Translated article "Anwendungsorientierte Absicherungsstrategie für Fahrerassistenzsysteme," ATZ extra 07/2017

A reliable validation strategy for driver assistance systems

Supplementing real test drives with virtual simulations offers enormous potential for designing an efficient validation process. Yet such testing must constantly be aligned with real driving situations and the underlying scenario catalogue must be expanded in an iterative process.

Looking ahead to the future

It is still unclear how drivers will use the time that self-driving cars free up for them. Some will gaze off into the distance; others will read the paper, answer emails, or play games on their laptops. Still others will keep their hands on the wheel because they enjoy driving. If they're not in the mood, the autopilot can always take over.

All this requires that passengers trust the active vehicle systems. With every advance toward automated driving, the responsibility of automotive manufacturers and their engineers grows. The industry needs reliable validation strategies for self-driving cars that observe and analyze traffic situations so as to completely relieve drivers of the task of driving.

Impossible to specify a complex environment in advance

The requirements of this system validation go above and beyond those defined in ISO 26262 for functional safety. That's because it's not enough to prepare the active assistance systems for the event of system failure at the functional level: safeguards have to be built in to ensure that situations aren't misinterpreted. But it simply isn't possible to address all eventualities of actual traffic situations in a system specification that is drawn up in advance. There are too many different scenarios inside and outside cities and on highways. Add to that a range of weather conditions (fog, snowstorms, etc.), various lighting conditions, and traffic laws and cultural conventions that vary from one country to the next.

The term for this set of problems is "functional insufficiency" [1]. In the context of software quality, this issue is referred to as "robustness". Robustness describes the "property of an observation unit (...) to work as defined even in unusual situations, and to take appropriate action" [2]. This definition indicates that, with respect to software systems in general, not all states can be identified in advance at acceptable levels of time, effort, and cost. When applied to validating assistance systems, it implies that it is by definition impossible to achieve a zero-percent accident rate. It also raises the question of how to bring the robustness of autonomous systems up to a socially acceptable level and continuously improve it.

Reliable validation strategies needed

Against this backdrop, probability-based validation approaches are one way to assess the robustness and the utility of assistance systems. Whether or not these approaches achieve social acceptance lies outside the scope of this paper. The chair of the German Ethics Council, Peter Dabrock, argues in favor of a pragmatic approach [3]. Instead of getting bogged down in "feverish preoccupation with thought experiments," Dabrock says it is better to constantly review and assess the shift toward automated driving using consistently updated documentation.

A pragmatic ethical evaluation, however, does not release vehicle engineers from their obligation to create the safest systems possible. H. Winner presents a probability-based validation approach for an autonomous highway pilot [4]. This model approach shows that, even in this relatively straightforward use case, a test vehicle would have to drive $2.4 \cdot 10^8$ kilometers to establish (with a 5% probability of error) that, on the highway, vehicles with assistance systems cause a maximum of half as many accidents resulting in injuries as do vehicles without such systems.

Equivalence-class-based scenario descriptions

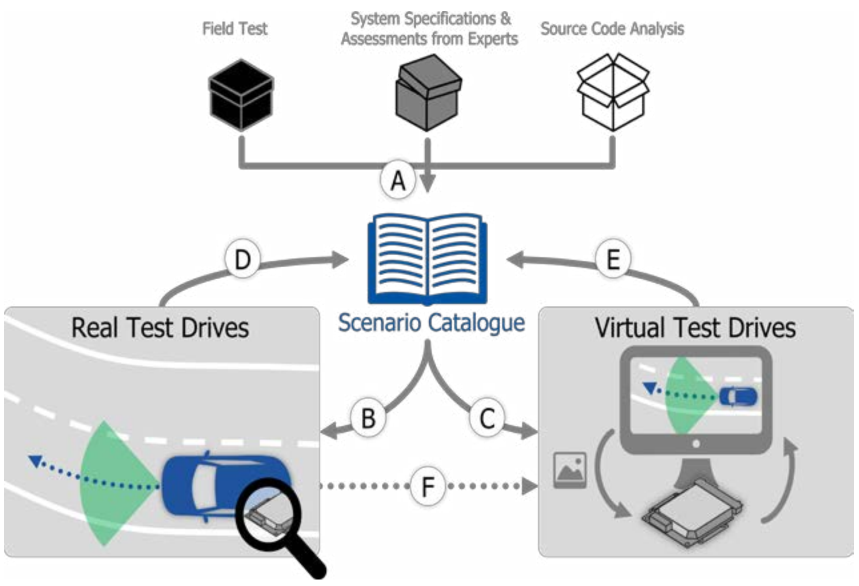
The aim of such a validation process is to demonstrate the probability P that a system meets metric M (for example, metric M could be: vehicles equipped with the assistance system cause only half as many accidents resulting in injuries as vehicles without the assistance system). Based on a test site d_E=highway, probability is determined by $P(M \mid \text{highway})$.

