Invitation to a virtual SafeTRANS Workshop

July 25, 16-18:30 MEZ

for the creation of a SafeTRANS Working Group
identifying key challenges and possible solutions to

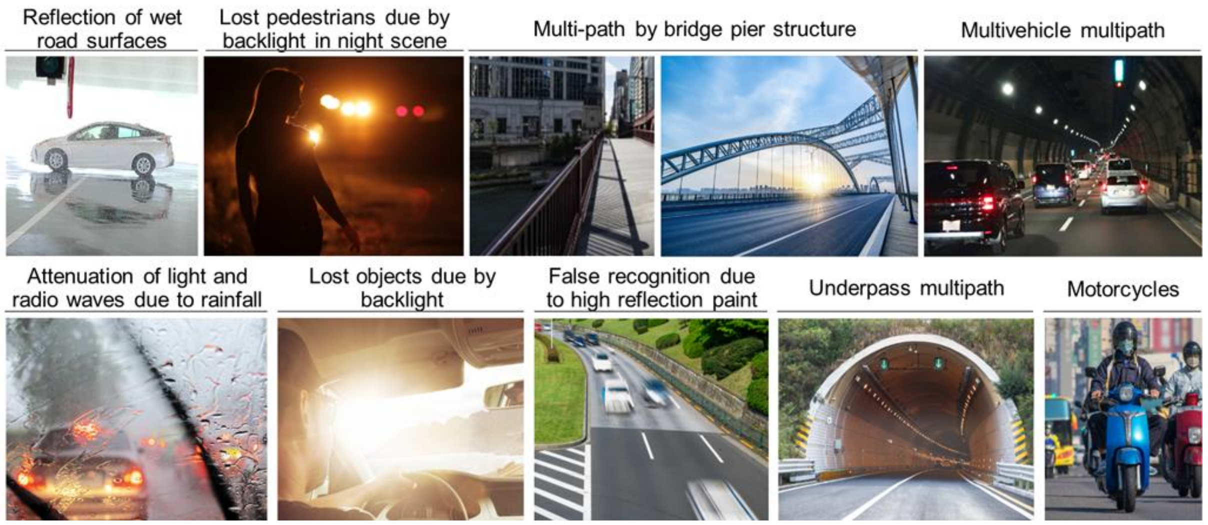
Closing the gap in deriving Virtual Assurance Based Safety Cases for Highly Automated and Autonomous Systems

as well as **preparing a formation of a new project**

Werner Damm, Chairman SafeTRANS
Henning Butz, previously head of AIRBUS System Development Hamburg
Peter Heidl, previously Chief Expert Research and Predevelopment, Robert Bosch GmbH
Roland Galbas, Projektleitung VVMethoden, Robert Bosch GmbH

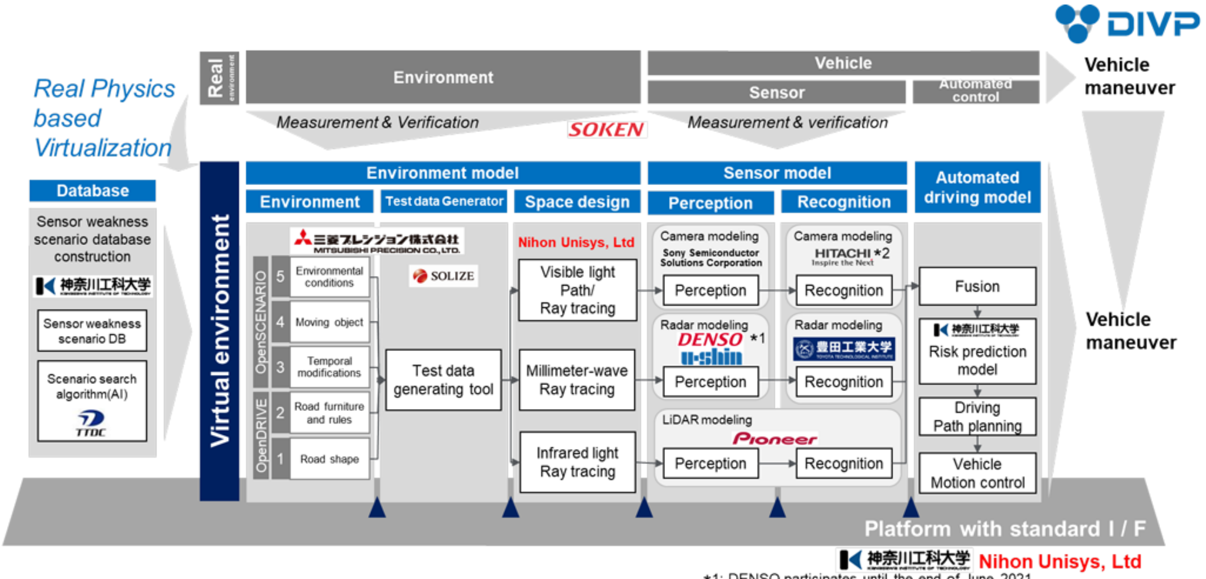
Significant investments have been made by the automotive industry towards establishing methods, processes, and tools for establishing functional safety of highly automated resp. autonomous vehicles.

