VMAD-03-11

Describe in a few sentences what should be the outcome of the ‘audit/virtual testing/in-use data reporting

Audit/assessment

- Audit: Confirmation that the manufacturers have appropriate processes in place to develop AV’s for the road through the management processes, development phase and lifecycle of the vehicle. This shall include the process of updating vehicles on the road.
    - An audit also proves, that the developers involved in the project are familiar with the corresponding processes and are using them.
- Assessment of vehicle safety: Assessment of manufacturer performance data demonstrating that the vehicle design, verification and validation done by the manufacturer has mitigated risk and meet the minimum performance requirements.
- Well adapted to assess performances that are not easy to test on track or on road.

What are the questions to be answered?

- What are the minimum documentation requirements to achieve this?
    - The processes that are considered essential for homologation need to be documented in a detail that allows to identify how the relevant work products are created – using a generally accepted documentation method (or comparable) e. g. use Stages Unified Process, Rational Unified Process, BPMN, SIPOC, RACI, or similar stuff…
    - Define ‘relevant work products’ → all documents, analysis and reports needed for homologation + documents, analysis and reports needed to support / prove relevant vehicle properties (e. g. safety, security, …)
    - Aspects like safety that are independently audited by a trustworthy third party according to the requirements in ISO 26262 can be re-used and do not need to be repeated

Audit/assessment

- How early in the development phase should this audit/assessment process start?

  Audit

  - If the processes are established with first project an audit should accompany at the very beginning to recognize deviations from homologation or additional requirements. If the processes are established and an initial audit was performed, an re-audit can be performed on annual frequency.

  Assessment:

  - Aerospace uses for SW a staged process (stages of involvement SOI#1 to #4 – planning, SW definition, V&V, SW accomplishment)
  - In analogy to this staged procedure the auditing should be split to cover the relevant phases. (It is not considered useful to perform an audit way after a phase has been closed.)

    stage#1: Development – requirement elicitation, HARA and safety analyses
    stage#2: (Verification &) validation and argument towards residual risks
    stage#3: Commissioning and risk mitigation strategy for issues from the field

- How prescriptive (how deep) do the requirements need to be and what level should aim for? Data provided by manufacturer to be confirmed by independent test?

  - The requirements wrt. audits should be set up such that it supports the argument why the product achieves the regulation requirements. I. e. the audit should check whether the procedures established by the applicant are suited to produce both a conforming product and the evidence for this. I. e. the audit shall check whether the process as such is able to achieve these two objectives, and it shall check whether the processes have been implemented correctly.

    → the check if the objectives, the applicant shall achieve should be phrased as requirements for the auditing

Audit/assessment

- Who should conduct the audit/assessment?
  - The auditor should be independent from the management, development and testing teams. (At least I3 as per ISO 26262-2 Table 1.)
  - The auditor should be familiar with audits, processes and have some understanding of the relevant technical topics (safety, security, etc.) Audits might also be split per topic and auditor to cover the expertise needed.
  - The Auditor shall be authorised from a designated Technical Service.

- What are pass/fail criteria/ an acceptable level of risk (link with WP29/GRVA/FRAV-VMAD/1a) & what is the appropriate method to demonstrate a certain level of risk?

  Level of risk:
  - The system must be at least as safe as the human driver. For the acceptance of the systems by society, a much higher level of safety than that of the human driver will be required.
  - PEGASUS: positive risk balance is mandatory… (also in terms of product liability)
  - But actually this is not a question for the audit. The audit can check whether the risk threshold for acceptance has been defined in a suited manor, and whether the residual risk estimate have been determined correctly.
  - An absolute risk threshold required by regulations is not specific to audits.

- Difference between harmonized track tests (link with VMAD/2b) and verification tests (depending on safety concept)?

Audit/assessment

Information on existing practices:

- Use R79 Annex 6 as a basis (Annex CEL). However, more is required.
- FMEA’s, Fault Tree Analysis will be included – how to manage the negative outcomes.
  - Audits will check, if sufficient analysis are generally in place and executed. A concrete inspection of the analysis is in scope of an assessment not of an audit. (Analysis like FTA and FMEA are not audit specific) However negative outcomes from the analysis can be handled with measures (FMEA: Optimization according to VDA recommendation … etc. … FTA analogously …)
- ISO26262 (mainly regarding failures) and SOTIF (some focus on driver assistance systems) taking the basic principles and applying them to an audit approach.
  - Security and Privacy might also be an aspect for auditing …
- UL 4600 draft standard

Virtual Testing

-Allow the manufacturer to validate safe driving without having to drive the vehicle millions of km in various traffic scenarios.

-This data can also be used to demonstrate validation/safety performance to authorities.

-Virtual testing is well adapted to critical/dangerous/complex scenarios, validate variants

What are the questions to be answered?

