indicate the time order.

7.3 Vehicle identifiable information (VII)

When EDR/DSSAD uploads their data to cloud systems, VII should be considered to identify the data. VII can be a vehicle plate number, a vehicle certificate, VIN, or anything that can be used as identification for the vehicle. VII can be considered as personally identifiable information (PII).

Regarding the future vehicle environments, we should consider the situations where multiple users are sharing a single vehicle, such as car sharing. In the situations where each user wishes to use cloud-based EDR/DSSAD systems while they are driving, the shared vehicle should be able to distinguish each user when they are driving. Nevertheless, it is hard to identify each user because there is no mandatory process to make a vehicle collect a user's information (example: user ID). User information could be obtained using personalized systems like smartphone digital key which utilizes an authentication process using the user's unique certificate. Thus, user information could be gathered and sent as a part of VII.

As described in clause 6.1, EDR data is gathered when a vehicle meets the triggering events which are predetermined while DSSAD data is gathered whenever there is an interaction between a vehicle and a driver. Since EDR and DSSAD are attached to a vehicle and data is gathered for each vehicle, identification of each vehicle is an essential task for the cloud-based EDR/DSSAD system. Therefore, VII is composed of the following elements:

– **Vehicle information** (mandatory): identification data for a specific vehicle such as VIN.

– **User information** (optional): identification data for a user or driver.

Figure 8 shows the transmission process of EDR/DSSAD from the vehicle to the cloud.

EDR/DSSAD collects data from each sensor and ECU in the in-vehicle network according to the predefined rules and then transmits it to the telecommunication device. The telecommunication device adds VII to the collected EDR/DSSAD data and sends it to the cloud system. EDR/DSSAD data and VII received through the cloud interface are transferred to the storage coordinator and then stored according to the cloud system policy.

EDR/DSSAD data stored in the cloud system can only be accessed by authorized users. Therefore, users who want to get information from the cloud system should send authentication information to prove themselves. The cloud system provides EDR/DSSAD data to authenticated users.

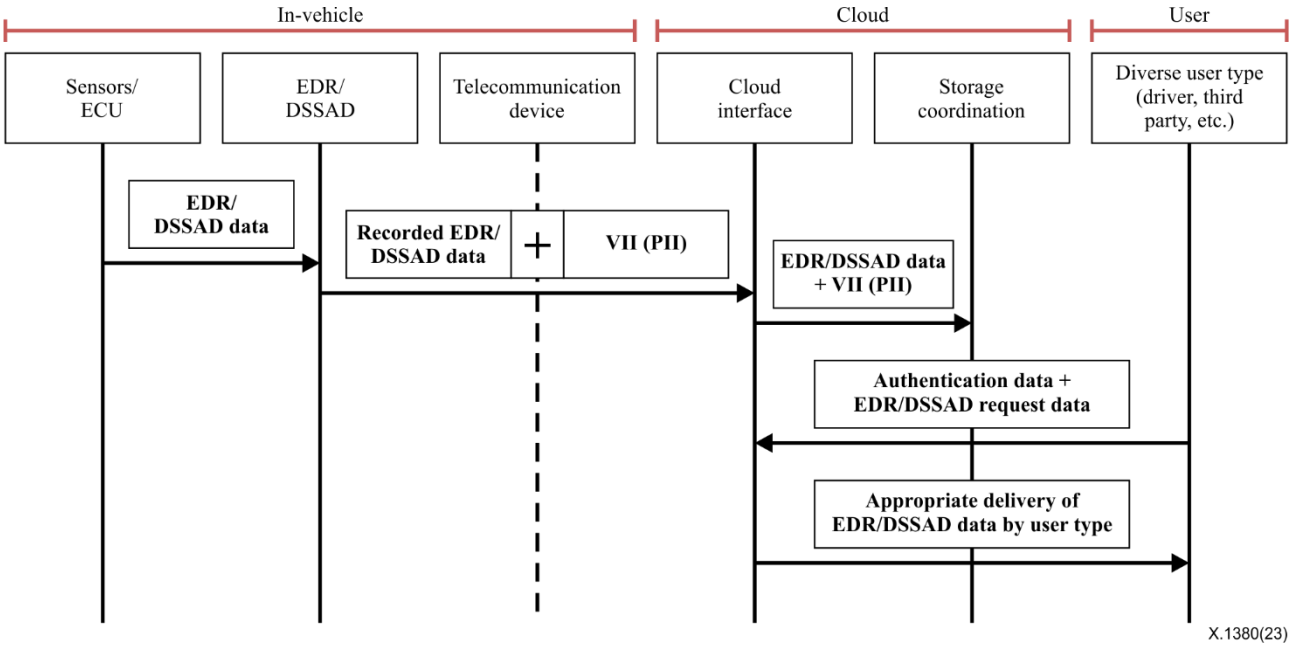

Figure 8 – The data flow of the cloud-based EDR/DSSAD

7.4 Cloud systems for EDR and DSSAD

7.4.1 Increased accessibility of recorded data

The conventional EDR has an access point on the OBD-II port. Only through the OBD-II port and the vehicle diagnostic tool, EDR data can be retrieved and utilized. This is the reason why EDR data are seldom used by owners of vehicles despite their ownership of the data.

On the other hand, cloud-based EDR/DSSAD gives the users increased accessibility to EDR/DSSAD data by uploading the EDR/DSSAD data in cloud environments. Users or third party may use their VII or predetermined identifications to load their EDR/DSSAD data for further usage. This can lead to the scalable expansion of EDR/DSSAD data and lead to the advancement of road safety.

7.4.2 Rule/policy update

A cloud-based EDR/DSSAD system provides the function of rule/policy update. The rule defines how to handle the data in a vehicle and the policy defines how to handle the data in the cloud. The rule is comprised of event condition, recording data type, recording time of a certain data type and the uploading procedure in a vehicle. The policy in the context of the cloud-based EDR/DSSAD is comprised of data access authority given to parties. The policy is handled by a storage coordinator in the cloud systems to store the EDR/DSSAD data.

The cloud-based EDR/DSSAD systems offer a function of rule/policy update. In general, national regulation departments define the mandatory event data set and its conditions. Following the

regulatory updates by authorities with their rightful request of the user/third party, the cloud-based EDR/DSSAD system executes rule/policy updates on the vehicle and the cloud.

8 Security threats analysis

8.1 Security assets and related security objectives

A security asset means any data object, function, or resource that should be protected. From a consideration of cloud-based EDR/DSSAD systems, the following assets and related security objectives are shown in Table 2.

Table 2 – Security assets and related security objectives

Security asset	Description	Related security objectives
EDR/DSSAD data stored in a vehicle	EDR/DSSAD data gathered in the vehicle	Integrity
EDR/DSSAD rules stored in a vehicle	EDR/DSSAD rules which can be updated by cloud policy	Integrity
EDR/DSSAD firmware	The firmware of EDR/DSSAD device	Integrity
Over-the-air (OTA) package	OTA package used for updating EDR/DSSAD rules	Confidentiality, integrity
Bus traffic	Bus traffic transmitted in in-vehicle network (IVN)	Confidentiality, integrity
EDR/DSSAD Log	Audit log for EDR/DSSAD device	Integrity, accountability
Communications with debugging/diagnosis.	Communication between EDR/DSSAD device and debugging tools or diagnostic tools	Confidentiality, authenticity
Communications with back-end	Communication between back-end and vehicles or users/third parties	Confidentiality, authenticity, availability
Cloud policy	Cloud policy	Integrity
VII	Private data used to identify users/vehicles	Confidentiality
Cloud log	Audit logs for cloud policies, requests from users/third parties, and other behaviours can affect the security of the cloud	Integrity, accountability
EDR/DSSAD data stored in cloud	EDR/DSSAD data received from vehicles	Integrity

8.2 Security threats

This clause describes security threats in cloud-based data recorder systems. Overall identified threats in connected vehicles are described in [ITU-T X.1371].

8.2.1 Threats to confidentiality

The data being delivered inside cloud-based data recorder systems is generally private data of the users. The ownership and scope of the collection of the data may be diverse to the regulations where the vehicle lies; however, the data of the data recorder system is generally regarded as VII. Failing to keep the confidentiality of the data in the cloud-based data recorder systems can be treated as an invasion of the data privacy of the users. For example, eavesdropping and wiretapping on the network may be typical threats to confidentiality.

– **Eavesdropping**: In wireless networks such as a cloud-based service, listening to the media is a potential attack that is easy to carry out. An attacker can sniff messages including VII in the cloud-based data recorder systems in two ways. First, it can happen between the vehicle

and the cloud server. In this case, event data from vehicles and rule/policy-update data from a cloud server can be leaked.

Second, an attack can happen between user/third-party and cloud systems. In this case, event data from the cloud system and rule/policy-update requests from user/third-party can be leaked.

