Draft Proposal Regarding AECD / AECS Self-Test and Status Indication

1 Background

The current draft of the AECS UN Regulation contains different requirements regarding the self-test and malfunction indication for AECD and AECS, which have not been agreed or harmonised yet by the working group.

Draft AECS UN Regulation (AECS-02-02-r4), Paragraph 6.5.2.:

> *"A warning signal shall be provided in case of AECD internal malfunction. Visual indication of the AECD malfunction shall be displayed while the failure is present. It may be cancelled temporarily, but shall be repeated whenever the device which starts and stops the engine is switched on and off."*

Draft AECS UN Regulation (AECS-02-02-r4), Paragraph 15.3.3.:

> *"A warning signal shall be provided when the onboard AECS is not functioning properly. Visual indication of the AECD malfunction shall be displayed at all times while ignition is turned on or the vehicle master control switch is activated (whatever applicable)."*

As per the proposal by the Russian Federation, the current draft of the AECS UN Regulation also requires a post-crash assessment of the malfunction indication, which indirectly includes elements that need to be covered by the self-test.

Draft AECS UN Regulation (AECS-07-02), Annex 6, Paragraph 5.:

> "*5. HMI operation assessment shall include the following*
>
> *[…]*
>
> *5.3. Malfunction indication is working properly. This is verified by checking malfunction indication in at least one of the following conditions:*
>
> *5.3.1. Communication module antenna is disconnected, or*
>
> *5.3.2. GNSS receiver antenna is disconnected, or*
>
> *5.3.3. Microphone(s) is (are) disconnected, or*
>
> *5.3.4. Loudspeaker(s) is (are) disconnected, or*
>
> *5.3.5. AECD control module is disconnected from the HMI module*"

In any case, a warning shall be given to the occupants of a vehicle in the event of a system failure which would result in an inability to execute an emergency call. This needs to be verified for type-approval. The background to this stipulation is that the emergency call function is only used in very rare occasions, which means that the vehicle user would not have the opportunity to pick up malfunctions of the system without a self-test and malfunction indicator associated with the IVS.

A procedure has been developed that allows the technical service to verify the self-test and malfunction indication requirements based on a physical test and supporting documentation (see Section 3, page 5). The procedure applies to AECD or AECS.

2 Context: Relevant legislative material

2.1 GOST R 54620

The Russian standard GOST R 54620 defines the self-test requirements for ERA-GLONASS systems. The requirements are restricted to apply "*whenever technically feasible*". The requirements are:

GOST R 54620, Section 6.17.6:

"Whenever technically feasible, the following checks during IVS self-tests shall be carried out:

- *integrity of software image;*
- *operational condition of GSM/UMTS communication module interface;*
- *operational condition of GNSS receiver;*
- *integrity (dependability) of navigation and timing parameters of GNSS receiver (RAIM function);*
- *sufficient battery charge level;*
- *operational condition (correct connection) of external GNSS antenna (if installed);*
- *operational condition (correct connection) of external GSM/UMTS antenna (if installed);*
- *operational condition of automatic RTA [road traffic accident] detector (for vehicles of Categories M1 and N1 only);*
- *operational condition of UIM [the manual call button];*
- *proper connection of microphone;*
- *operational condition of microphone;*
- *operational condition of loudspeaker (loudspeakers)."*

2.2 UN Regulation No. 13-H

UN R13-H (braking) defines self-test requirements for anti-lock braking systems (ABS) and electronic stability control systems (ESC).

UN Regulation No. 13-H, Annex 6 (ABS), Paragraph 4.1.:

"Any electrical failure or sensor anomaly that affects the system with respect to the functional and performance requirements in this annex, including those in the supply of electricity, the external wiring to the controller(s), the controller(s) and the modulator(s) shall be signalled to the driver by a specific optical warning signal."

UN Regulation No. 13-H, Annex 9 (ESC), Paragraph 3.4.:

"3.4. ESC MALFUNCTION DETECTION

The vehicle shall be equipped with a tell-tale that provides a warning to the driver of the occurrence of any malfunction that affects the generation or transmission of control or response signals in the vehicle's electronic stability control system."

UN R13-H also defines certain characteristics of the malfunction indicator. While these might not be applicable, in full, to AECD/AECS, because ESC is a primary safety system, they give an indication of what is defined in other regulations.

