

### Differences between EDR & DSSAD

Key: CLEPA-OICA inputs are indicated **green**

		EDR for conventional vehicles	EDR for ADS	DSSAD for ALKS
<b>System</b>				
	<b>Purpose</b> (why do the contracting parties want to introduce this function into the vehicle?)	<ul style="list-style-type: none"> <li>Accident reconstruction through:               <ul style="list-style-type: none"> <li>- Assessment of the dynamic behaviour of the vehicle before and after an impact and</li> <li>- Assessment of the behaviour of the occupant protection systems</li> </ul> </li> </ul>		Clarify if the system or the driver <ul style="list-style-type: none"> <li>Was in dynamic control of the vehicle and/or</li> <li>Was requested to be in dynamic control of the vehicle, at a certain time.</li> </ul>
	<b>What it shall/should not do</b>	<ul style="list-style-type: none"> <li>Detect who is driving [Identifying the user/owner/holder of the vehicle on the basis of the stored data.]</li> <li>Provide any information about the surroundings of the vehicle</li> </ul>		<ul style="list-style-type: none"> <li>Provide data aimed at accident reconstruction that are already available in the EDR</li> <li>Identify the user/owner/holder of the vehicle</li> </ul>
	<b>PTI</b>	TBD No specific need for PTI because: <ol style="list-style-type: none"> <li>There are no feedback indicating difficulties to reach the EDR data after more than 10 years of usage in the USA.</li> <li>As there is no accident before a PTI, there is no data in the EDR at PTI.</li> <li>checking EDR function at PTI would then necessitate 'write and read' inside the internal safety related ECUs of the vehicle, which is contradictory with the needs of cybersecurity and brings a risk of triggering all the restraint system.</li> </ol>		TBD No specific need for PTI because DSSAD will be internally (by ALKS) self-diagnosed and it will be indicated in the ALKS regulation that ALKS does not work and can't be engaged if DSSAD does not work. As so, a malfunction of DSSAD will be visible in PTI through the dedicated information from the ALKS
	<b>Recording Period</b>	Just before & during crash <i>Reference: "5s before events 300ms after event" in Part 563</i>		Records timestamped flags while ALKS operates (there is no need for any sampling of any continuous parameter for DSSAD)

		<b>EDR for conventional vehicles</b>	<b>EDR for ADS</b>	<b>DSSAD for ALKS</b>
	<b>System storage capabilities</b>	1+ 1subsequent “EDR event” (multi event during 5 sec only if main (12V) battery not out of order)		Records “ALKS/driver interactions after ALKS is turned ON until it is turned OFF (“disengaged””, With a dual limitation of [ X.000 of timestamped flags / X months], first to be achieved. (TBC according to ACSF) (regardless to crash)
	<b>System <del>crash</del> survivability</b>	For vehicles in the scope of R94: Resistance to R94 crash test for a minimum of 300 milliseconds (EDR does not have to record anything later than 300 ms after that kind of crash) For other vehicles: agreement with Technical Service.  For all vehicles: no survivability to immersion of fire (as in CFR)		No recording required after an EDR is triggered (for vehicles in the scope of R94): there is no “driver/ALKS interaction” after a R94 crash  For all vehicles: no survivability to immersion of fire (as in CFR)
	<del>Battery restitution</del> <b>Data survivability after a crash event</b>	All data mandatory per the table, must be stored and retrievable after R94 crash test.		All the data mandatory per DSSAD regulation must be stored and retrievable after R94 crash test  ACSF to confirm what they expect.
	<b>“event” definition</b>	“Event” means a crash or other physical occurrence that causes the trigger threshold to be met or exceeded, <del>or an airbag a non-reversible restraint system</del> to be deployed, whichever occurs first.		<del>[Event: e.g. change of HAD system status, TD emission, MRM engagement/end, TO].</del> <b>DSSAD does not record any trace of that kind of “event” that triggers EDR, and is not triggered by any “event” of this kind.</b>
	<b>Environmental robustness (vibrations, etc.)</b>	Out of this regulation scope: the vehicle is crashed when data are stored, and not subject to any specific vibrations or else		Self-diagnosis system: if the DSSAD does not work, ALKS is not available. (= no specific risk related to DSSAD itself)
	<b>Malfunction detection</b>	There are no feedback indicating difficulties to reach		Input from ACSF is expected: DSSAD will be internally (by