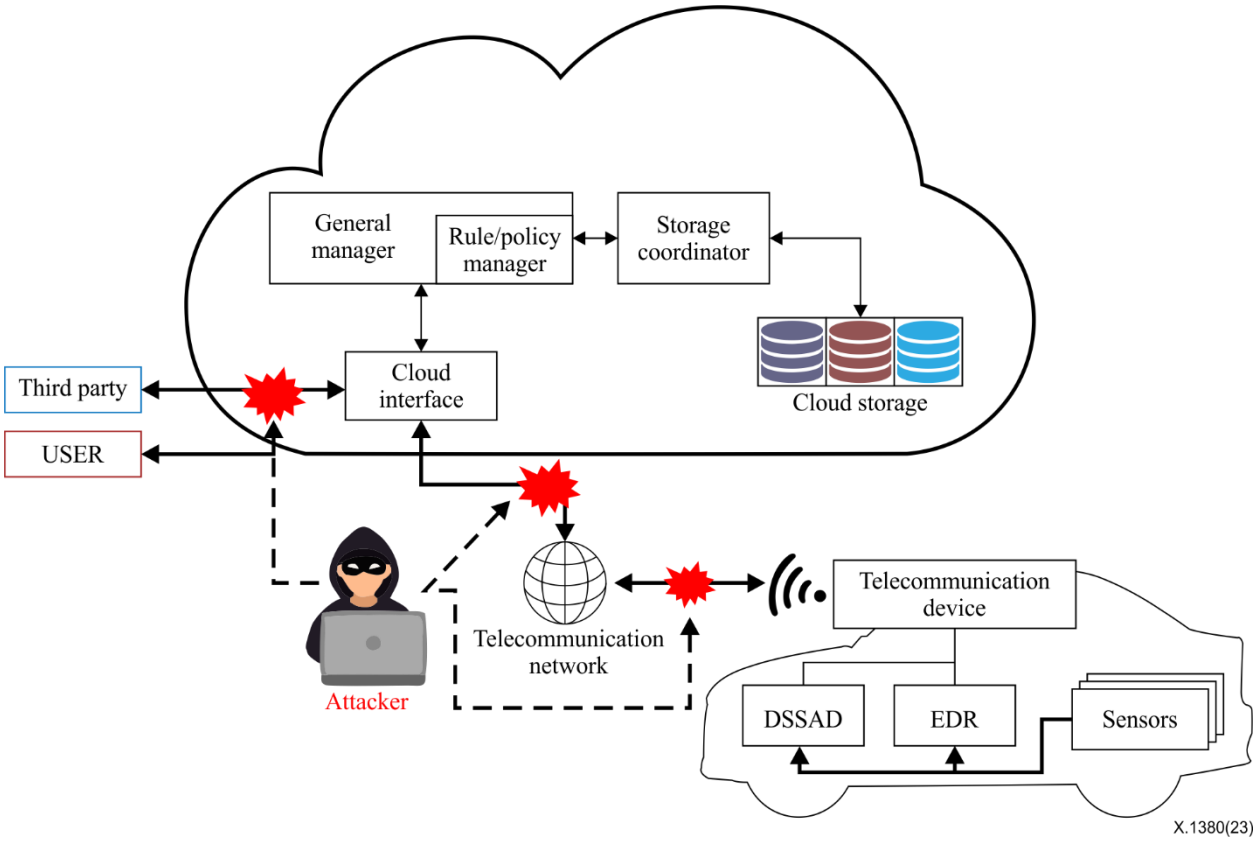

Figure 9 – Eavesdropping on cloud-based data recorder systems

Third, an attacker can capture and analyse the OTA package transmitted to update EDR rules. Based on this, the attacker may send fake rules to compromise security measures.

– **Sniffing by wiretapping**: As one of the physical attacks, a direct tapping to an in-vehicle network can happen. Modern vehicles have multiple controller area network (CAN) buses; the access to any bus is strictly controlled by a security gateway (or in-vehicle firewall). It is not possible to monitor the whole traffic of all CAN buses if the attackers do not get the privilege of the security gateway. Thus, attackers can try to access the target vehicle physically by wiretapping to sniff all of the traffic of CAN buses including EDR/DSSAD data.

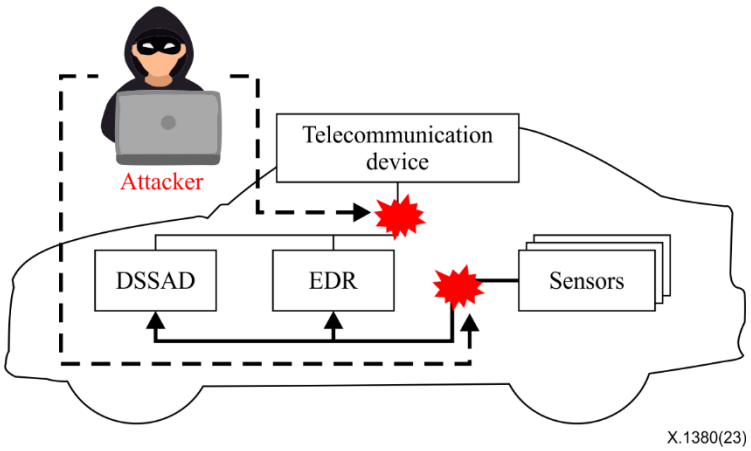

Figure 10 – Wiretapping on cloud-based data recorder systems

8.2.2 Threats to integrity

EDR data is used for vehicle crash or accident analysis, and DSSAD data is used for distinguishing who carries the burden of liability. Therefore, it should be ensured that the data is not altered in storage and transit. Integrity is one of the most important security objectives of audit logs such as EDR/DSSAD data. Attackers want to compromise the integrity of EDR/DSSAD data by using the methods given below.

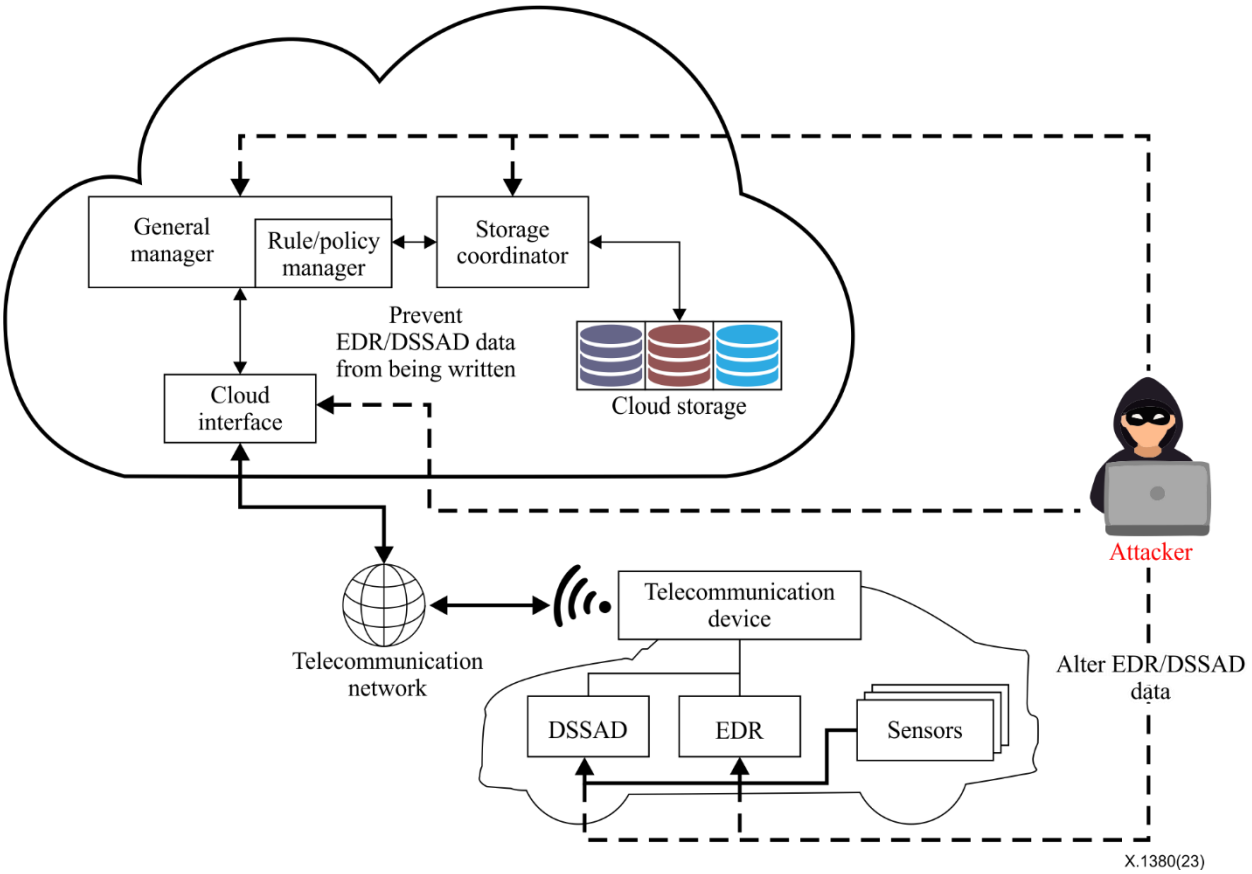

Figure 11 – Manipulate the control flow on cloud-based data recorder systems

By manipulating the control flow of a cloud-based data recorder system, an attacker might alter EDR/DSSAD data or prevent EDR/DSSAD data entries from being written. For example, the attacker identifies and accesses the debug interface on the printed circuit board (PCB) of the EDR/DSSAD and uses this interface to manipulate the executed code. Further, an attacker can manipulate firmware

or EDR/DSSAD rules on the EDR/DSSAD. The attacker can also modify bus traffic and manipulate EDR/DSSAD log.

