AECS REGULATION

POST-CRASH CHECK WITH HMI TEST METHOD

SUMMARY

- ASIL determination – ISO26262
- Pre-requirements for HMI test method
- HMI check procedure proposal
- Glossary

01

ASIL determination – ISO26262

ASIL = Automotive Safety Integrity Level

Determination of the level of ASIL for AECS

The ISO26262 standard provides a risk-based approach to determine ASIL (Automotive Safety Integrity Level) for safety function in E/E systems for road vehicles. It also provides analytical method to identify impacting defaults on safety functions.

Classification of hazardous events

Class of severity : **S2** (severe and life-threatening injuries - survival probable)

Class of probability of exposure : **E1** (very low probability)

Class of controllability : **C3** (Difficult to control / uncontrolable)

ASIL Classification

➔ According the $Table4_{ISO26262}$ ➔ ASIL = **Quality Management (QM)**

➔ **The class QM means no high level requirement for safe design** (see annex) to comply with ISO26262, and therefore, AECS is not considered as a Safety System

Consequences for AECS

AECS should not be considered as a safety system, and therefore, it doesn’t need to have a complete and complex approval method.

Nevertheless, for using the HMI test method, this methodology (ISO26262) shall be a pre-requirement.

02

Pre-requirements for HMI test method

1- FAILURE DETECTION

2- STATUS and FAILURE INDICATION

Method Pre-requirements : FAILURE DETECTION

This test method can be used only if the AECD/AECS is capable to check and diagnose :

1- the electrical connections between all of the following devices :

- AECD control unit
- PLMN communication module (NAD, SIM, …) + antenna
- GNSS receiver + antenna
- Power source (for a dedicated source)
- 

Warning signal and Information signal devices (HMI)
- 

Microphone
- 

Loud speaker
- [-Trigger signal generator (e.g. Airbag Control Unit)]

2- the status of the :

- PLMN and GNSS modules (internal failure)
- 

PLMN coverage
- Energy available in the power source (autonomy)

Pre-requirements : STATUS and FAILURE INDICATION

This test method can be used only if the AECD/AECS is capable to indicate by a visual or audible mean :

1- a failure *(see the list of failure in the previous slide)*

2- the status information for the following :

- AECS operational
- PLMN availability
- Automatic trigger detection + Establishment of a connection with the PSAP (*)
- Connected to the PSAP + MSD sending (*)
- Voice communication with PSAP (*)
- End of normal call
- Impossible to contact PSAP

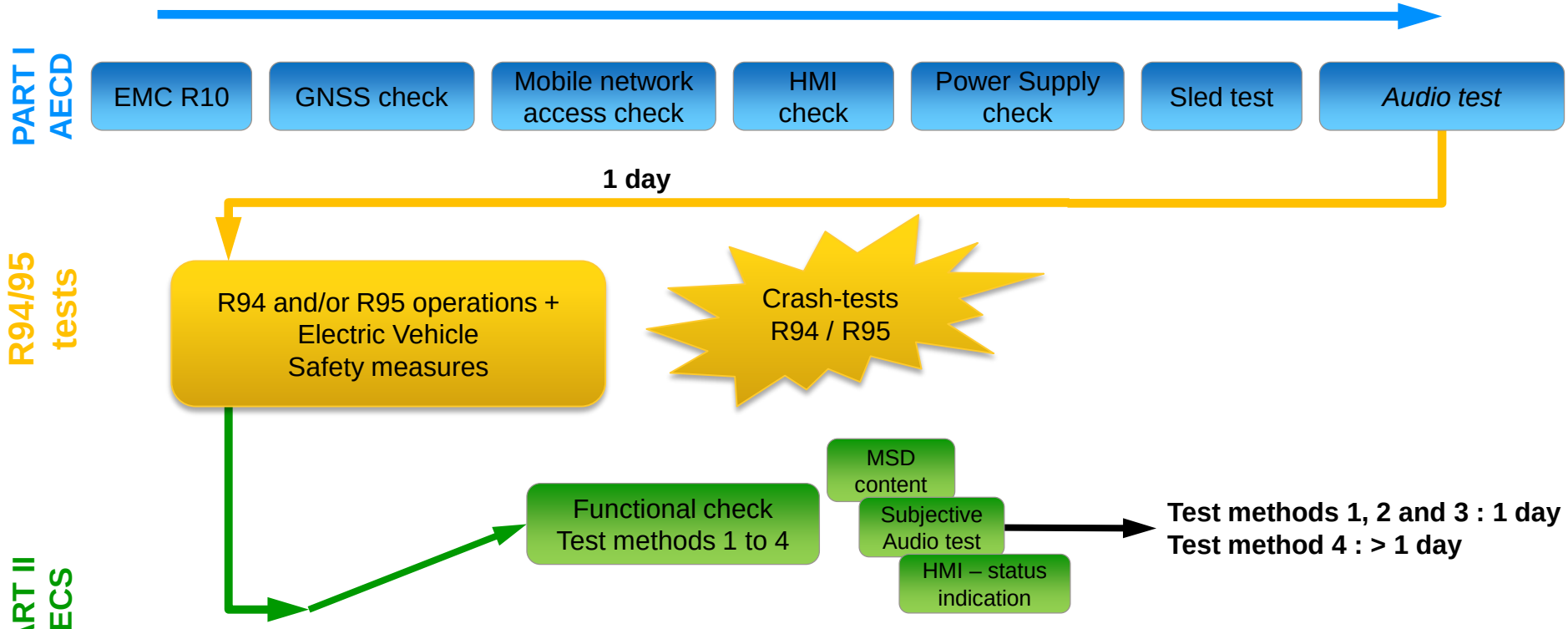
The status above identified by a (*) are merged in the AECS information signal (« system is processed »)