UN Regulation 13-H, Annex 9 (ESC), Paragraph 3.4.:

"3.4.1. The ESC malfunction tell-tale:

3.4.1.1. Shall be displayed in direct and clear view of the driver, while in the driver's designated seating position with the driver's seat belt fastened;

3.4.1.2. Shall appear perceptually upright to the driver while driving;

3.4.1.3. Shall be identified by the symbol shown for "ESC Malfunction Tell-tale" below or the text "ESC":

3.4.1.4. Shall be yellow or amber in colour;

3.4.1.5. When illuminated shall be sufficiently bright to be visible to the driver under both daylight and night-time driving conditions, when the driver has adapted to the ambient roadway light conditions;

3.4.1.6. Except as provided in paragraph 3.4.1.7., the ESC malfunction tell-tale shall illuminate when a malfunction exists and shall remain continuously illuminated under the conditions specified in paragraph 3.4. for as long as the malfunction exists, whenever the ignition locking system is in the "On" ("Run") position;

3.4.1.7. Except as provided in paragraph 3.4.2., each ESC malfunction tell-tale shall be activated as a check of lamp function either when the ignition locking system is turned to the "On" ("Run") position when the engine is not running, or when the ignition locking system is in a position between "On" ("Run") and "Start" that is designated by the manufacturer as a check position;

3.4.1.8. Shall extinguish at the next ignition cycle after the malfunction has been corrected in accordance with paragraph 5.10.4.;

3.4.1.9. May also be used to indicate the malfunction of related systems/functions, including traction control, trailer stability assist, corner brake control, and other similar functions that use throttle and/or individual torque control to operate and share common components with ESC.

3.4.2. The ESC malfunction tell-tale need not be activated when a starter interlock is in operation.

3.4.3. The requirement of paragraph 3.4.1.7. does not apply to tell-tales shown in a common space. […] "

For ESC malfunctions UN R13-H defines a physical test to be carried out that allows the technical service to verify the self-test function. This simulates at least one malfunction by disconnecting the power source to a relevant component and verifies that the malfunction under defined subsequent driving manoeuvres is as expected:

UN Regulation No. 13-H, Annex 9 (ESC), Paragraph 5.10.:

"ESC MALFUNCTION DETECTION

5.10.1. Simulate one or more ESC malfunction(s) by disconnecting the power source to any ESC component, or disconnecting any electrical connection between ESC components (with the vehicle power off). When simulating an ESC malfunction, the electrical connections for the tell-tale lamp(s) and/or optional ESC system control(s) are not to be disconnected.

5.10.2. With the vehicle initially stationary and the ignition locking system in the "Lock" or "Off" position, switch the ignition locking system to the "Start" position and start the engine. Drive the vehicle forward to obtain a vehicle speed of 48 + 8 km/h. 30 seconds, at the latest, after the engine has been started and within the next two minutes at this speed, conduct at least one left and one right smooth turning manoeuvre without losing directional stability and one brake application. Verify that the ESC malfunction indicator illuminates in accordance with paragraph 3.4. by the end of these manoeuvres.

5.10.3. Stop the vehicle, switch the ignition locking system to the "Off" or "Lock" position. After a five-minute period, switch the vehicle's ignition locking system to the "Start" position and start the engine. Verify that the ESC malfunction indicator again illuminates to signal a malfunction and remains illuminated as long as the engine is running or until the fault is corrected.

5.10.4. Switch the ignition locking system to the "Off" or "Lock" position. Restore the ESC system to normal operation, switch the ignition system to the "Start" position and start the engine. Re-perform the manoeuvre described in paragraph 5.10.2. and verify that the tell-tale has extinguished within this time or immediately afterwards."

2.3 UN Regulation No. 48

UN R48 (lighting installation) requires an indicator (tell-tale) for lighting malfunctions under certain conditions and allows the signal to be switched off temporarily.

UN Regulation No. 48, Paragraph 6.2.8.1.:

"[The visual tell-tale] shall remain activated while the failure is present. It may be cancelled temporarily, but shall be repeated whenever the device, which starts and stops the engine, is switched on and off."

2.4 UN Regulation No. 79

UN R79 (steering equipment), Annex 6, and the identical UN R13-H (braking), Annex 8, describe documentation requirements with regard to the safety aspects of complex

electronic vehicle control systems for type-approval. These requirements were designed for steering and braking equipment, which are complex dynamic systems, vital for the safe operation of vehicles. After careful consideration, it is concluded that such an approach is likely to be too onerous to be applied in full for assessing the self-test function of AECD/AECS. However, the general principle of requiring suitable documentation and verifying it by a physical test is useful for the present task.