In the case of the cloud system, the attacker can access the storage and manipulate the EDR data, audit logs and cloud policy by using malware and insecure application programming interfaces (APIs).

Figure 11 shows the attack of manipulating the control flow on the cloud-based data recorder system.

8.2.3 Threats to authenticity

A man in the middle, impersonation, and replay attack may be typical threats to authenticity.

– **Man in the middle attack**: In a cloud-based data recorder system, the attacker can intercept messages being transmitted between a vehicle and a cloud or the cloud and a user, and then retransmit them with arbitrarily manipulated messages. The sender does not recognize that the receiver is an unknown attacker trying to access or modify the message before retransmitting it to the receiver. Thus, the attacker can control the entire communication between them.

– **Impersonation attack**: An impersonation attack can be done in four ways in a cloud-based data recorder system:

  • False retrieve request of EDR/DSSAD data to the cloud system;

  • False rule update request of a designated vehicle to the cloud system;

  • Request to store false EDR/DSSAD data to the cloud system;

  • False rule update to vehicle EDR/DSSAD system.

  Impersonation attacks can cause serious harm to the integrity of the whole cloud-based data recorder system because they can generate fake event data or change event rules/policies. Also, an attacker can leak private data stored in the cloud system through an impersonation attack.

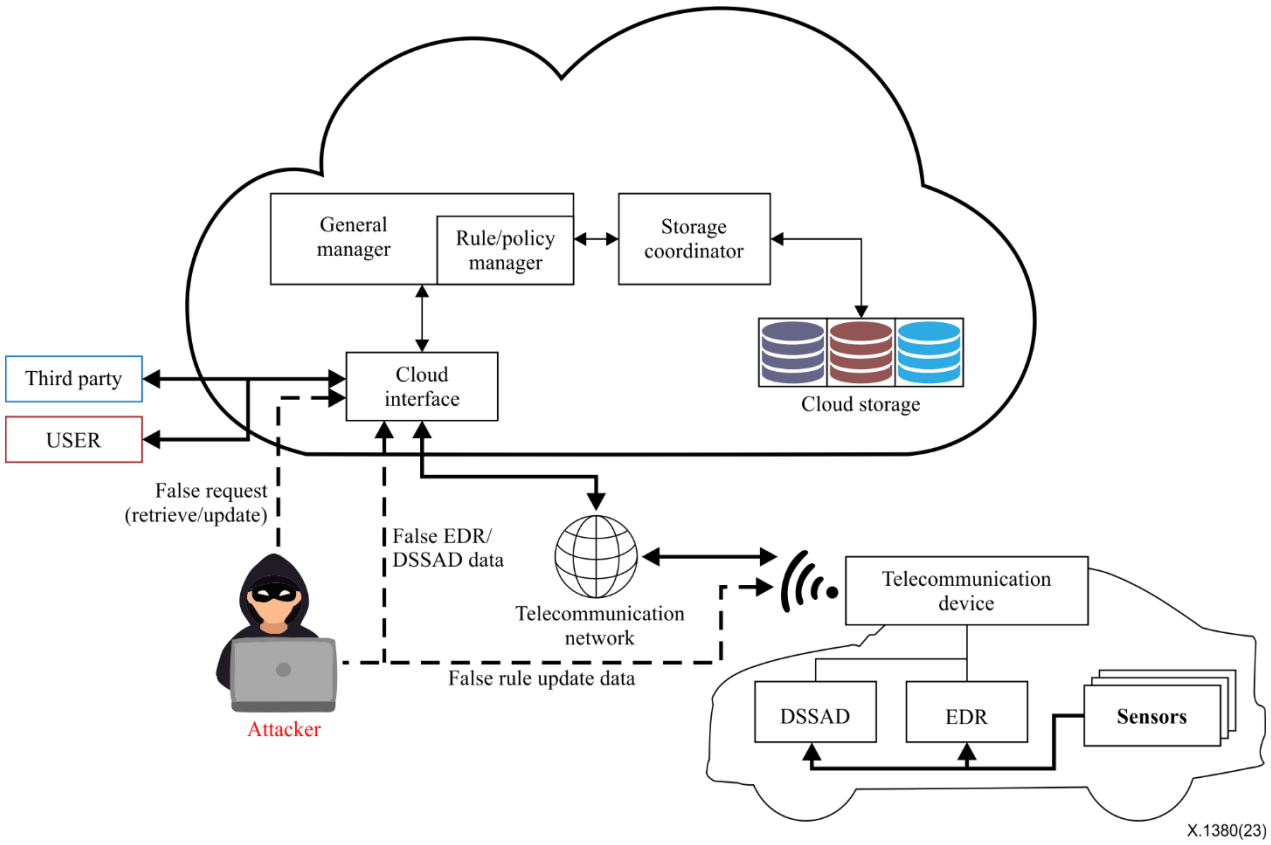

Figure 12 – Impersonation attack on cloud-based data recorder systems

– **Replay attack**: EDR/DSSAD data duplication and unwanted rule/policy rollback can be take place by replay attack.

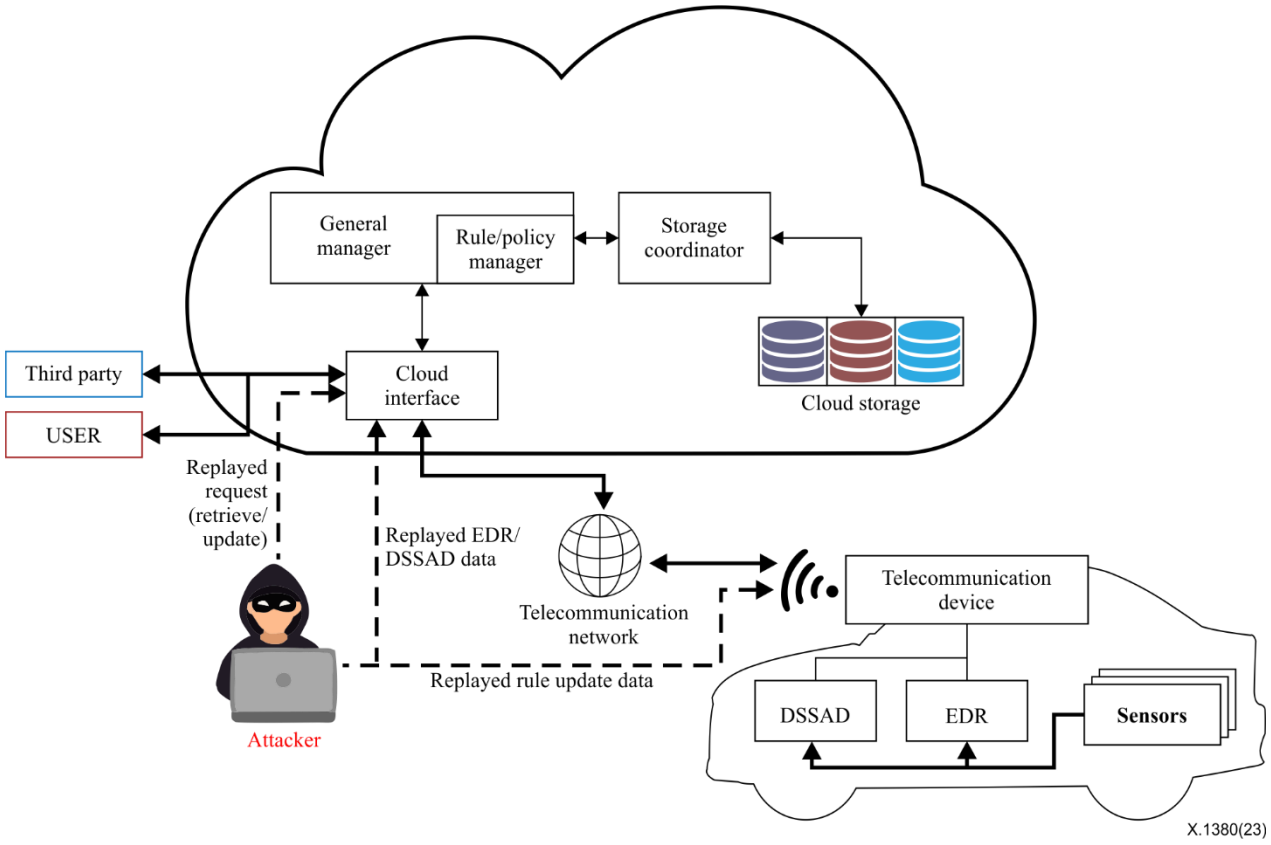

Figure 13 – Replay attack on cloud-based data recorder systems

– **Physical access**: If the attacker can access the vehicle via the debug port, another set of attacks can be performed. A joint test action group (JTAG) is the most common interface as a debug port. Access via JTAG provides the ability to read and write memory, which leads to manipulating firmware and compromising security measures.

