Questions VMAD Working Group 2a

Audit/assessment

1. **What are the minimum documentation requirements to achieve this?**

Beyond the topic that the manufacturers do not like to provide too much details about their controller concept, there is of course the challenge, that for a judgment some details are requirement. The design of the function defines beyond others which scenarios could occur and what could not occur. Simple example: if for a function only radar is used (not camera), reflections of sun light etc. will have no influence. On the other hand maybe, the manufacturer would not like to share that he solved the issue without any camera…

It is hard to say what is the minimum of documentation of the system.

On the other had the documentation must deal with ISO26262, SOTIF, etc.

The risk assessment is an established method and seems to be also very promising, especially in combination in combination with UL4600. The risk assessment must be done very detailed and is also a learning process. Analogue to a standard risk assessment it must be worked out what is relevant and how different things are avoided. This is the one of the most important things

2. **How early in the development phase should this audit/assessment process start?**

Much more earlier than today… It would be efficient if the authority attends the development process from the very beginning. Realizing major bugs or issue late in the process is dramatic for the manufacturer. Early involvement of auditors in risk assessments processes is best practice.

3. **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?**

Deep is maybe the wrong word. If you get detailed data which are not structured well, you cannot use them. The key is that you get structure data according a standard process. E.g. overview cockpits, based on standard templates (e.g. risk analysis), etc. Further aspects see first point.

4. **Who should conduct the audit/assessment?**

Somebody who is certified to do that. Maybe an expert tea, for the different areas (especially when it comes to simulation).

5. **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?**

Not easy to answer. It will not be one catalogue or one method. There are different approaches and it should be a combination. (according what we are discussing in our workshops in Brussels – “Technical Workshops on new approaches for automated vehicles certification”)

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

I am not yet in the details of VMAD/2b. As far as I understand now, the harmonized track tests are VALIDATION tests and the tests e.g. depending on the safety concept are VERIFICATION tests.

The difference can be defined according VDI:

Verification describes the formal comparison of system properties with system requirements, i.e. verification represents the process that evaluates whether a system has been properly developed.

Validation, on the other hand, describes the process, which checks whether the correct system has been developed, i.e. whether it meets customer expectations.

Questions VMAD Working Group 2a

Virtual Testing

1. **Need to clarify the different concepts of simulation/models/virtual testing? What is used today?**

We need a glossary. Today in several documents a lot of things are mixed up. The most important terms are:

- Simulation Tool (purpose, focus, etc.)
- Models (purpose, fidelity, Model classifications according ISO 11010 Part 1, etc.)
- Co-Simulation Platform (synchronization, interpolation because of different sampling times of different tools, etc.)

2. **Do we need one standardised tool or can multiple solutions be permitted?**

Best would be, of course, to have a standardized tool because then the certification of the tool could be done easier. There are several problems why this will not work resp. is not a suitable way:

- It will not be one tool. The AD simulation world has so many factettes which can only hardly cover by one tool supplier (e.g. vehicle dynamics which requires a physical understanding, environment simulation which requires computer graphics expertise, traffic simulation which require corresponding skills, sensor models which require deep sensor know how, etc.)
- Beyond the tool, the models and the model parameterization (including model validation) are crucial. The best tool is not enough if the models of the tool are not parameterized in the right way and validated against the real vehicle
- OEMs, suppliers, etc. already have tools and models for different purposes in place. Forcing the to use a standardized tool will extend their effort tremendously and will not be accepted. A transfer from one tool or model to another is in most cases not trivial because the behavior the level of details is completely different
- If different tools are used (see point one), beyond the tools and models the toolchain resp. the integration and co-simulation of all parts must be guaranteed and approved. Maybe for the integration and connection standard coupling elements could be defined?

Questions VMAD Working Group 2a

3. How do we describe the ODD in a standardized manner?

Question is not 100% clear for me even if we talked about.

Some thoughts about that:
The simulation must be validated for the ODD. I think we need an extended ODD description for simulation validation. Simple example:
The ODD is highway and the function is a highway pilot. For the validation of the simulation we need some wore properties of this ODD. E.g. steering angle between XX and YY degrees; speed between XX and YY km/h, long. acceleration between XX and YY m/s², lat. acceleration between XX and YY m/s², etc.
Based on that validation tests can be derived.