UN Regulation No. 79, Annex 6:

"3.4. SAFETY CONCEPT OF THE MANUFACTURER

[…]

3.4.4. The documentation shall be supported, by an analysis which shows, in overall terms, how the system will behave on the occurrence of any one of those specified faults which will have a bearing on vehicle control performance or safety.

This may be based on a Failure Mode and Effect Analysis (FMEA), a Fault Tree Analysis (FTA) or any similar process appropriate to system safety considerations.

The chosen analytical approach(es) shall be established and maintained by the Manufacturer and shall be made open for inspection by the technical service at the time of the type approval.

3.4.4.1. This documentation shall itemize the parameters being monitored and shall set out, for each fault condition of the type defined in paragraph 3.4.4. of this annex, the warning signal to be given to the driver and/or to service/technical inspection personnel.

4. VERIFICATION AND TEST

4.1. The functional operation of "The System", as laid out in the documents required in paragraph 3., shall be tested as follows:

[…]

4.1.2. Verification of the safety concept of paragraph 3.4.

The reaction of "The System" shall, at the discretion of the type approval authority, be checked under the influence of a failure in any individual unit by applying corresponding output signals to electrical units or mechanical elements in order to simulate the effects of internal faults within the unit.

4.1.2.1. The verification results shall correspond with the documented summary of the failure analysis, to a level of overall effect such that the safety concept and execution are confirmed as being adequate."

3 Draft proposal

1. Requirements

1.1. Information shall be provided regarding the status of the emergency call transaction when the AECD/AECS is automatically or manually activated. The following statuses shall be displayed:

1.1.1. ***call triggered and connection is being set up****; this status shall be displayed immediately after trigger is received and until data communication or voice connection to PSAP is established; it shall also be displayed if connection was interrupted for any reason and is being re-established.*

This status indication shall be demonstrated in course of normal call transaction.

1.1.2. ***data transmission in progress;*** *this status shall be displayed when data transmission to PSAP is being performed, but voice conversation with PSAP operator has not been yet established.*

This status indication shall be demonstrated in course of normal call transaction.

1.1.3. ***data transmission successfully completed;*** *this status shall be displayed when data transmission to PSAP has been successfully completed, but voice conversation with PSAP operator has not been yet established.*

This status indication shall be demonstrated in course of normal call transaction.

1.1.4. ***voice call in progress;*** *this status shall be displayed when voice conversation with PSAP operator is in progress regardless MSD transmission status.*

This status indication shall be demonstrated in course of normal call transaction

1.1.5. ***call not possible;*** *this status shall be displayed when attempts to transmit MSD and establish voice connection failed and no further attempts are currently being made.*

This status indication shall be demonstrated by triggering a call in absence of network coverage, which can be simulated e.g. by disconnecting or shielding the communication module antenna

1.1.6. ***system malfunction****; this status shall be displayed when emergency call transaction could not be performed due to AECD/AECS malfunction.*

This status indication shall be demonstrated when simulating AECD/AECS malfunction as explained in section [1.5]

1.2. A warning signal in form of a visual tell-tale shall be provided in case of AECD/AECS internal malfunction.

1.2.1. Where technically feasible with the chosen system design and architecture, the self-test function shall monitor at least the technical items listed in Table 1.

1.2.2. Visual indication of the AECD/AECS malfunction shall be displayed while the failure is present. It may be cancelled temporarily by the driver, but shall be repeated whenever the device which starts and stops the engine is switched on and off.

1.2.3. This shall be demonstrated according to [section 1.3 – 1.4] [Annex XXX]

2. Warning signal documentation requirements and test methods

2.1. The manufacturer shall provide the technical authorities with documentation in accordance with Table 1, which shall contain the following information.

(a) Which of the items listed are being monitored by the self-test function.

(b) For each item that is being monitored: The technical principle applied to monitor the item.

(c) For each item that is not being monitored: A technical reason, to the satisfaction of the type-approval authority, why it is not feasible to monitor the item with the chosen system design or architecture.