  Diagnostics is another physical access to the vehicle. An attacker can access the OBD-II port using diagnostic tools or directly to a gateway that has remote diagnostic functions. Unified diagnostic service (UDS) is a standard protocol of diagnostics that allows monitoring and manipulating of the in-vehicle network and the ECUs in the vehicle.

8.2.4 Threats to availability

Availability is a critical factor for a cloud-based data recorder system because useful information about accidents or crashes can be stored at any time. A denial of service (DoS) attack is the most famous threat to availability.

– **DoS attack**: DoS attacks can have serious consequences for cloud-based data recorder systems because an attacker tries to block the principal means of communication/storage/ management of EDR/DSSAD data which results in making a cloud-based data recorder system meaningless in the aspect of accident analysis. As an example of DoS attacks, flooding the network channel, with high volumes of messages generated by an attacker, can paralyze the network nodes or the entire cloud systems. The network nodes (in vehicle or cloud system) will not be able to handle the huge amount of received data, and causes a malfunction in storing the EDR/DSSAD data to the cloud systems or updating the rule/policy in-vehicle and cloud systems.

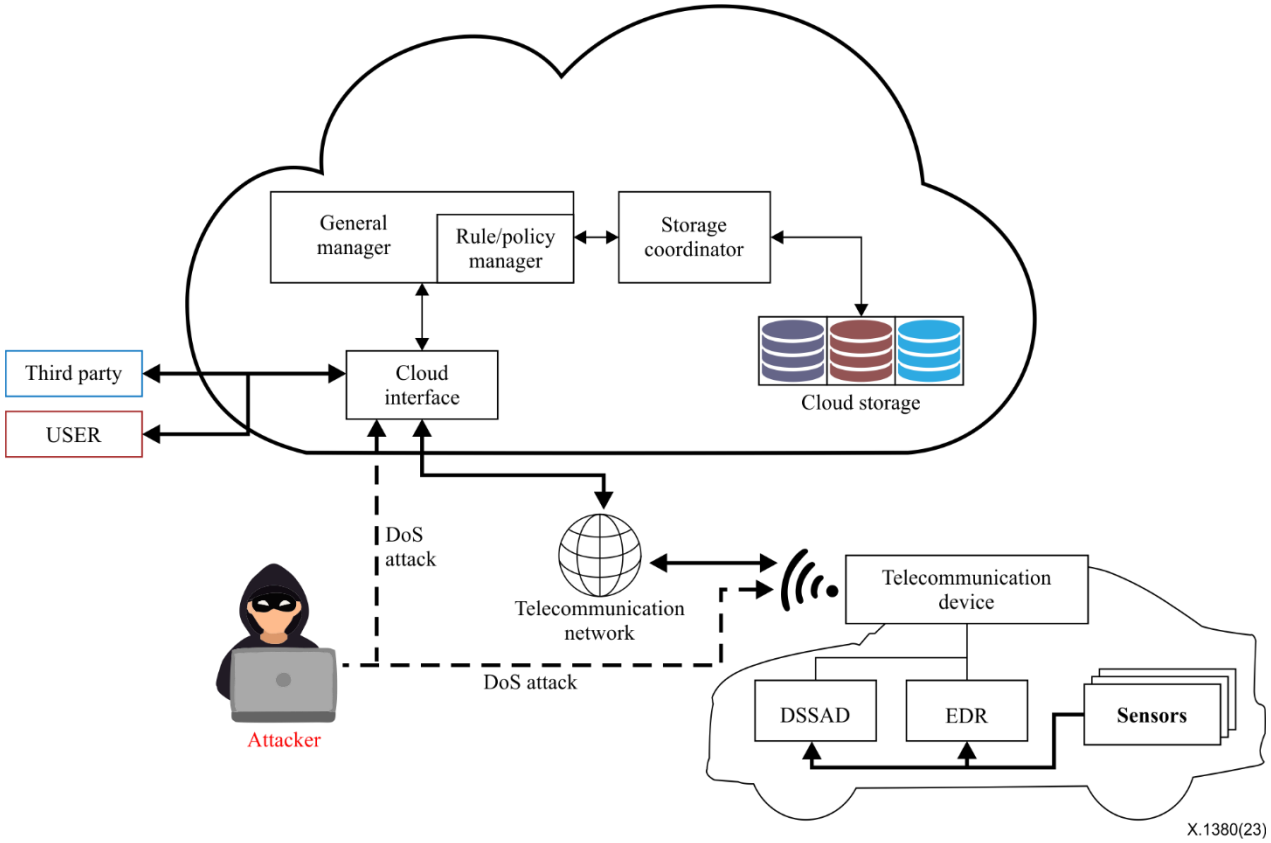

Figure 14 – DoS attack on cloud-based data recorder systems

8.2.5 Threats to accountability

– **Loss of events traceability**: Components such as rule/policy manager and storage coordinator included in the cloud system works according to the rule/policy set which is installed by the user with authority. Therefore, managing the rule/policy change log is very important in terms of accountability. An attacker can create confusion by tampering with or deleting the event log.

9 Security requirements

9.1 Secure boot

It is recommended that the firmware stored in the memory of the EDR/DSSAD devices should be checked for integrity before or during execution. It is also recommended that EDR/DSSAD rules and related configuration, and calibration data should also be checked for integrity.

The protection process of firmware and rules consists of two steps. Firstly, during the installation of firmware and rules, they are tested for authenticity before being written to the internal memory and then configured as the current firmware and rules. Secondly, during each boot, the current firmware and rules are checked for integrity.

It is recommended that the secure boot mechanism should employ either symmetric or asymmetric cryptographic means to verify the integrity of the firmware and rules with adequate levels of security. It is also recommended that the EDR and DSSAD devices should use a hardware trust anchor such as a hardware security module (HSM) to store cryptographic keys safely and accelerate the computation of cryptographic algorithms.

9.2 Secure log

It is required that the integrity of the logging data should be ensured using secure cryptographic methods. Since EDR/DSSAD data are pieces of evidence for specific situations, EDR/DSSAD data should be protected from unauthorized manipulations.

In the case of the cloud system, the general manager should put logs at each case as given below:

– Authentication attempts from users/third parties;

– Policy update.

It is recommended that logs should be stored securely. Cryptographic measures such as a message authentication code (MAC) can be attached to the logs and/or stored in a secure storage with adequate access control. Minimum log storage retention should be defined following the policy of a cloud service provider or the regulation of each country.

9.3 Secure communication

The cloud-based data recorder systems have several communication channels as given below:

– Communication between cloud systems and vehicles;

– Communication between users/third parties;

– Communication between ECUs, sensors and actuators in vehicles.

It is recommended that the confidentiality and authenticity of the messages in communication between the cloud system and vehicles or users/third parties should be ensured. Confidentiality and authenticity can be achieved by using cryptographic measures such as transport layer security (TLS).

It is also recommended that the communication between the cloud system and vehicle should ensure availability. It means that a huge amount of EDR and DSSAD data from numerous vehicles should be stored in the cloud storage appropriately.

It is recommended that the integrity of messages and data in communication between ECUs, sensors, and actuators in vehicles should be ensured to generate correct EDR/DSSAD data, because data from the ECUs and sensors are related to crash events or the driving activities.

9.4 Secure access

It is recommended that debug interfaces such as JTAG on the EDR/DSSAD device, which are not mandatory for field operation should be disabled and should not bypass the secure boot. The debug interface disabling method are classified as follows:

– Permanently removed;

– Conditionally disabled by applying access control.

In the case of re-enabling the debug interfaces for warranty return analysis, the debug interfaces should only be accessible by authorized and authenticated parties. It is recommended that the privileges of applications receiving on hardware and software interfaces should be limited according to the principle of least privilege.

It is recommended that security-critical functions and data via diagnostic commands and requests should be protected by a cryptographic mechanism. This means that the subject who wants to access EDR/DSSAD device should be authenticated before sending commands.

9.5 Secure update

It is recommended that the update procedure of firmware and rules should ensure authenticity and integrity, i.e., only authenticated and unmodified update packages are permitted to be flashed. In addition, it is recommended that the firmware and rules should not be downgraded to a prior version to prevent using former security vulnerabilities maliciously. It is also recommended that the OTA packages should be transmitted through a secure channel that is protected by cryptographic methods.