This test method can be used only if the AECD/AECS is capable to treat/manage an emergency call during the approval crash tests even if there is no mobile phone network coverage.

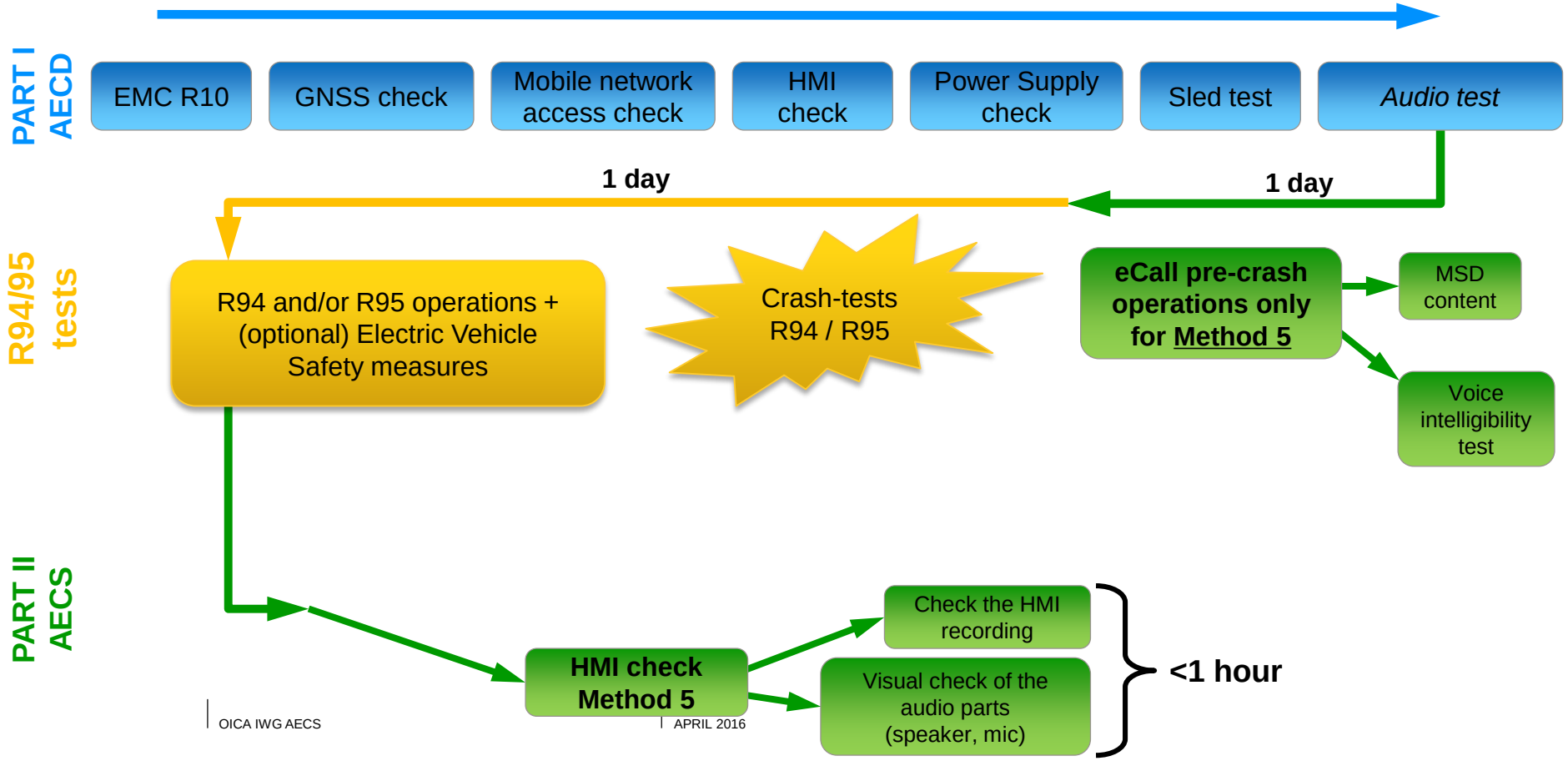
03

HMI check procedure proposal

AECD/AECS test phases for test methods 1 to 4 (current situation)



AECD/AECS test phases for test method 5 : HMI test method (new)



Pre-crash procedure

These operations are to be done <u>before</u> the R94 (frontal) and/or the R95 (Lateral) crash tests :

1- Proceed to a functional check by test methods 1 to 4 following a manual call :

- Conformity of the content of the MSD (location, time stamp, vehicle identification)