If the system behavior is to be observed somewhere other than the highway, then the test site is d_E=non-highway, yielding the overall probability P_{tot} of meeting the metric, **EQUATION 1**.

Eq. 1

$$\begin{aligned} &P_{tot}(M) \\ &= P(M \mid \text{highway}) \\ &\cdot\ P(\text{highway}) \\ &+ P(M \mid \text{non-highway}) \\ &\cdot\ P(\text{non-highway}) \end{aligned}$$

Image 1: The validation approach.



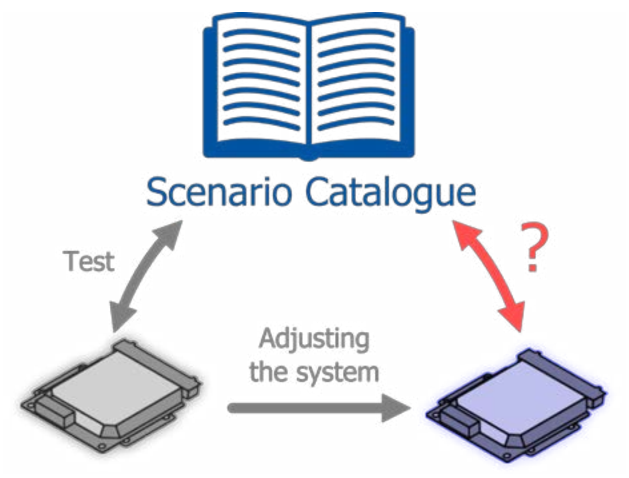


Image 2: Can a scenario catalogue be adjusted when the system has been modified?

Should the test drives reveal that the non-highway sites can be split into urban and rural areas within which the system behaves in an equivalent fashion (equivalence classes, cf. [2]), then the test site can be completely split into three equivalence classes: d_E={highway, urban areas, rural areas}. Consideration of the metric is thus complete for the defined parameter space.

A detailed examination of a test campaign may reveal that the system works perfectly on dry roads, but frequently fails on wet surfaces. This finding can be incorporated into the description by introducing a further dimension, road conditions d_S={dry, wet}, resulting in six scenarios in which the metric must be tested.

Generally speaking, a scenario S can be defined as the combination of each equivalence class with each dimension: $S=[d_1, d_2, \ldots, d_n]$. The overall probability P_{tot} of meeting the metric is generally calculated for n dimensions d_n, **EQUATION 2**,

Eq.2

$$P_{tot}(M) = \sum_i P(M \mid S_i) \cdot P(S_i)$$

where the number of scenarios i is the result of the cardinality of the equivalence classes of all dimensions, i.e. $i = \Pi \mid dn \mid$.

In the experiment, specific test cases are needed to determine $P(M \mid S_i)$. A test case is an element of a scenario (cf. [5]). Software quality assurance methods can be used when selecting the test cases. The overall sum of the various scenarios serves as a reference value for the number of different test cases and is essential for reliable system validation.

Iterative expansion of scenario descriptions

Scenario descriptions, which are based on equivalence classes and can be refined with an iterative method, can now be applied in an application-based process for validating autonomous systems. This process is depicted in IMAGE 1.

At the core of the iterative validation strategy is a scenario catalogue based on information drawn from three qualitatively different sources (A). One consists of findings from endurance and field tests in which the system did not behave as expected. Further scenarios can be created by incorporating system specifications as well as assessments from experts, and the third source is static source code analysis.

The resulting scenario catalogue not only helps produce a flow chart for systematizing real test drives (B), but it also serves to parameterize virtual test drives (C), which offer multiple advantages. For example, virtual tests can be run simultaneously on any number of computers, so they aren't dependent on the availability of expensive test vehicles. In addition to the reduced cost, time, and administrative effort, a further advantage is that engineers can take critical situations that occur during real test drives and reproduce and modify them as needed in virtual testing.