9.6 Relationship of identified threats and security requirements

The following Table 3 provides mapping information between the identified threats in clause 8 and the security requirements.

Table 3 – Relationship of identified threats and security requirements

Security requirements	Threats	Security objectives
Secure boot	Manipulate the control flow – manipulate the firmware – manipulate EDR/DSSAD rules	Integrity of EDR/DSSAD rules stored in vehicles Integrity of EDR/DSSAD firmware
Secure log	Manipulate the control flow – manipulate logs Loss of event traceability	Integrity of EDR/DSSAD data in vehicles, Integrity of cloud log
Secure communication	Eavesdropping Sniffing by wiretapping Manipulate the control flow Man in the middle attack Impersonation attack Replay attack DoS attack	Confidentiality and/or integrity of bus traffic Confidentiality and authenticity of communication with back-end systems Availability of back-end systems
Secure access	Physical access	Confidentiality and/or authenticity of communications with debugging/diagnosing.

Table 3 – Relationship of identified threats and security requirements

Security requirements	Threats	Security objectives
Secure update	Eavesdropping Manipulate the control flow – manipulate EDR/DSSAD rules Impersonation attack	Confidentiality and integrity of the OTA package

10 Implementation guidelines for cloud-based data recorder systems

Strict data protection is required on using and managing EDR/DSSAD data in cloud-based data recorder systems. Cloud-based data recorder systems further give functionality to research and development for safer vehicles by using recorded data which conventional data recorders cannot provide. This clause introduces the implementation guidelines for a cloud-based data recorder system.

10.1 Cloud storage separation

Due to the essentiality of VII in a cloud-based EDR/DSSAD system, it is required to protect VII securely. Physically separating EDR/DSSAD data and its VII is required in cloud-based EDR/DSSAD systems. It not only provides security benefits, but also allows additional functions such as providing third party EDR/DSSAD data without any privacy violations. The storage should be physically separated and separately managed in independent storages. Storage for VII (described as VII database in Figure 15) requires a higher security level than other data due to its relative importance.

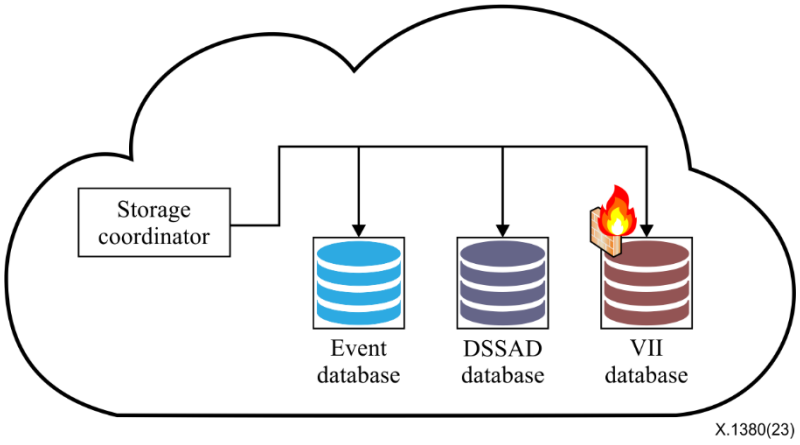

Figure 15 – Storage separation

10.1.1 Data storing procedure

To ensure confidentiality and authenticity of communication data with a back-end, a secure channel should be established in advance before EDR/DSSAD data is sent from a vehicle to the cloud system.

When data is delivered to the storage coordinator from a vehicle through a cloud interface, the storage coordinator separates the EDR/DSSAD data and the VII. After the separation, the storage coordinator generates the link data to make the EDR/DSSAD data tangled with the VII data. Then, two data sets get stored in different storages (databases). As described in Figure 16, VII and EDR/DSSAD data with link data get stored in the VII database and in the event/DSSAD database accordingly. After the storing procedure, the result of the storing process, success or failure of the data storing procedure should be logged.

One of the most important things in data storage procedures is to comply with the relevant regulations such as the General Data Protection Regulation (GDPR). Therefore, getting consent from a data owner is recommended before collecting any data from the vehicle.

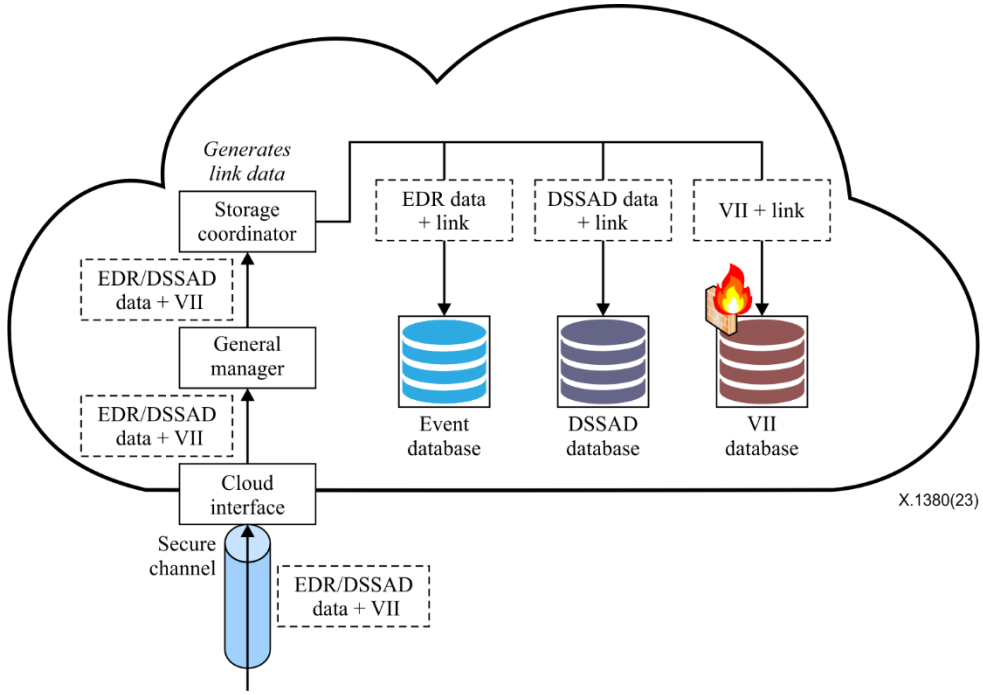

Figure 16 – Storing procedure of storage separation

10.1.2 Data retrieving procedure

Retrieving EDR/DSSAD data procedure starts with the EDR/DSSAD data retrieval request from the user/third party. When the user/third party accesses the cloud system, the cloud interface should authenticate the user/third party and log all the attempts. If the authentication succeeds, the storage coordinator uses the presented VII to find the link data in the VII database (refer to Figure 17 (a)). With the found link data, the storage coordinator searches for the EDR/DSSAD data. When the EDR/DSSAD data is found, the storage coordinator provides the data to the requesting party after the general manager's access control procedure differs by the authorization level of the requesting party. Retrieving VII data is restrictively allowed and a high level of authority is required. On the other hand, EDR data or DSSAD data which does not include VII can be retrieved by the third party. EDR data or DSSAD data can be retrieved without the VII search process when the VII data is deleted and transferred to a separated neutral server (refer to Figure 17 (b)).

