An Evaluation of Mobile with the Hierarchical Approach

Yi Cao

Depart. of Automobile Engineering, Zhengzhou University of Science & Technology, Zhengzhou, China

Abstract. The safety evaluation of MOBILE demonstrates the applicability and benefits of the hierarchical approach. Quantitative figures give a rough impression of the safety level. Additionally, relative changes in failure rates after modifications to components or the architecture of electronics can be observed. Working with a group of students showed that the hierarchical approach supports splitting of the complex vehicle design task into a number of smaller work packages that are easier to handle. At the same time, the system context is kept available and traceable for all developers.

Keywords. Evaluation, mobile, hierarchical approach.

1 Introduction

This paper evaluates the safety of the vehicle control function of MOBILE using the hierarchical approach introduced in the previous section. As MOBILE is a primarily student driven university project, some restrictions have to be regarded:

(1) Up to 20 students were working on parts of the vehicle in parallel. Each student works on a specialized field on a low hierarchical level. The students are assumed to be the experts for a specific field. The work on higher levels is mostly done by members of the scientific staff.

(2) Failure rates are not available for all parts of MOBILE. For these parts typical values were derived from literature. Failure rates of software under development is roughly estimated based on previous in-field experience.

(3) Aging effects are approximated by typical bath-tub curves given in literature. Thereby, one observes slightly higher failure rates of hardware components in early phases of the part's life time and a significant increase towards the end of the life time.

(4) Only the hierarchical layers "vehicle", "system"and "subsystem" have so far been taken into account. Some individual components of the underlying hierarchical layers are currently being investigated and results are fed back to the evaluation of MOBILE.

(5) Processes performed during development of MOBILE do not comply to the requirements imposed by ISO 26262.

(6) As the construction of MOBILE is not yet finished, only qualitative results are given that origin from quantitative but not yet complete data.

Still, the safety evaluation of MOBILE demonstrates the applicability and benefits of the hierarchical approach. Quantitative figures give a rough impression of the safety level. Additionally, relative changes in failure rates after modifications to components or the architecture of electronics can be observed. Working with a group of students showed that the hierarchical approach supports splitting of the complex vehicle design task into a number of smaller work packages that are easier to handle. At the same time, the system context is kept available and traceable for all developers.

2 Assumptions for the safety analysis of mobile

As indicated before, top level assumptions on the mode of operation of MOBILE are required to evaluate the functional safety of MOBILE: The mission time of MOBILE is limited to 30 min. After 30min, the lead-acid drive batteries are assumed to be emptied anyways or the test driver is expected to have a break. In case of a failure, the emergency operation interval that has to be guaranteed is set to 30s. This time span suffices to get MOBILE to a safe halt even if the failure occurred while driving at MOBILE stop speed of approx.160km/h(44m/s). It is assumed that only one independent fault has to be tolerated. For MOBILE, one "point in time" is defined as a 4ms time slot. This slot length is derived from the cycle time of the Flex Ray network in MOBILE that facilitates synchronization of all network nodes and precise triggering of the diagnostic algorithms. If two faults occur within a 4ms time slot, they are treated as a double fault at one point in time. A similar assumption for small diagnostic time intervals is, e.g., made by Sieglin.

3 Evaluation of complexity of the hierarchical approach

On "system layer" of MOBILE, eight units were defined: front and rear axle control system consisting of the according FTUs, user input control system (also embodied by the according FTU), two power supply systems, emergency off systems for front and rear drive motors and the stability control system [1]. Due to the design of MOBILE, these systems can be regarded as insusceptible to common cause failures—except loss of power. If cross couplings between the systems exist, the couplings are assumed to be irrelevant during the emergency operation interval of 30s, e.g., low voltage buffer batteries can compensate the loss of charging power due to failure of the high voltage system. In particular, this independence of the elements at "system level" led to the definition of the virtual systems as given and not to the classical system partitioning into braking, drive and steering system. For each of the chosen virtual systems, 2 to 9 generalized failure states, not including the "0k" / "no failure present" state, were defined. Resulting, 31 failure states have to be evaluated on vehicle layer. Thereby, the controllability of the vehicle has to be evaluated after occurrence of a given first and second system failure, summing up to 702 state transitions. Especially, for the second faults, several transitions need not be regarded as they do not furthermore impact the controllability of the vehicle [2].

Additionally, several transitions are identical for more than one system and thus only have to be considered once. For each failure scenario, the state of the vehicle is well defined as the generalized failure states are part of a first order Markov Chain. Thus, all relevant information is contained in the state descriptions and no knowledge about the failure history is needed. Given the knowledge about the effects of the system failures on vehicle dynamics, it takes the developer approximately an hour to go through all states and define the according consequences. Table8.5 shows a simplified classification for MOBILE after the first failure for each system [3]. Within the tool environment, the classification is done graphically based on Excel tables by color highlighting. For the evaluation of MOBILE on vehicle level, several experiments with a 1:5 scale vehicle were performed to estimate the effect of actuator or power supply failures on the controllability of the vehicle. Additionally research results of other groups were taken into account to fully exploit functional redundancies. Still, the classification at vehicle level is a challenging and not fully solved task from a scientific point of view but easy to handle formally, which allows the researcher to focus on his main tasks.