(d) For each item that is being monitored: feasibility of malfunction simulation during compliance testing; if simulation is not possible: the technical reason why malfunction simulation is not feasible

Table 1: Template of information for self-test function

Item	*Monitored by self-test function?*	*If yes: Technical principle applied for monitoring*	*If no: Technical reasons prohibitive of monitoring*	*Malfunction simulation feasible?* *If no: technical reasons prohibitive of simulation*
AECD/AECS is in working order (e.g. no internal hardware failure, processor/memory is ready, firmware is loaded successfully, logic function in expected default state)	*yes/no*			
External mobile network antenna is connected	*yes/no*			
Mobile network communication device is in working order (no internal hardware failure, responsive)	*yes/no*			
External GNSS antenna is connected	*yes/no*			
GNSS receiver is in working order (no internal hardware fai lure, output within expected range)	*yes/no*			

Crash control unit is in working order (e.g. no internal hardware failure, processor is ready, logic function in expected default state)	*yes/no*			
No communication failures (bus connection failures) of relevant components	*yes/no*			
SIM is present	*yes/no*			
Dedicated battery is connected	*yes/no*			
State of health of dedicated battery	*yes/no*			
Microphone(s) are connected	*yes/no*			
Loudspeaker(s) are connected	*yes/no*			
Manual call button is connected	*yes/no*			
Status indicator is connected	*yes/no*			

2.2. Self-test function and warning signal verification test

The following test shall be performed on a vehicle with an AECD/AECS installed or on a representative arrangement of components for the approval of vehicles, components or separate technical units.

2.2.1. Simulate a malfunction of the AECD/AECS by introducing a critical failure in one or more of the items monitored by the self-test function according to the technical documentation provided by the manufacturer. The item(s) shall be selected at the discretion of the technical service among the items which are feasible of simulation.

2.2.2. Power the AECD/AECS up (e.g. by switching the ignition 'on' or activating the vehicle's master control switch, as applicable) and verify that the malfunction indicator illuminates and remains on.

2.2.3. Power the AECD/AECS down (e.g. by switching the ignition 'off' or deactivating the vehicle's master control switch, as applicable) and restore it to normal operation.

2.2.4. Power the AECD/AECS up and verify that the malfunction indicator does not illuminate or extinguishes shortly after illuminating initially.

4 Justification

4.1 Purpose of the procedure

The purpose of the proposed procedure is to verify the stipulation in the draft UN Regulation regarding warning of the occupants in case of system failures.

Draft AECS UN Regulation (AECS-02-02-r4), Paragraph 6.5.2.:

> *"A warning signal shall be provided in case of AECD internal malfunction. Visual indication of the AECD malfunction shall be displayed while the failure is present. It may be cancelled temporarily, but shall be repeated whenever the device which starts and stops the engine is switched on and off."*

Draft AECS UN Regulation (AECS-02-02-r4), Paragraph 15.3.3.:

> *"A warning signal shall be provided when the onboard AECS is not functioning properly. Visual indication of the AECD malfunction shall be displayed at all times while ignition is turned on or the vehicle master control switch is activated (whatever applicable)."*

4.2 Technical items to be covered by the self-test function

It will be shown in the following sub-sections that it is not technically feasible for a system self-test to detect all possible failures that would result in an inability to execute an emergency call. Hence, the potentially far-reaching stipulations in the draft UN Regulation, such as that a malfunction indication should be given "*when the onboard AECS is not functioning properly*" need to be further specified and simplified to be suitable for verification during type-approval.

A sensible definition of the technical items to be covered by the self-test ensures that the range of expectations is uniform between different technical services and type-approval authorities and therefore ensures a level playing field for manufacturers and a comparable level of self-test capabilities across the range of vehicles and systems. The remaining potential failure cases, which cannot be detected by a system self-test, should be covered during PTI.

4.2.1 Self-test capabilities of current TPS system designs

The self-test capabilities of the TPS system designs of three European premium segment vehicle manufacturers (A, B and C) are listed below. This can give an indication of what is currently done on a voluntary basis. The driver is not informed of all the failures below via a malfunction indicator (some failures are just stored as fault codes). Components that will not be required for a mandatory AECD/AECS IVS, such as a Bluetooth antenna, were omitted for these lists.