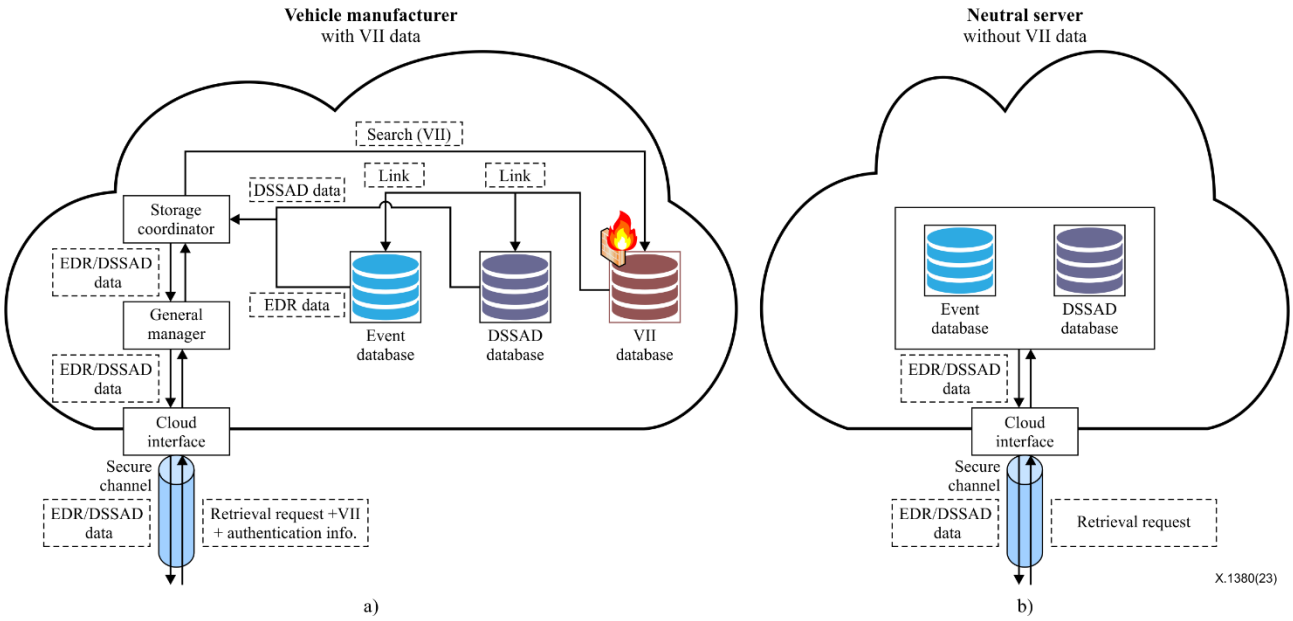

Figure 17 – Retrieving procedure of storage separation

10.1.3 Data deletion procedure

The cloud system for EDR/DSSAD should obtain the user's consent including the expiration date or the duration of the recorded data for the collected VII data. When the expiration date or given duration of the stored data comes due, the collected data should be deleted automatically from the cloud system.

When users request to delete their data before the expiration date, the cloud systems should delete the data according to the request. When a user requests deletion, the cloud interface should authenticate the user and log all attempts. If the authentication succeeds, the storage coordinator should use the presented VII to find the link data that is stored in the VII database. With the found link data, the storage coordinator should search for the EDR/DSSAD data and delete it when found. The storage coordinator should then store the log regarding the result of the deletion and report the result to the requesting party.

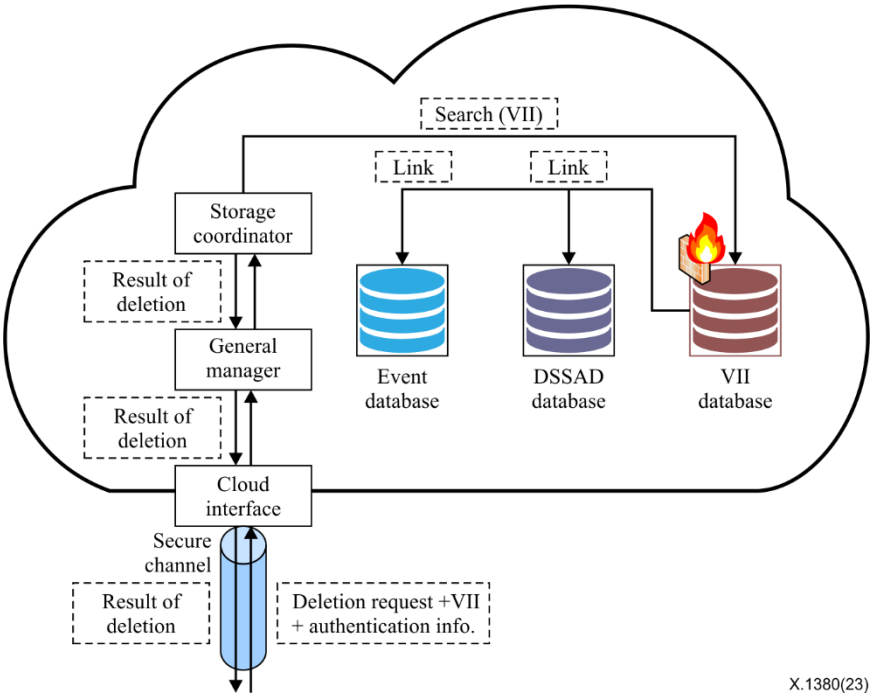

Figure 18 – Deletion procedure of storage separation

10.2 Cloud service registration

The registration procedure of cloud-based data recorders in automotive environments is shown in Figure 19.

Referring to Figure 19, if an authentication request for the registration of a cloud-based data recording service, i.e., a vehicle authentication request, is received from a vehicle in a service execution mode in step 1, the ID of the vehicle should be verified, e.g., using a digital signature algorithm of a public key cryptosystem, in step 2. Herein, the authentication request of the vehicle may be performed in a manner of transmitting a message signed with a private key of the vehicle to the cloud-based data recording service system. As a result of the verification in step 2, if the ID of the vehicle is determined to be invalid, the cloud-based data recording service system generates a corresponding authentication failure response and transmits this response to the vehicle, as shown in step 3.

As the result of the verification in step 2, if the ID of the vehicle is determined to be valid, the cloud-based data recording service system generates an authentication response for the vehicle and transmits this response to the vehicle, as shown in step 4.

Thereafter, when the authentication response is received, i.e., the authentication of the vehicle is achieved, after a user inputs and generates the cloud-based recording service registration information including recoding data types and reporting period, etc., the vehicle transmits the cloud-based data recording service registration information to the cloud-based data recording service system to thereby request the registration of the cloud-based data recording service, as shown in step 5.

Subsequently, if a request for the registration of the cloud-based data recording service, which includes the cloud-based data recording service registration information, is input from the vehicle, the cloud-based data recording service system generates a security policy using the cloud-based data recording service registration information such as the recording data types and recording period, and so on, and then stores/registers the information, as shown in step 6.

After that, the cloud-based data recording service system assigns a pseudonym to each vehicle, as shown in step 7, generates a certificate request message for requesting the generation of a pseudonym certificate for the pseudonym assigned to each vehicle, and transmits the certificate request message to the authentication centre, as shown in step 8.

The cloud-based data recording service system monitors whether or not the pseudonym certificate is acquired from the authentication centre in step 9. As a result of the monitoring, if the pseudonym certificate is secured, the cloud-based data recording service system stores the pseudonym certificate in the cloud-based data recording information DB. The pseudonym certificate may be a digitally signed message from the authentication centre. It is possible to guarantee the justification of the pseudonym through the pseudonym certificate.

A plurality of pseudonyms may be assigned to each vehicle. Since the pseudonym does not have information associated with an ID of each vehicle, it is possible to protect the PII of each vehicle.

If the notification is received thereto, the cloud-based data recording service system generates cloud-based data recording service registration information for each vehicle, stores the information DB, and transmits the same to each vehicle in step 10. Herein, the cloud-based data recording service registration information may include a pseudonym assigned to each vehicle, a pseudonym certificate for the pseudonym, and so on. Each vehicle, i.e., a user of the vehicle, in the cloud-based data recording service that is registered can accomplish the cloud-based data recording by performing communications between the cloud centre and vehicles using the cloud-based data recording service registration information provided from the cloud-based data recording service system.

