Journal of Systems Architecture 85–86 (2018) 1–13

Contents lists available at ScienceDirect

Journal of Systems Architecture

journal homepage: www.elsevier.com/locate/sysarc

Reliability and test effort analysis of multi-sensor driver assistance systems

Florian Bock*,[a], Sebastian Siegl[b], Peter Bazan[a], Peter Buchholz[c], Reinhard German[a]

[a] Department of Computer Science 7, Friedrich-Alexander University Erlangen-Nürnberg (FAU), Erlangen 91058, Germany
[b] Audi AG, Ingolstadt 85045, Germany
[c] Department of Computer Science IV, University of Dortmund, Dortmund 44227, Germany

ARTICLE INFO

Keywords:
Discrete-time Markov chain
Reliability analysis
Test effort estimation
Sensor-based
Driver assistance system
Multi-sensor

ABSTRACT

Modern driver assistance systems for self-driving cars often rely on data collected by different sensors to determine the necessary system decisions. To prevent system failures, different validation techniques are used. The development is often split between car manufacturers and suppliers, whereby the requested test effort is one main project acceptance criterion. Already available effort estimation methods are not applicable, because they rely on implementation details that do not exist at early phases or on project experiences or individual expert expectations, which are not reliable enough to be employed as trustworthy source. Therefore, we provide in this paper an analytic approach for the computation of the error probability of a multi-sensor system. Based on this, we can give estimations for the test effort such that with statistical confidence no errors of the sensor system can be expected during the tests. The approach is able to take both the dependencies between successive sensor errors and the correlation between different sensors into account, mainly by using discrete time Markov chains. The provided approach therefore allows to design multi-sensor systems such that a specified overall error probability can be met and to give an estimation for the upper bound of the test effort.

1. Introduction

Automotive systems have evolved during the last decades from purely mechanical to complex electronic cyber-physical systems. The first generation of driver assistance systems during the 1970s [1] offered driving support in the form of simple security enhancements, such as *ABS* [1]. Advanced versions of these systems were capable of braking in emergency situations or maintaining the vehicle speed via cruise control [2]. Nevertheless, those systems are only first steps in the ongoing development of modern driver assistance systems.

In the course of the last years, a great number of such systems have been developed, introduced, evaluated under real circumstances, and extended. As a logic result of this rapid development, the threshold, at which enough systems are available to be combined into a completely self-driving system, is getting closer and closer [3]. Although many technical and legal issues are not yet addressed properly [4], such prototypes are already capable of handling complex traffic situations autonomously for a certain limited time span [5]. In theory, from a technical point of view, autonomous navigation without any human interaction from one point A to a destination point B is already possible, although extensive use of driver assistance systems would be required [3,5].

The involved driver assistance systems are highly complex decision systems, which use aggregated data to calculate certain system decisions or recommendations. These decisions are used to correctly address diverse actors and - in succession - to control the car properly. The aggregated data is mostly collected and delivered by different types of sensors, which measure certain environmental or scenario-related data (e.g. vehicle speed, temperature, trajectory data, etc.). The correctness of the collection, aggregation, fusion, and interpretation of this data is essential for the reliability of the successive decision calculation.

Therefore, the development of advanced highly reliable sensors with a wide range of functions is one main ongoing topic for the automotive supplier industry. It is the task of the automotive manufacturers to choose appropriate sensors out of the suppliers' product portfolio, so that the requirements of the driver assistance systems under development are met.

Especially during the project specification phase, many details about the future implementation of the currently developed driver assistance system are not yet defined. Nevertheless, especially if the development tasks are outsourced to external suppliers, the specification does have to include a reference value for the test amount that has to be carried out by the supplier in order to guarantee a certain level of system reliability. This value is currently mainly based on previous

* Corresponding author.
E-mail addresses: florian.inifau.bock@fau.de (F. Bock), sebastian.siegl@audi.de (S. Siegl), peter.bazan@fau.de (P. Bazan), peter.buchholz@cs.tu-dortmund.de (P. Buchholz), reinhard.german@fau.de (R. German).

https://doi.org/10.1016/j.sysarc.2018.01.006
Received 15 November 2017; Accepted 23 January 2018
Available online 14 March 2018

project experiences and individual expectations [6]. Particularly in the case of modern driver assistance systems for self-driving cars, much more conclusive and reliable values are required. Because most of the available estimation methods are based on technical system information or detailed implementation analysis, they cannot be used during an early specification phase.

To address this, we proposed a new analytical approach to estimate the test effort for multi-sensor-based systems that is required to guarantee a certain level of statistical significance [6]. Here a systematic and extended presentation is provided.