The self-test of vehicle Manufacturer A covers:

- Microphone: Connection failure
- Speakers: Failure (based on electrical signal)
- Manual call button: Failure
- State indicator LED: Failure

- Internal backup battery: Connection failure (non-rechargeable)
- Crash sensor: Failure
- Communication Module Interface: Failure
- GNSS receiver: Failure
- GNSS antenna: Failure

From communication with Manufacturer A it was inferred that:

- Only external antennas are monitored and not internal backup antennas (because the likelihood of faulty diagnostics would be similar to the likelihood of antenna failure).

The self-test of vehicle Manufacturer B covers at least the following items:

- Microphones: Short circuit; ground or plus pole
- Microphones: Connection failure
- Speakers: Short circuit; ground or plus pole
- Speakers: Connection failure
- GPS antenna: Short circuit; ground
- GPS antenna: Connection failure
- Manual call button: Connection failure
- Buttons: Buttons stuck
- Control unit: Fan malfunction
- Control unit: Internal hardware malfunction (detected by ‘watchdog’ function)
- Control unit: Software error
- Control unit: Bus communication failure
- Control unit: Communication failure on direct connections
- Control unit: Voltage level; high or low
- Power supply: Voltage level; high or low
- Wake-up cable: Short circuit; ground or plus pole
- Radio antennas: Short circuit; ground or plus pole
- Radio antennas: Connection failure

The self-test of vehicle Manufacturer C covers at least the following items:

- Speakers: Short circuit; ground or plus pole
- Speakers: Connection failure
- Microphone: Connection failure
- Control unit: Power supply failure
- Control unit: Communication failure
- State indicator LED: Failure
- Mobile network antenna: Connection failure

- Backup mobile network antenna: Connection failure

A comparison of the items on the above lists reveals that there is a certain variety in the likely extent of what failures manufacturers might cover with the self-test function. In a separate communication received, ACEA indicated that the extent varies depending, for example, on the abilities of the vehicle's CAN bus (advanced, limited CAN bus or no CAN bus link of the application) and that the control unit (ECU) was the only part commonly monitored across different manufacturers.

4.2.2 Possible failure modes and mechanisms

A self-test function of IVS can cover a variety of electrical failures; however, not all possible failures of IVS components can be detected with reasonable effort. Also, the technical capabilities vary between manufacturers and vehicles depending on aspects of AECD/AECS and CAN bus design. This needs to be reflected in the proposal in order to not unduly restrict the system design.

Table 4 provides a high-level list of potential failure modes and mechanisms of IVS components. The colour-coding indicates for each failure whether it is technically feasible to cover it in a system self-test or not. The consideration of technical feasibility is based on the responses comprising Section 4.2.1, general technical considerations and additional stakeholder input. The green elements of the list formed the basis for the required items to be monitored as a default. It is considered to be likely that the red elements cannot be monitored by a self-test function in a typical system design.

Table 1: Potential failure modes and mechanisms of IVS parts; colour-coding indicates feasibility to check via IVS self-test (green: generally feasible; yellow: feasible in some instances; red: generally not feasible)

Part	Failure mode / mechanism	Comment
Control unit, network access device, GNSS receiver	Power supply failure (connection failure, short circuit, voltage high/low)	
	Communication failure (bus connection failure)	
	Internal hardware failure	e.g. via monitoring signal from NAD and GNSS receiver
	Software error	e.g. software image integrity via checksum
	SIM failure/not present	
	SIM invalid	Not feasible to test without network communication (dormant mode SIM)
Dedicated battery	Connection failure, short circuit	e.g. via voltage monitoring
	Output voltage high/low	Generally feasible; challenging in high/low temperature conditions

	Reduced state of capacity	Generally feasible for rechargeable batteries; challenging for primary batteries to be performed at every vehicle start (gradually discharging battery)
	Reduced state of charge	When applicable to rechargeable batteries only
Mobile network antenna (GSM / UMTS)	Connection failure, short circuit	
	Reduced performance/failure due to unintended manipulation (e.g. non-approved replacement part, installation faults) or mechanical degradation (e.g. corrosion of contacts)	Not feasible to test because similar to weak signal situation and dormant mode SIM
	Failure due to deliberate manipulation (shielding of antenna or jamming of signals), e.g. based on concerns the vehicle could be tracked	Not feasible to test because identical to no-signal situation and dormant mode SIM
GNSS antenna	Connection failure, short circuit	
	Reduced performance/failure due to unintended manipulation (e.g. non-approved replacement part, installation faults) or mechanical degradation (e.g. corrosion of contacts)	Not feasible to test because similar to weak signal situation
	Failure due to deliberate manipulation (shielding of antenna or jamming of signals), e.g. based on concerns the vehicle could be tracked	Not feasible to test because identical to no-signal situation
Microphone(s)	Connection failure, short circuit	
	Reduced performance/failure due to degradation (e.g. soiling, ageing, mechanical defects)	Would require playback and recording of audio signal at vehicle start (unreliable in noisy conditions, nuisance for occupants)
	Reduced performance/failure due to manipulation (e.g. non-approved replacement part, installation faults, covered by retrofit elements)	Would require playback and recording of audio signal at vehicle start (unreliable in noisy conditions, nuisance for occupants)
Loudspeaker(s)	Connection failure, short circuit	