By systematically or randomly varying the elements of a scenario in test drives, engineers can identify new scenarios in which the system doesn't respond as expected. After analyzing them, they then methodically add the newly identified scenarios to the catalogue (D and E), allowing for continuous improvement of test coverage. If this transfer step is omitted, the problems detected during the test drives are meaningless.

Any overall cross-domain simulation of assistance systems requires reliable validation of the underlying models. This, in turn, calls for comparing the individual scenarios in real and virtual test drives (F). The comparison makes it possible to issue reliable statements regarding the accuracy of the overall simulation as well as the scopes of the models. Moreover, this process gradually produces an increasingly precise and comprehensive basis for virtual testing of assistance systems.

Simulation: the key to validation system variants

When such tests discover and fix errors in the driver assistance systems, this changes both the system to be tested in real test drives and $P_{tot}(M)$. This appears at first to be problematic, inasmuch as the measurements taken thus far can no longer be used in the validation without further reasoning. And that raises the question: can a scenario catalogue be adjusted when the system is modified? (IMAGE 2)

Answering this question requires determining whether or not the equivalence classes are still equivalent and how $P(M \mid S_i)$ is affected. One way to do to this would be to use model-based simulation. If the behavior of the driver assistance system is validated based on scenarios, and the scope of the underlying models has been defined, then the modified system can also be evaluated using the validated models in the simulation – provided the modifications are within the model scope. This flexibility is the key to validating any system variants that arise.

The authors of [6] describe, for example, a physically based model for environment sensors. Their model can be validated for various positions of an ultrasonic sensor for specific scenarios S_i, thereby validating the scope for this model. In this way, any changes to the position of a real sensor in the simulation can be evaluated, and the model can be used to review the equivalence classes and to assess $P(M \mid S_i)$ of the modified system.

Conclusion

The iterative approach presented here is a viable validation method with which engineers can address the challenge of functional insufficiency in self-driving cars. Endurance tests produce insights, experience, and findings that flow into a central scenario catalogue. The compiled scenarios, all described in a standardized way, can help in the parameterization of both real and virtual test drives. And because this description of real and virtual tests is consistent, it is also possible to use the scenarios as a basis for validating the simulation. The method presented here is therefore a good way to make the testing of safety-relevant assistance systems in self-driving cars more flexible and to expand it by including a learning dimension. It provides a transparent and comprehensible basis for designing robust autonomous driving functions.

Authors

Marius Feilhauer, M. Sc., develops simulation models for driver assistance systems in Test and Validation at ETAS GmbH in Stuttgart.

Dr. Jürgen Häring is head of product management in Test and Validation at ETAS GmbH in Stuttgart.

[1] Wilhelm, U.; Ebel, S.; Weitzel, D.: Funktionale Sicherheit und ISO 26262. Validierung von Systemen mit funktionaler Unzulänglichkeit. Bd. 3. In: Winner, H.; Hakuli, S.; Lotz, F.; Singer, C. (Hrsg.): Handbuch Fahrerassistenzsysteme: Grundlagen, Komponenten und Systeme für aktive Sicherheit und Komfort. Wiesbaden: Springer Vieweg, 2015, S. 85-103

[2] Liggesmeyer, P.: Software-Qualität: Testen, Analysieren und Verifizieren von Software. 2. Auflage. Heidelberg: Spektrum, Akademischer Verlag, 2002

[3] Dabrock, P.: Ethische Dilemmata unterlaufen oft Akzeptanz von autonomen Fahrzeugen: Ethik und autonomes Fahren. In: Tagesspiegel vom 23.03.2017

[4] Winner, H.: Quo vadis, FAS?, Bd. 3. In: Winner, H.; Hakuli, S.; Lotz, F.; Singer, C. (Hrsg.): Handbuch Fahrerassistenzsysteme: Grundlagen, Komponenten und Systeme für aktive Sicherheit und Komfort. Wiesbaden: Springer Vieweg, 2015, S. 1167-1186

[5] Schmidt, A.: Einführung in die algebraische Zahlentheorie. Berlin, Heidelberg: Springer-Verlag, Berlin Heidelberg, 2007, S. 7

[6] Feilhauer, M.; Häring, J.: Ein echtzeitfähiges Multi-Sensor Modell zur Validierung von Fahrerassistenzsystemen in einer virtuellen Umgebung. In: 3. Internationale ATZ-Fachtagung Fahrerassistenzsysteme, 2017