- Hands-free voice communication assessment

➔As in the European eCall regulation, the subjective voice intelligibility test method should be allowed, as the objective test method, at the demand of the applicant.

2- Install, in the vehicle, a mean of record the behavior of the warning and information signals during the crashes (R94 and R95). It could be, for example, a video/audio camera, or a recorder for electrical signals.

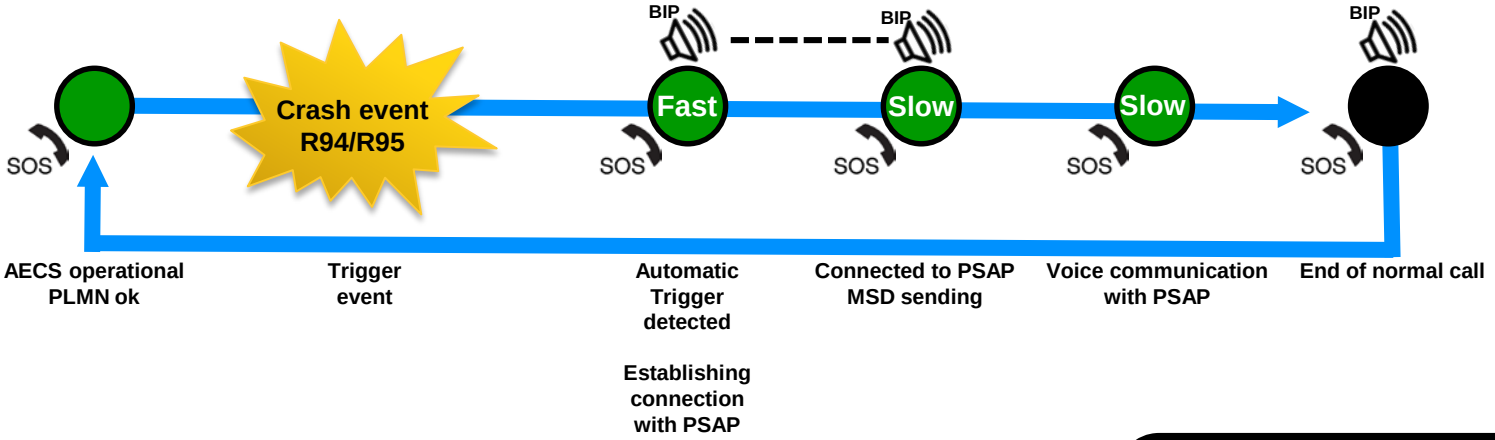
Post-crash procedure

After the R94 or R95 crash, the Technical Service will check the recording of the warning and information signals to verify if the HMI sequence defined by the manufacturer is compliant.