First, we provide a systematic definition of relevant events and then derive analytic expressions to compute the corresponding event probabilities. In case of independent events, a simple multiplication of probabilities is possible. However, since we also allow for dependencies between events, both between successive sensor detections and between the detections of different sensors, we must provide a more complex stochastic model. For this purpose, discrete time Markov chains are used, they have an intuitive semantics, they are able to represent the relevant memory by the state information, and lead to feasible computational solution formulas. In case of correlations between sensors the problem of parameter fitting needs to be addressed, a possible solution based on optimization is presented. A discrete-event simulation of the system is used for comparisons, validations, and illustrations. Based on the error probability from the analysis or simulation, a systematic approach is then given to compute an upper bound of the test effort such that with a predefined statistical significance the sensor system shows no errors, this can be used in practice to specify an upper bound for the test effort.

This paper is organized as follows. Section 2 describes the problem domain. Section 3 summarizes related work and rates them with regard to the present use case. In Section 4, all relevant details about the multi-sensor system are listed and explained. The relevant system and sensor events used in our approach are introduced in Section 4.2. Section 5 contains the main contribution of this paper, the analytical approach for the test effort estimation. Here, three different cases are discussed, the related formulas are given and explained. Section 7 describes an exemplary implementation of the approach as standalone simulation and computation tool, where different aspects such as graphical evaluation possibilities are emphasized and Section 6 discusses, how the required parameter fitting can be done by means of solving an optimization problem. For illustration and proof of concept purposes, Section 8 includes several examples with the corresponding results, which are evaluated. To conclude, Section 9 gives a short summary and an outlook to outstanding issues.

2. Problem definition

The development and the introduction of new driver assistance systems is only possible in conjunction with extensive testing. Although it can never be guaranteed that a system is 100% error-free [7], the goal is to test as long as required to guarantee the correctness with a predefined level of confidence.

The required feasible test effort is affected by different facts:

- Iterative rapid development mostly leads to frequent regression tests to maintain the system quality.
- Testing in the automotive context often involves real cars as prototype systems, which are expensive and therefore only available as limited resource.
- Especially in case of self-driving systems, the unclear legal situation [4] limits the available testing scenarios and locations.
- Due to the vast number of possible usage scenarios and the involved influencing factors, a complete test plan is hardly obtainable.

The resulting test length that addresses all the above mentioned influencing factors defines the amount of testing that is required to achieve an approval of the system. Therefore, the automotive manufacturers as well as the suppliers have to carry out such tests in order to successfully complete the development projects. As project definition provider, the manufacturer is able to conduct and verify the necessary tests as long as the development is performed in-house. However, as soon as the development is outsourced to external companies, reliable key indicators have to be defined in the project specification documents for the tests to be carried out. These indicators are then used as guideline for the developing company to attest their testing effort and as control value for the project manager to verify the quality.

One crucial point regarding the required test effort is the used method to determine exact values. Although there are many established analytical methods to determine the effort by analysing the implementation details and the specific detailed scenario characteristics, they are not applicable here due to the early specification phase. Details about the system under development and the related implementation are probably neither created, nor even defined. Therefore, the test effort for many projects is currently estimated by experiences from previous projects or by the assessment of individual project experts. Especially in case of cyber-physical systems such as driver assistance systems for self-driving cars with the corresponding sensors and actors, such experiences are not sufficient and previous projects do not exist. Nevertheless, a reliable estimation method is required and was developed as response to this need.

3. Related work

The approach from Herpel et al. [8] allows the selection of appropriate sensors for a given project scenario by utilizing a so-called ξ-function with the sensor-range limitations, sensor resolution and related field-of-view limitations as input. Although the resulting sensor rating is an indicator for suitable sensors, the lack of a test length determination method does not satisfy the requirements in our use case.

The approach from Brumback and Srinath [9] uses navigation systems as example for the fault tolerance of multi-sensor-based systems. For this, the use of a parametrized *Kalman filter* [10] is proposed. It is configured for the detection of faulty sensor data. Although it is quite common in the automotive industry, such a parametrization is not possible during the specification phase due to the lack of detailed system information. Because of this and because of the missing consideration of test lengths as key indicator, the approach is not applicable in the given context.

Berk et al. [11] focus on Bayesian networks in order to take environmental disturbances and other effects on sensor data into account. The detailed analysis of sensor data and the data collection are helpful during the implementation or the test phases, but not during the specification phase. Nevertheless, the results determined by this approach can be used during later project phases as comparison values to our test lengths for verification and validation purposes.

During the last decades, the topics of sensor data verification and data fusion were part of ongoing research and development. Besides the summarized approaches, many more are available. However, to the best of the author's knowledge, none of the existing methods specifically deals with test effort estimation for sensor-based driver assistance systems at early project phases and is based on a rigid analysis of the system error probability also taking correlations into account. Because of this, the method proposed below was developed.

4. System description

In order to develop a reliable test effort estimation method for multi-sensor-based driver assistance systems, as preparation step, the target system has to be analyzed and described in detail. Besides the main goal to achieve a trustworthy analytical method, there are three different aspects that are noticeable in this context: the usage of multiple sensors, the specification phase as given development period, and