The failure states on "system layer" are derived from approximately 60 failure states on "sub system layer". In average, on system level approx. 100 state transitions have to be evaluated per system. Thereby, the behavior of the system for all "first faults" has to be considered. Additionally, selected "second faults" have to be investigated. Second faults that have to be regarded are identified automatically top down from "vehicle level". The number of state transitions that have to be investigated by the developer serves as an estimate for work load and complexity. If compared to "vehicle level" and depending on the individual system, the individual researcher on system level has to evaluate a similar amount of relevant combinations [4]. On lower levels (component and elementary) the number of total failure states furthermore increases but again can be handled due to the partitioning into virtual systems and allocation of tasks to local experts. Third party components can easily be integrated at any hierarchical level. Within the project MOBILE several such components exist (steering motors, drive motors, etc.). As mentioned, the evaluation process in the project MOBILE is supported by an Excel Sheet. Necessary calculations and the linking between hierarchical layers are automatically derived from "graphical" inputs of the user.

As the input tables are continuously being updated during the development process, the current state of the vehicle with regard to safety as well as the most critical components are known at any point in time. The generalized failure states including proper documentation support transparency and long time usability of the results of the safety analysis. These state descriptions also form the basis for discussions between experts in different fields and on different hierarchical levels. A further extension of the tool environment to automatically link graphical architecture descriptions or descriptions of state transitions with the inputs in the Excel environment would be useful. Currently, these steps are performed manually, which is acceptable for the scope and scale of the project. Summarized, the analysis results for MOBILE can serve as a well documented and tailored safety report and support continuous monitoring during development. The tailoring of the analysis by front loading knowledge on dependencies lowers work effort compared to other hierarchically structured approaches.

4 System monitoring and failure rates

This illustrates the failure rates of MOBILE at vehicle level over lifetime. Thereby, the failure rate was calculated using the approach detailed in Sect.8.3 for several points in time. The curvy form of the graph with high increase in failure rates towards the end of the vehicle lifetime results from the assumed aging of hardware parts. As introduced above, software parts that feature a high probability of failure are also taken into account—differently from the approach in ISO 26262. Of course, these failure rates are highly volatile, but are several orders of magnitude higher than the failure rates of the underlying hardware and thus have to be considered. Of course, software components are unconcerned by aging. Figure8.24b visualizes the huge benefit for failure compensation in the vehicle by considering interactions at “system” and “vehicle layer”. E.g., the curve for “system layer” considers only cross-compensations between different systems up to “subsystem level” and so on. On higher layers, these cross-compensations are more and more due to functional redundancies. Thus, a highly flexible vehicle as MOBILE especially profits. Analogously, the efficiency of the diagnostic coverage over lifetime is automatically derived from the gathered data.

Tendencies show, that the proposed integrated safety concept relying on functional redundancies can increase functional safety while also maximizing the functional benefit from additional actuators and limiting system costs due to reduction in required hardware redundancy. Still, final results can only be provided after the vehicle has been completed, and further experiments can be conducted.

5 Conclusion

This contribution introduces a novel system architecture for an experimental drive by-wire vehicle with high functional integration and over-actuation. For this vehicle, a system architecture is derived top-down driven by according requirements. Especially, the top-down partitioning of the system can reveal novel structures also for series vehicles. Resulting, a system structure that exploits functional redundancies instead of hardware redundancies for safety purposes is presented. Exploiting functional redundancies necessitates a clearer definition of the safe state of the vehicle compared to typical part-oriented safe-state assumptions. For MOBILE, a model of the desired minimal vehicle dynamics is used. Consequently, control algorithms for vehicle dynamics play an important role in the proposed safety concept, and assessment of quality of these algorithms has to become more quantitative. To evaluate the safety of complex and integrated systems as proposed for MOBILE, a hierarchical approach to safety analysis is introduced. The approach complements already existing means for safety evaluation by taking a holistic view of the overall vehicle. It especially focuses on the targeted evaluation of highly integrated systems that provide functional redundancies. Therefore, virtual systems and generalized failure states support early reduction of the number of faults that have to be analyzed quantitatively. At the same time, system partitioning promotes allocation of work packages to developers that are best suitable. As given, the proposed approach features some restrictions and potential for further development. Especially, questions related to a development process in industry as intellectual property, responsibilities, or process management are not regarded in this contribution. Future work will focus on completion of the safety evaluation of

MOBILE. Starting from there, the further usage of the structured information on the system architecture for online self-representation of the vehicle and diagnostics will be investigated. Another important topic of future work will be the ongoing evaluation of control algorithms for vehicle dynamics to exploit functional redundancies between different types of actuators by coordinated control of remaining actuators. In parallel, analysis of critical components of the EE system will go on with regard to functional safety and failure rates.

References

1. Abele, A.: Design and realization of an integrated safety concept based on an architecture model with the given example for the serial development of a power train control unit used in electric driven vehicle. In: Hybrid and Electric Vehicles, pp. 481–525. Braunschweig (2012).
2. Adachi, M., Papadopoulos, Y., Sharvia, S., Parker, D., Tohdo, T.: An approach to optimization of fault tolerant architectures using HiP-HOPS. Softw. Pract. Experience 41(11),1303–1327(2011).
3. Anwar, S., Niu, W.: Analytical redundancy based predictive fault tolerant control of a steer-by-wire system using nonlinear observer. In: 2010 IEEE International Conference on Industrial Technology, pp. 477–482 (2010).
4. Baustein zukünftiger funktional strukturierter Domänenarchitektur im Fahrzeug. In: AUTOREG 2011, pp. 375–387. Baden-Baden (2011).