	Reduced performance/failure due to degradation (e.g. soiling, ageing, mechanical defects)	Would require playback and recording of audio signal at vehicle start, (unreliable in noisy conditions, nuisance for occupants)
	Reduced performance/failure due to manipulation (e.g. non-approved replacement part, installation faults, covered by retrofit elements)	Would require playback and recording of audio signal at vehicle start, (unreliable in noisy conditions, nuisance for occupants)
Crash control unit	Power supply failure (connection failure, short circuit, voltage high/low)	Potentially separate self-test that is fed back to the ECU
	Communication failure (bus connection failure)	
	Internal hardware failure	Potentially separate self-test that is fed back to the ECU
Manual call button	Connection failure, short circuit	Depends on button design (open circuit design would not allow resistance check)
	Mechanical failure (e.g. button stuck)	
Status indicator	Connection failure, short circuit	Detection feasible, but only possible to indicate if status indicator is separate from malfunction indicator
	LED failure	Detection feasible, but only possible to indicate if status indicator is separate from malfunction indicator
	Failure due to deliberate manipulation	Detection feasible, but only possible to indicate if status indicator is separate from malfunction indicator
Malfunction indicator	Connection failure, short circuit	Detection feasible, but indication to driver not possible
	Failure due to deliberate manipulation	
	LED failure	Detection feasible, but indication to driver not possible

4.3 Documentation and verification procedure

As outlined above, there are a large number of potential failures that can lead to an inability of the IVS to execute an emergency call and which can be detected by the self-test function. Testing each of these failures would impose a disproportionally high testing effort on the manufacturers and might, altogether, not even be technically feasible in many cases; relying exclusively on documentation (without verifying the system conformance in a physical test) may result in a large variation in how this rule is applied by different type-approval authorities. The general principle applied in these UN regulations, such as UN R13-H and UN R79, is to cover the variety of cases by documentation and verify selected cases in physical tests:

- Require documentation that explains the design provisions taken; and
- Verify the system behaviour by applying one or more failures (at the discretion of the type-approval authority) and assessing the outcome against the documentation.

This general approach is considered suitable also to be applied to the issue at hand.

The provision of documentation in accordance with Table 1 shall prompt system suppliers and vehicle manufacturers to implement a wide range of self-test functions. Emphasis has been given to pragmatic self-testing, which should be possible without having to significantly change the system design or architecture, which is governed by the vehicle's communication and information sharing protocols. This has been referred to as "*technically feasible*" testing within the draft proposal. If it is not feasible to monitor a certain item with reasonable effort, the manufacturer can provide a technical reason to opt out of monitoring this item (e.g. open-circuit design of manual call button does not allow electrical resistance check; or, no communication monitoring because application not linked to CAN bus).

Note that feedback received from ACEA indicated that the definition of a list of specific items to be monitored was considered problematic in particular for the transition phase, because this could require wiring harness modifications of new vehicles design specifications that were already fixed for the next model generation. Particular concerns were raised regarding mandatory monitoring of loudspeaker connection status, because these components were typically part of the vehicle's infotainment system. Therefore, monitoring might require changes to the vehicle system architecture in some cases. The intention is for this to be addressed by the definition "*where technically feasible with the chosen system design and architecture*". It was nevertheless suggested to omit these items from the list based on the fact that MSD transmission would still be possible without loudspeakers, which would be sufficient to dispatch emergency services.

The documentation allows the technical service to verify that all required items are being monitored by suitable means unless there are technical reasons inherent to the current system design or architecture that prohibit monitoring of the specific item. It also enables the technical service to select a test case for the physical verification test.