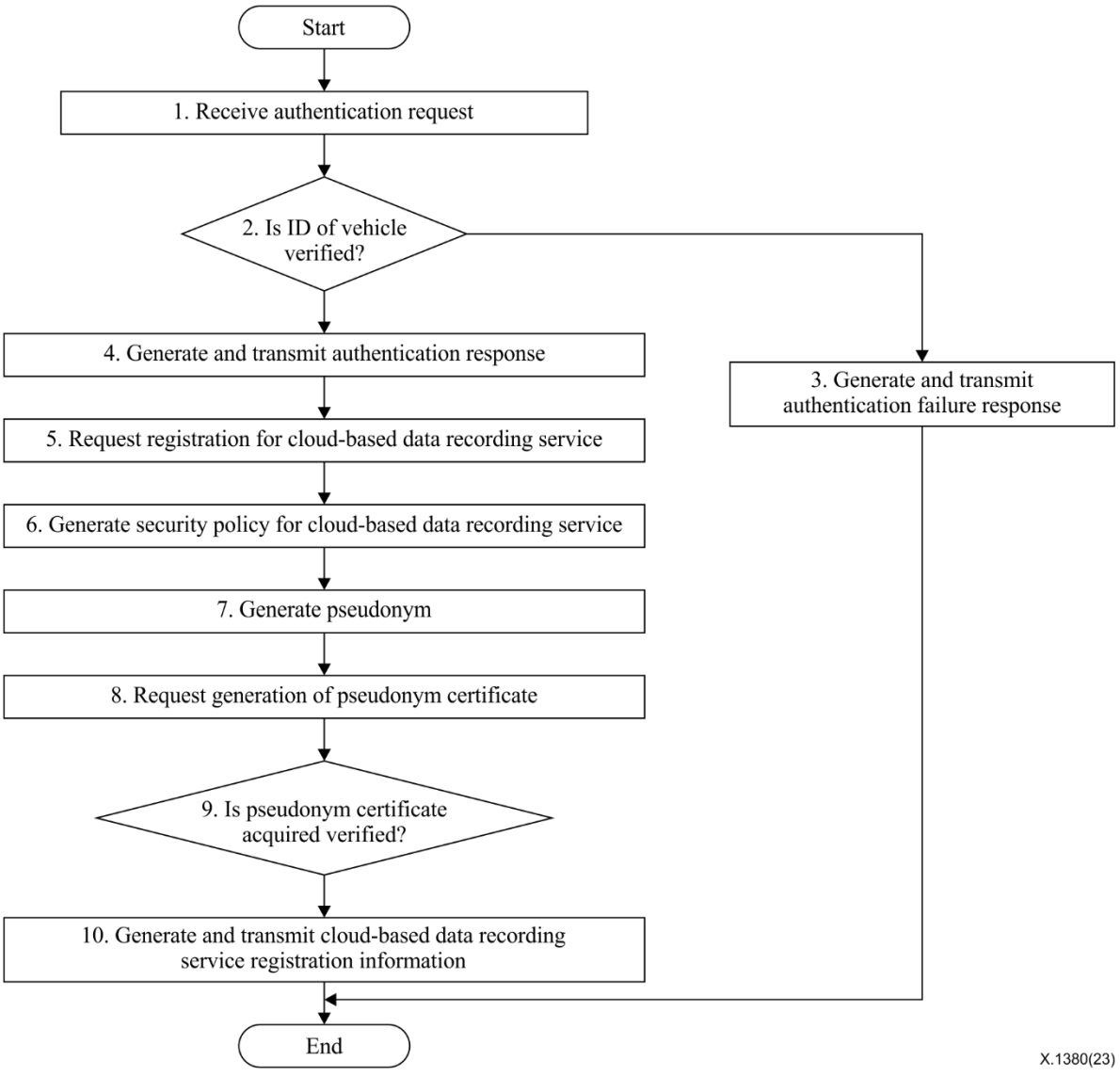

Figure 19 – Cloud-based data recording service registration

The deregistration procedure of cloud-based data recorders can be considered for use cases such as car rentals, used vehicles, etc. because changed car owners do not want to provide EDR/DSSAD data to the cloud system.

11 Use cases for cloud-based data recorders in an automotive environment

When a car accident occurs, EDR/DSSAD data can be used meaningfully to analyse the cause of an accident and to determine whether the vehicle and the driver are responsible. Figure 20 shows the flow of EDR/DSSAD data. The EDR/DSSAD data generated in the vehicle is transmitted to the cloud through wireless communication. A vehicle owner, manufacturer, suppliers, or authorized third parties (e.g., insurance companies) can utilize the EDR/DSSAD data in the cloud.

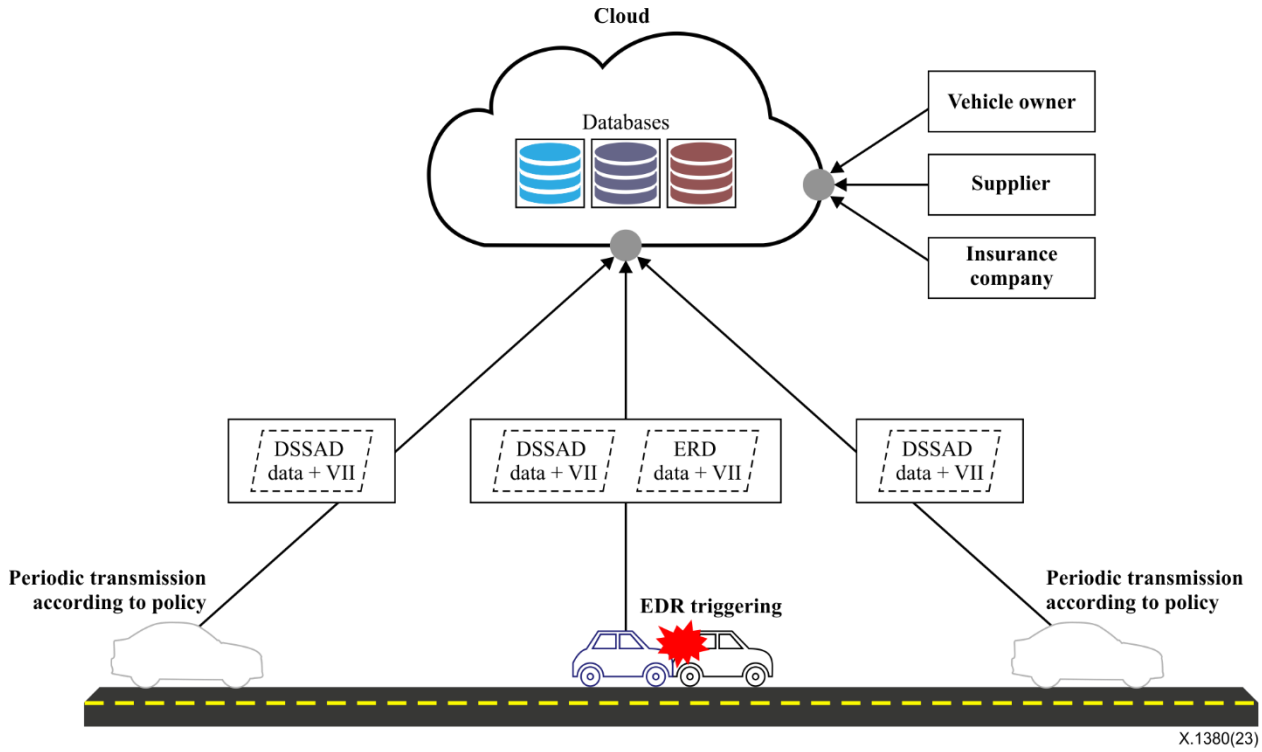

Figure 20 – The flow of EDR/DSSAD data

A cloud-based data recorder system has many advantages. Firstly, it is easy to obtain EDR/DSSAD data, even in potential risk situations (e.g., vehicle fires, vehicle flooding). Secondly, authorized accident analysts can acquire data from the cloud system more easily than ECUs in a vehicle directly.

11.1 Case 1: A crash between vehicles

Figure 21 shows a scenario in chronicle order when a vehicle equipped with an automatic lane keeping system (ALKS) is driving on the road. The car accident occurs at (e) and an EDR event is triggered. The cloud stores the EDR/DSSAD data from (a), when ALKS is activated, to (e), when the accident occurs. The stored EDR/DSSAD reports the following information:

Since ALKS is activated by the driver at 10:19:10, the system is handed over the control of the vehicle. After 1 minute 50 seconds, the weather deteriorates and the ALKS asks the driver to transit control of the vehicle, but the driver does not respond. ALKS then automatically initiates a minimum risk manoeuvre (MRM) at 10:22:00. And the crash then occurs at 10:22:30.

Through analysis of EDR/DSSAD data, it is possible to check the period and circumstance of the accident. The cloud-based data recorder systems store the EDR/DSSAD data in the storage at the cloud system by the predefined data transfer policies. Thereby, reducing the efforts of gathering the crash information compared to direct retrieval from the EDR storage in the vehicle.