- Need to clarify the different concepts of simulation/models/virtual testing? What is used today?
- Do we need one standardised tool or can multiple solutions be permitted?
  - No, a standardized tool is not necessary as long as all tools used are validated according the same method / standards.
  - For the exchange of simulation models, the interfaces between the models urgently need to be standardized. The exchange of results is less time-consuming than the exchange of simulation models, but a standardization of the data format and the measurement channels is also desirable here.
- How do we describe the ODD in a standardized manner?
  - An ODD is often described very simply (e.g. motorway), although it is very extensive and complicated --> see Koopman, Philip; Fratrik, Frank (2019): How Many Operational Design Domains, Objects, and Events? In: SafeAI. AAAI Workshop on Artificial Intelligence Safety.

Virtual Testing

How do ensure that the results of virtual Testing make sense? (e.g. correlation to the expected results, scope, traceability, etc.)?

Interchange of Simulation models / results:

- For the exchange of simulation models, the interfaces between the models urgently need to be standardized. The exchange of results is less time-consuming than the exchange of simulation models, but a standardization of the data format and the measurement channels is also desirable here.

Methodology used for simulation (e.g. from OEM)

- The methodology of the OEM must be ensured during an audit by a third party. The type and scope can be based on existing and currently developed standards such as "ISO/AWI 11010-1:Passenger cars -- Simulation model taxonomy -- Part 1: Vehicle dynamics manoeuvre".
- According to 2007/46/EC or more up-to-date (EU) 2018/858 Article 30 a manufacturer need to apply for an agreement from the authority. The fundament of such an application is a report from a Technical Service.

- Who validates virtual testing? Manufacturers? Authorities? determine some parameters to be checked?
  - Validation can also be based on standards. A multi-level concept should also be introduced. Individual components are validated separately and then the overall system is validated again. An assembly of validated individual systems does not necessarily result in a valid overall system. Comparison with real world data from proving grounds and road tests is mandatory which is in accordance with (EU) 2018/858 Annex VIII.
  - Sensor model also has to be validated as one specific component of the simulation
- **Information on existing practices:**
- R140 is a good example for validation of simulation tools.

In use reporting

- To track and report “unkown” scenarios/minimize risks
- To improve traffic models/scenarios
- Verify compliance on the ground

What questions need to be answered?

- How to ensure that manufacturer minimize risks over the lifetime of the vehicles?
    - Sensor data and sensor fusion data continues to evolve through the OEM development process, machine learning and later SW-Updates over the air (SOTA). New technological insights are already being brought to the market through new OTA updates or ECUs.
    - The question what is the lifetime of the vehicle is necessary.
        - Vehicle components and vehicles are subject to a replacement period of 15 years (mass market). Very exclusive brands up to 40 years (RR, Bentley).
        - The product cycle for complete cars is between 4 and 8 years, depending on the vehicle manufacturer.
- How to ensure that the newly foreseen scenarios are added to the vehicle capability over the lifetime of the vehicle.
    - Through the initial homologation as well as a continuous technical inspection (CTI) of the technical services and authorities. Periodical assessments by TS or authority like for AES/BES (emissions). This would include new models as well as already sold vehicles.
    - Additional to a "car data assessment" within the OEM-workflow and infrastructure.
- How do ensure operational feedback from the field on traffic scenarios?
- In use monitoring during development phase or also once the vehicle is on the market?

In use reporting

- What kind of data shall be collected by manufacturers?
  - Definition of "collected": data already stored in the car; a very small amount will be transferred to the OEM backbone.
  - Cannot be answered in general. This requires an extensive specification: Which functionalities have to be monitored? Which ECUs are involved? Which driving modes and scenarios should be evaluated? What is the cost-benefit aspect, as the OEM has already implemented a continuous review?
- What kind of data shall be reported to authorities? How often?
  - Emergency or C2C data immediately (e.g. eCall); maintenance data "time-" or "event triggered", ”high priority data” on every vehicle startup.
  - The question is linked to previous question
- Who has access to the data?
  - The vehicle owner as well as official institutions and technical services. All others (including OEM) only after authorization by the vehicle owner (DSGVO).
  - What about anonymized data? In case of anonymized data, the traceability to a person via several systems must be prevented and proven.
- What shall authorities do with this data? How do we ensure suitable oversight of the reporting?
  - Through the initial homologation as well as a continuous technical inspection (CTI) of the technical services and authorities. Periodical assessments by TS or authority like for AES/BES (emissions). This would include new models as well as already sold vehicles.
  - Usage of CTI and the certification of OTA-processes within the OEM. The manufacturer shall report and describe their decision-making like for AES/BES.
- How this data should be collected? Use EDR/DSSAD for in use reporting?
  - It is to be supported to use as much synergies as possible.
- How do we ensure compliance after an OTA?

CITA

c) **Indicate which persons/organisations need to be involved in this group?**

- CP’s, TAA’s, Tech services, OEM’s, Suppliers, Software companies should be involved
- Companies that are deep into validating simulation tool chains
- Keep as one group Audit/virtual testing/in-service