The physical verification test is limited to only one exemplary test case (unless the technical service has reason to believe more test cases are necessary, for example if the specifications in Table 1 are not fully adequate). This limited approach to physical verification is considered appropriate because the complexity of the static AECD/AECS IVS is limited compared to complex electronic vehicle control systems for dynamic functions such as braking or steering.

The simulated malfunction shall be at the discretion of the technical service to introduce a random element in the verification test. Ways of introducing a critical failure could, for example, be: Disconnecting the power supply or bus connection of a monitored active component, disconnecting direct connection of a monitored component (e.g. loudspeaker, microphone or antenna), manipulation of the power supply or removing the SIM.

4.4 Malfunction indicator provisions

The requirements of the draft proposal regarding the appearance of the malfunction indicator ensure that a visual malfunction tell-tale is available and that it is activated whenever a failure is present, unless it is temporarily cancelled by the driver. Note that a temporary lack of mobile network coverage is not considered a failure that should be indicated to the driver using the malfunction indicator.

These requirements are based on UN R48, with the added limitation that the cancellation of the tell-tale has to be performed by the driver; this was added to avoid automatic cancellation after a defined period of time, which could lead to false assumptions that the system has returned to working order. This shall not prohibit system designs that initially display a comprehensive message about a failure and then reduce the tell-tale to a simple failure indicator symbol.

It is expected that aspects such as colour, location and the symbol for the visual tell-tale will be specified elsewhere, if considered necessary.

4.5 Sequence of status displays

Status indication of emergency call transaction ensures vehicle occupant awareness of the AECD/AECS operation. Potentially injured person may decide to take action or wait for help depending on information communicated via indicator. Such decision can be vital for efficiency of emergency response (e.g. the person can decide to stay in the vehicle to talk to PSAP operator, or leave the vehicle to search for help / make a phone call). The following scenarios shall be taken into account:

- Normal AECD/AECS operation
- Absence of network coverage
- Damage of some of AECD/AECS components as a result of the crash

The following information is important for potential decision making by the vehicle occupants:

- Is AECD/AECS in operating condition?
- Was event information communicated to PSAP?
- If event information was not communicated, are attempts still in progress, or already discontinued?
- Shall I expect voice connection to PSAP?
- I do not hear any voice. Is there a chance PSAP operator is currently hearing me?

Based on the above rationale and the sequence of AECD/AECS emergency call transaction, the following status indications shall be provided:

- **call triggered and connection is being set up**; this status means AECD/AECS is attempting to establish communication, but attempt has not succeeded yet; vehicle occupants can be advised to wait.
- **data transmission in progress;** this status means AECD/AECS succeded to establish network connection and is currently transmitting event information; vehicle occupants can be advised system is operating properly and voice connection can be expected soon.
- **data transmission successfully completed;** this status means event information has been successfully transmitted to PSAP, but voice conversation with PSAP operator has not been yet established; vehicle occupants can be advised that PSAP is aware of the accident, and voice connection can be expected soon.
- **voice call in progress;** this status means voice conversation with PSAP operator is in progress; vehicle occupants can be advised that PSAP is aware of the accident even if they cannot hear PSAP operator voice (e.g. because in-vehicle speaker has been damaged). In addition, vehicle occupants should be aware that PSAP operator can currently hear their conversation.
- **call not possible;** this status means event information was not communicated to PSAP and no further attempts are currently being made; vehicle occupants can be advised to find other ways to call for help, even though AECD/AECS might retry to establish communication.
- ***system malfunction****; this status means AECD/AECS is not operating properly;* vehicle occupants can be advised to find other ways to call for help.

5 Glossary of terms

Term	Definition
AEBS	Automatic emergency braking systems
AECD	Automatic emergency call device
AECS	Automatic emergency call system
ECU	Electronic control unit
FMEA	Failure mode and effect analysis
FTA	Fault tree analysis
GNSS	Global navigation satellite system
GSA	European Global Navigation Satellite Systems Agency
GSM	Global System for Mobile Communications
HMI	Human-machine interface
IVS	In-vehicle system
MSD	Minimum set of data
PSAP	Public safety answering point
PTI	Periodic technical inspection (roadworthiness testing)
SIM	Subscriber identity module
TPS	Third party service
TPSP	Third party service provider
TS11, TS 12	Teleservice 11, Teleservice 12
UMTS	Universal Mobile Telecommunications System