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

A process must be defined how validation of the toolchain, the tools and the models resp. the combination of all of them will be performed.

Base for the correlation are the results of the simulation in comparison with the real vehicle. According ESC homologation it must be distinguished between active validation (e.g. steady state circle, sine sweep, etc.) and passive vehicle validation (with function). For the validation KPIs needs to be defined and a tolerance band. Those KPIs are of course different to those of the final test of the AD vehicle.

Traceability is important (analogue to other homologation tasks). For simulation traceability of the following things is required (models, tools, toolchain (configuration), model and simulation parameters (version, etc.) to reproduce at each time the simulation. Versioning and storage should be software supported (data base)

Everything needs to be document in a report.

The most challenging thing in validation of simulation is that you can optimize and adjust parameters that certain tests correlate but other will not (because the wrong parameters are adjusted). Simple example: a certain deceleration of the vehicle is required (based on real measurements): you can increase the friction coefficient of the brakes in your model or you can reduce the mass to improve the decelerations…

One approach would be to define the validation scenarios completely. Another would be that the authority does some spot testing. Does a real test with a data logger and reproduce those data in simulation… (for a random scenario within the ODD).

Sensor models is one challenging aspect here. Especially here some concept have to be worked out.

5. **Who validates virtual testing? Manufacturers? Authorities? determine some parameters to be checked?**

The validation process is complex and must be done by manufacturers. The authority can only approve. There are different approaches to do that (see point above): audit the process, check the results of the validations tests (KPIs and measurements), do some spot testing for validation.

Questions VMAD Working Group 2a

In use reporting

1. **How to ensure that manufacturer minimize risks over the lifetime of the vehicles?**

The concept/architecture must consider this use case. The general possibility should be assessed in the audit. E.g. software updates (maybe over the air) must be considered.

To be checked in regularly inspection. Maybe critical scenarios are collected (compare to airplane industry). Regularly inspection is checking what the manufacturer did in this direction.

Software Updates must be described in detailed and provided to the authority

2. **How to ensure that the newly foreseen scenarios are added to the vehicle capability over the lifetime of the vehicle.**

See above. Challenge: how to deal with new function which could not be implemented with the existing sensor setup. Reducing ODD is not an option, adding sensor is not an option.

3. **How do ensure operational feedback from the field on traffic scenarios?**

According airplane industry, central incident database.

4. **In use monitoring during development phase or also once the vehicle is on the market?**

In use monitoring in development is collecting data with prototype fleet? Should be required as part of the certification and the audit

5. **What kind of data shall be collected by manufacturers?**

Basic vehicle data, sensor data, meta-data (also possible from external sources) like weather conditions, etc. Data shall be collected only in case of an event (triggered). Trigger must be defined. Hard deceleration, etc.

Questions VMAD Working Group 2a

6. **What kind of data shall be reported to authorities? How often?**
   - Incident data according question above
   - Maybe also data of critical scenarios or homologation-relevant scenarios to show that the system works for such scenarios also in the reality
   - Continuously (to be defined based on e.g. robustness of sensors, after accidents, etc.)

7. **Who has access to the data?**

The manufacturer and the authority who assess the data. Not really a technical topic but a topic of data privacy. Maybe similar approach as in the airplane industry?

8. **What shall authorities do with this data? How do we ensure suitable oversight of the reporting?**

Continuous check: compare with initial data of the approval (did the behavior change, where did it change, etc.). Of course there will never be the same situation, some algorithms could help to automate the evaluation

Incidents: must be analyzed manually in detail

9. **How this data should be collected? Use EDR/DSSAD for in use reporting?**

Synergies to EDR/DSSAD make sense, maybe also synergies to the airplane industry

10. **How do we ensure compliance after an OTA?**

Continuous check of in-use data after an OTA. Compare with initial data (see question 8), depending on the content/size of the OTA (main release), additional tests are required.

Especially for OTA, simulation could help. The manufacturer must validate the new software against simulation?