In Germany, the Pegasus project has been proposing a basic initial scenario-based approach for system verification and validation, driven by highway applications. The VVM project focusing on Methods, toolchains, specifications for technical assurance, driven by urban applications, providing key achievements in identifying criticality measures, providing a scenario-based approach for assessing functional safety in given ODDs, and identifying typical classes of perception problems as well as developing methods for assuring robustness against such perception problems. The Set Level 4to5 project addressing the construction of simulation platforms, toolchains, and definitions for simulation-based testing. In particular, this project identified the key need to assess both credibility of simulations and credibility of models used in simulations wrt to sufficiently represent all relevant real-world phenomena. Measures for quality assurance of simulation and models, and process steps assessing the achieved quality, form an integral part of the proposed processes and methods. The Set-Level-4to5 project approached the challenging problem of developing models of Lidar Systems which faithfully reproduce the imperfections of such systems in different classes of environmental conditions. The Vivaldi project focusses in particular on virtual test environments for the sensor systems that are of central importance for connected and automated driving, allowing to simulate the functions of sensors, and the impact of the environment on the performance of sensors. The VVM process then provides guidance in how verification and validation methods jointly developed in both projects can providence the required evidences for assurance cases for highly automated and autonomous driving.


Reflection of wet road surfaces
Lost pedestrians due by backlight in night scene
Multi-path by bridge pier structure
Multivehicle multipath
Attenuation of light and radio waves due to rainfall
Lost objects due by backlight
False recognition due to high reflection paint
Underpass multipath
Motorcycles

In Japan, the Driving Intelligence Validation Platform (DIVP®)" project funded by the “Strategic Innovation Promotion Program (SIP) Phase Two - Automated Driving (Expansion of Systems and Services) (Building a safety evaluation environment in Virtual Space)”, is developing a safety validation platform in a virtual space featured by a series of "driving environment objects – electromagnetic wave propagations - sensors" models simulating real phenomena highly faithfully that could substitute for evaluation experiments in actual environments. Significant results have been achieved in providing virtual models of radar, lidar, and video-camera based systems.

DIVP has been developing a spatial propagation model enabled by a ray tracing system based on the reflection characteristics (Retroreflection, diffusion, specular reflection, etc.) and transmission characteristics of visible light for camera, millimeter wave for radar and near-infrared light for Lidar. This model is furthermore capable of duplicating the real physics that has influence of the surrounding environment such as rain, fog, and ambient illumination.



*1: DENSO participates until the end of June 2021
*2: HITACHI Astemo participates until the end of September 2021

Despite these significant achievements, these projects also show that **further significant research is needed to provide complete assurance cases combining evidences gained in virtual validation and verification with evidences generated in field testing** to achieve the high confidence levels required for safety assurance of level 4 vehicles.

We see the following gaps which must be addressed:

- There are[1] still **significant limitations in realism of models and simulations**, such as caused by
    - Perception:
        - Sensor phenomenology – anomalies based on noise, EMI, bad lighting (low sun angle, specular reflections), poor target resolution, …
        - Vision-specific errors – shadows, foreign objects on road, reflections, glare, worn or occluded signs and markings
    - Motion: Vehicle imperfections – worn components, tire contact friction, suspension bottoming, surface condition imperfections …
    - Localisation /Mapping: Road geometry and location
    - Contextual diversity of traffic interaction: Actions of other road users to try to avoid crash or driver override interventions
- **Even if we were able to find models which faithfully represent all artefacts of the physical system which is modeled, such models would be way to complex to allow large-scale cloud-based system testing**[2].
    - Much as in EDA design, we therefore propose to give up the strive for **one** "golden model" for each critical environment/system component for cloud based virtual simulation fitting, and instead propose a **use-case driven approach**:
        - Define and agree upon typical **abstraction layer**s in the design of highly automated driving functions.
        - For each abstraction layer, define and agree
            - All **use cases**: what types of analysis questions must be answered at this given level of abstraction to close the argumentation chain in assuring safety of the ADS
            - For each use case: agree upon a measure of **sufficient precision between real-world data and results from simulation**: How closely do simulations need to match test data to be considered "valid" for creating verification evidences for safety assurance at this abstraction layer?
        - For each abstraction layer and all use cases defined at this layer, define and agree upon measures to **validate the quality of models and simulators to prove sufficient preciseness between real-world data and simulation results**.

[1] *Safety Assurance to Earn Public Trust: Formalizing the Safety Case for ADS*, Steven E. Shladover, Sc.D.

California PATH Program, presentation at the midterm VVM project meeting, March 2022

[2] As a particular instance, consider the vast improvements made in Japan within the DIVP project on modelling radar systems. These models are high dimensional non-linear differential systems of equations. Any attempt to do real-time or close to real-time simulation can only work, if abstractions to lower dimensional models are applied. But then the question arises, whether this abstraction is sufficiently precise.

        - For each abstraction layer, **define constraints and safety requirements on the realization of system components at the next lower design layer**, such that any implementation of the system on the lower design layer meeting the design constraints and meeting the safety requirements can be "plugged in" the component representation at the higher design layer without violating any of the constrains and safety requirements established on the higher layer.
        - Analysis of "causal relation" of influencing factors towards the limitation of system by e.g. causal graphs and bayes networks (combining systematic approaches with data driven approaches). Development of models expressing this "causal relations".
        - Analysis of the modelling limitations towards the influence to perceptional preprocessing (e.g to the dense optical flow, radar reflectance points or lidar point-cloud) and furthermore to their influence to the semantic processing (e.g. object detection).
        - Deep Analysis of modeling influences towards AI based semantic processing w.r.t. the special characteristics of neural networks.
        - Building up quality metrics for each layer and thus enable e.g. AI based perception processing to be fused and integrated effectively.
- **Dealing with rare events/ corner cases**:
    - Crash-imminent situations stretch simulations beyond their normal validity (extreme conditions, nonlinear performance)
    - Cannot represent huge diversity of human performance realistically in models or tests, in particular safety-critical scenarios amplify randomness and diversity in human behavior
- We therefore propose to **complement** the above compositional approach **by an analysis of extreme corner cases** and to define and agree upon coverage measures for such corner cases as sufficient verification evidences to covering such rare cases for safety assurance (this is analogous to taking into account the likelihood of being exposed to such traffic situations and their persistence when analyzing the risk classifications in ISO 26262)
    - Define and agree on the abstraction layer required to perform a particular corner case analysis
    - define and agree upon the analysis use cases (which verification challenges must be answered for this corner case analysis) and a measure of sufficient precision between real-world data and results from simulation for each corner case and each of its use cases: How closely do simulations need to match test data to be considered "valid" for creating verification evidences for safety assurance
    - A particular challenge arises in generating the required test-data, because of ethical considerations. What tests are needed to produce a validation data set containing those extreme combinations of conditions? How can they be generated safely?
    - Emergences
        - Analysis of relevant systemic emergences (w.r.t. safety)
        - Analysis of relevant classes of uncertainties (aleatoric, epistemic, otologic) and their influence towards the systemic emergences (w.r.t. safety)
        - Monitoring of uncertainties
        - Modelling of uncertainties within system

- We define methods and processes allowing to integrate all verification evidences generated by corner case analysis and use-case driven compositional analysis into an **overarching safety assurance argument**.

In a kick-off workshop organized by SafeTRANS on July 25, we will get together key experts in the above topic areas to discuss the **creation of a SafeTRANS Working Group** identifying key challenges and possible solutions to **Closing the gap in deriving Virtual Assurance Based Safety Cases for Highly Automated and Autonomous Systems**, as well as **preparing a formation of a new project building** on and incorporating the results of the foreground projects addressed above.