		EDR for conventional vehicles	EDR for ADS	DSSAD for ALKS
		the EDR data after more than 10 years of usage in the USA.		ALKS) self-diagnosed and it will be indicated in the ALKS regulation that ALKS does not work and can't be engaged if DSSAD does not work.
<b>Data technique</b>	<b>Where to store (in the vehicle vs. the cloud)</b>	A Technical Regulation should be technology neutral. The request is that "Data are available and retrievable" according to the request (For EDR = "after event" / For DSSAD = "when requested, including after an event that triggers EDR")		
	<b>Data format</b>	The final authorized user (will be defined by each National Legislation) must get data in comprehensive format, without any risk of corruption.		
	<b>Data element</b>	Refer to text proposal by OICA (NB: any engagement/disengagement of ALKS is visible through the DSSAD data as well as any significant interaction between the ALKS and the driver		Refer to text proposal by OICA : basically "engagement (ON), disengagement (OFF) of the system, and all significant interaction between the ALKS and the driver in the meantime.
	<b>Storing duration</b>	not less than 10 days after EDR is triggered (to be checked at Type Approval)		[X] months if EDR is not triggered (to be determined according to storing capacity)  "not less than 10 days after EDR is triggered" (same as EDR)
	<b>Retrieval means</b>	A Technical Regulation should be technology neutral. The request is that "Data are available and delivered in due time" according to the request (For EDR = "after event" / For DSSAD = to be determined)		
	<b>Accuracy</b>	Refer to table incorporated in the draft		<ul style="list-style-type: none"> <li>• Accuracy of timestamp to be determined and indicated in the text</li> <li>• The "data elements" must be stored in the order of occurrence.</li> </ul>
	<b>Access means</b>	See "retrieval means"		
	<b>Erasing means (?)</b>	FIFO type, when the memory is full (see "storage capabilities") No erase by any mean except the overwriting of the system		
	<b>Sampling rate</b>	Refer to table incorporated in the draft		Not Applicable
	<b>Data identification (this data really belongs to that vehicle)</b>	This question goes far further the technical requirements (stops at retrieval): In the case the data are "on board", the VIN number of the vehicle is available on the vehicle itself.		

		<b>EDR for conventional vehicles</b>	<b>EDR for ADS</b>	<b>DSSAD for ALKS</b>
		In the case the data are “outboard”, the VIN number of the vehicle that provides the data will be incorporated in the data set, and the management of the data will be compliant with the local rules applying to “road safety related data privacy” (GDPR or else).		
	<b>Triggering parameter</b>	See “event definition”		Records permanently a set of timestamped significant interactions between the ALKS and the human driver, after the ALKS is engaged, and until it is disengaged, with no need for any other trigger.
<b>Data usage</b>	<b>Data ownership</b>	Out of the scope of a technical regulation		
	<b>Data protection (privacy)</b>	Out of the scope (legal aspects covered nationally / security covered by regulation for cybersecurity)		
	<b>Information to the user (driver, vehicle owner)</b>	See text proposal by OICA		To be determined
	<b>Who must access which data?</b>	Out of the scope (but important to know because of technical impact)		
	<b>Plausibility</b>	Not feasible to challenge the reliability of the Inputs. Keep current practise with current EDR: “data coming from vehicle sensors/information”		
	<b>Authorization process</b>	Out of the scope (probably covered on a national basis)		
	<b>How fast to deliver the data to a third party</b>	Out of the scope (it will be covered by the same national law that will establish “who is authorized to get the data”)		
	<b>Cybersecurity</b>	Covered by another Technical Regulation under establishment		