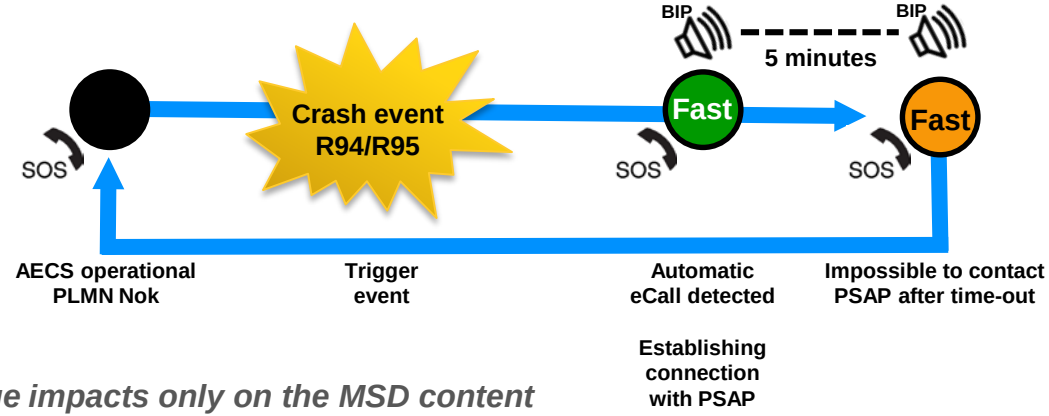
Post-crash procedure

Examples of <u>compliant</u> <u>sequences</u>** of warning and information signal during a crash test in function of the PLMN availability **(not to be considered as a reference for HMI which could include texts or speaches, other colors..)

With PLMN coverage



Without PLMN coverage



If a failure is detected, the warning indication will be <u>permanently</u> switched ON

The GNSS coverage impacts only on the MSD content

Past/Fail criteria

1- After the R94 or R95 crash, the Technical Service will check the recording of the warning and information signals to verify if the HMI sequence defined by the manufacturer is compliant.

2- A visual check will be done to verify the eventual damage on the audio devices (loud-speaker and the microphone) and PLMN antenna, if visible.

➔ ***In the case of the audio devices or PLMN antenna are not visible, or if the audio devices or PLMN antenna show important damages, at the demand of the Technical Service, an additional subjective audio test should be done by test methods 1 to 4.***

Thank you

04

Glossary

AECD : Accident Emergency Call Device

AECS : Accident Emergency Call System

ASIL : Automotive Safety Integrity Level

HMI : Human Machine Interface/Interaction

PLMN : Public Lan Mobile Network

GNSS : Global Navigation Satellite System

NAD : Network Access Device

SIM : Subscriber Identity Module

MSD : Minimum Set of Data

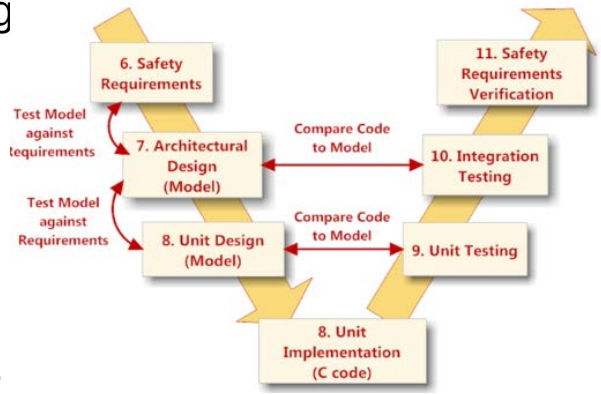
PSAP : Public Safety Answering Point

05

Annex on high level requirement for safety functions, ISO 26262

ISO 26262, a method for safe design

This design method rates ASIL of safety functions (e.g. driving braking functions..) and leads to design concepts including safe fallback mode and redundancies for safety and availability, according **to default impacts on given architecture**



1- a functionnal analysis based on customer final risks (OEM's agreement through international standard)

2- a detailled analysis indentifies impacts from **all** system defaults

From functional architecture..

Customer feared event:
e.g. no braking !

System feared event:
e.g. command failure !

all defaults

.. to associated default tree