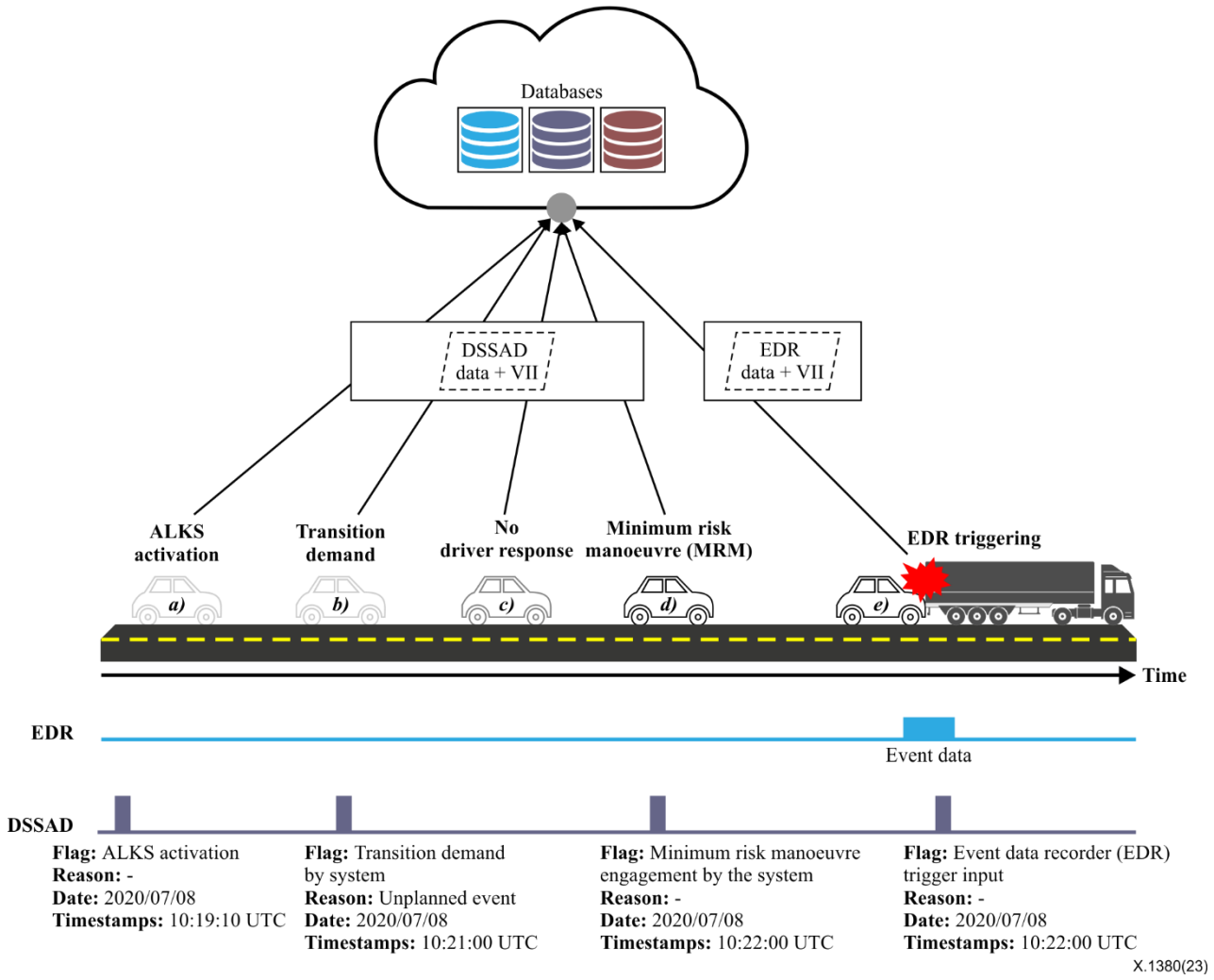

Figure 21 – A crash between vehicles

11.2 Case 2: A collision between a vehicle and a bike

Figure 22 shows a scenario in chronological order when a vehicle equipped with an ALKS is driving on the road. The vehicle has a soft crash with a bike at (c), but since the impact is quite weak the EDR is not triggered. However, all the recent DSSAD data is uploaded to the cloud. The stored EDR/DSSAD reports the following information:

> ALKS is activated by a driver at 10:19:10. After 15 seconds, the driver operates the steering directly and then the ALKS gets deactivated. The crash between vehicle and bike occurs at 07:10:16.

In this case, the impact on the vehicle is so slight that the EDR triggering condition is not met and no EDR data is gathered. Nevertheless, the detailed accident situation can be simulated and analysed easily because DSSAD data is stored in the cloud system.

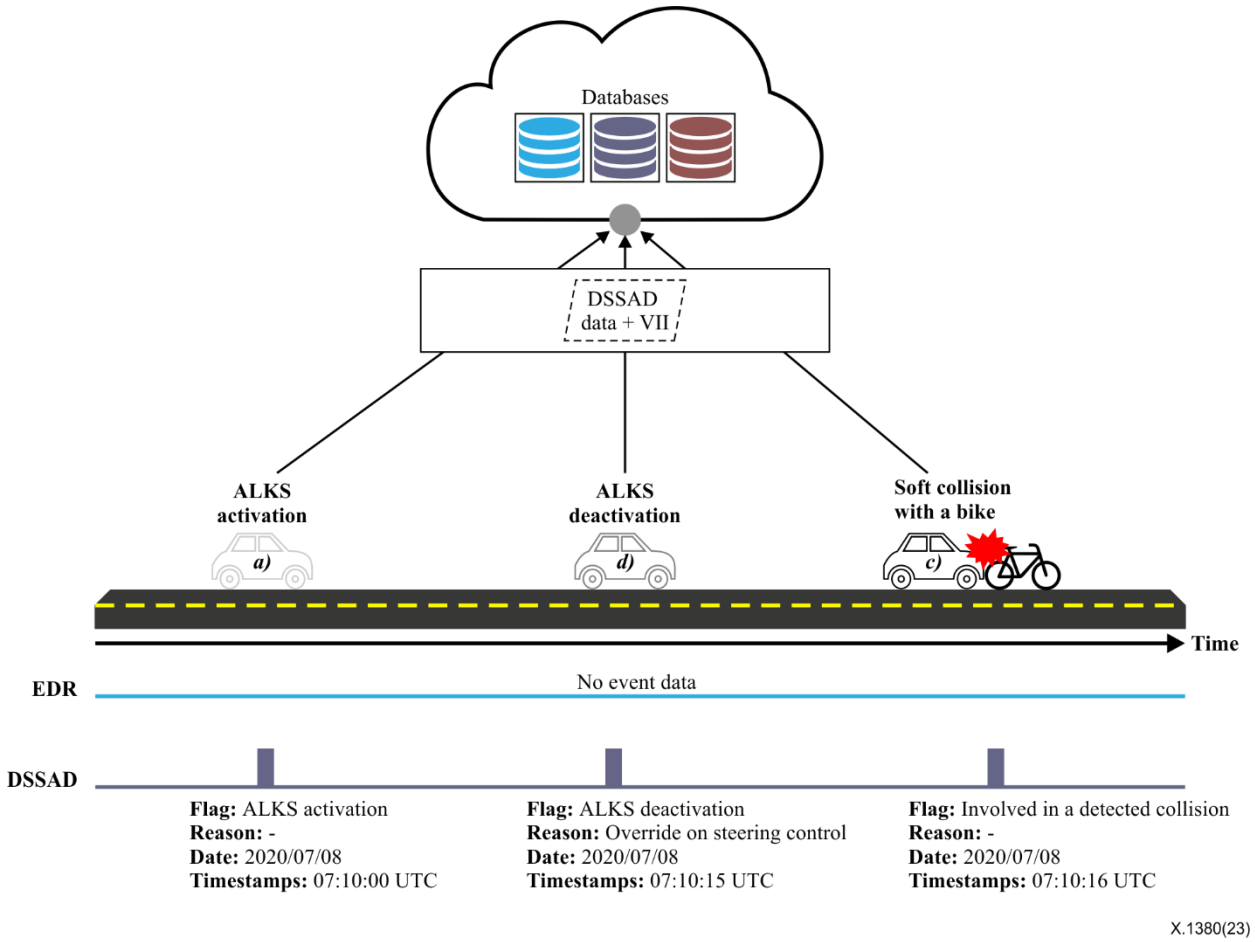

Figure 22 – A crash between a vehicle and bike

Appendix I

(This appendix does not form an integral part of this Recommendation.)

Example of conventional EDR data set

This example dataset is a required essential data element for conventional EDRs in the United States of America (USA), regulated by the NHTSA (National Highway Traffic Safety Administration).

Table I.1 – Required essential data elements in conventional EDR [b-NHTSA EDR]

Item #	Data Elements	Recording Time*	Sampling Rate	Range	Accuracy	Resolution
1	Delta-V, Longitudinal	0 – 250 ms or 0 to end of event plus 30 ms, whichever is shorter	100/s	-100 to 100 km/h	± 10%	1 km/h
2	Maximum delta-V, Longitudinal	0 – 300 ms or 0 to end of event plus 30 ms, whichever is shorter	N.A.	-100 to 100 km/h	± 10%	1 km/h
3	Time, Maximum delta-V, Longitudinal	0 – 300 ms or 0 to end of event plus 30 ms, whichever is shorter	N.A.	0 – 300 ms or 0 to end of event plus 30 ms, whichever is shorter	± 3 ms	2.5 ms
4	Speed, vehicle indicated	-5.0 to 0 s	2/s	0- 200 km/h	± 1 km/h	1 km/h
5	Engine throttle, % full (accelerator pedal % full)	-5.0 to 0 s	2/s	0 – 100%	± 5%	1%
6	Service brake, on/off	-5.0 to 0 s	2/s	On/off	N.A.	On/off
7	Ignition cycle, crash	-1.0 s	N.A.	0 – 60,000	± 1 cycle	1 cycle
8	Ignition cycle, download	At time of download	N.A.	0 – 60,000	± 1 cycle	1 cycle
9	Safety belt status, driver	-1.0 s	N.A.	On/off	N.A.	On/off
10	Frontal air bag warning lamp	-1.0 s	N.A.	On/off	N.A.	On/off
11	Frontal air bag deployment time, Driver (1st stage, in case of multi-stage air bags)	Event	N.A.	0 – 250 ms	±2 ms	1 ms
12	Frontal air bag deployment time, RFP (1st stage, in case of multi-stage air bags)	Event	N.A.	0 – 250 ms	±2 ms	1 ms
13	Multi-event, number of events (1 or 2)	Event	N.A.	1, 2	N.A.	1, 2
14	Time from event 1 to 2	As needed	N.A.	0 - 5.0 s	0.1 s	0.1 s
15	Complete file recorded (yes or no)	Following Other Data	N.A.	Yes/no	N.A.	Yes/no

Bibliography

[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)*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2023