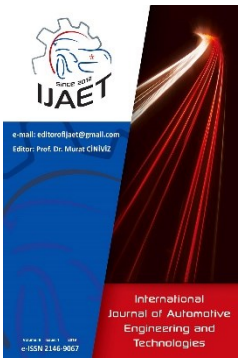
e-ISSN: 2146 - 9067

International Journal of Automotive Engineering and Technologies

journal homepage:
https://dergipark.org.tr/en/pub/ijaet



Original Research Article

Dimensioning of fail-operational powertrain for automated driving

Ahmet Kılıç

Robert Bosch GmbH, Germany

ARTICLE INFO

* Corresponding author
kilicahmet40@gmail.com

Received: Jan 02, 2020
Accepted: Jan 30, 2020

Published by Editorial Board Members of IJAET

ABSTRACT

The automotive industry is changing due to automation, e-mobility, connectivity and shared mobility. For realization of automated driving systems, a high degree of safety, security and reliability is required. In today's vehicles a driver serves as a fallback for control, mechanical and energetic levels. Automated driving is a new market and requires fail-operational subsystems and components enabling the highest required safety level. One possibility to fulfill these requirements is designing a redundant system. Since such a design is not always possible and optimal in a vehicle due to the cost, size and weight factors, new system architectures are needed. A fail-operational electrical powertrain (power net, electric machine with inverter and battery) is a main prerequisite for introducing automated driving. This paper presents the concepts for developing fail-operational powertrain solution for automated driving.

Keywords: Automated driving, Fail operational Powertrain, Topologies Powernet, Electric vehicle.

1. Introduction

A new mobility solution is required due to the increasing of the person and goods transportation as well as the growing of urbanization. The mobility of the future is expected to undergo a major shift from the individual mobility towards shared solutions. According to a study published by Roland Berger [1], the amount of the worldwide driven kilometers with privately and commercially owned vehicles will be reduced by approximately 28% in 2030 compared to 2015. In the same period, it is expected that the amount of kilometers driven by Robo-Taxi will increase to approximately 27% [1].

Motivated by the ongoing urbanization megatrend, a vision for future urban mobility can be derived from the main problems like space scarcity, congestion, vehicle emissions and road safety, which most major cities have in common. Urban transportation planning shifts the priority from maintaining free flowing traffic towards facilitating access to destinations. For enabling this shift, the automotive industry is currently working on new technologies following the three main trends for electrification, driving automation and connectivity. The advantages of using these new technologies are very promising. In urban areas for example, the road congestion might be reduced and the air quality as well as the road safety increased. Also in rural areas, a better

public transport could be established enhancing the social aspects of the people living outside the cities. Internal analyses of the Robert Bosch GmbH regarding future mobility scenarios show that the market for Urban Automated Shuttle UAS and Urban Automated Taxi UAT will clearly rise until 2030 (Figure 1).

Automated vehicle required a new concept. New automated vehicle concepts have to fulfill complex requirements regarding reliability and availability. In addition, the load collectives will change due to the changing driving profiles. The introduction of fail-operational systems and components substitutes the driver as a mechanical fallback level. In this context Bosch develops scalable and fail-operational concepts for the use in automated vehicles, which do fulfil the increased availability and safety requirements [2].

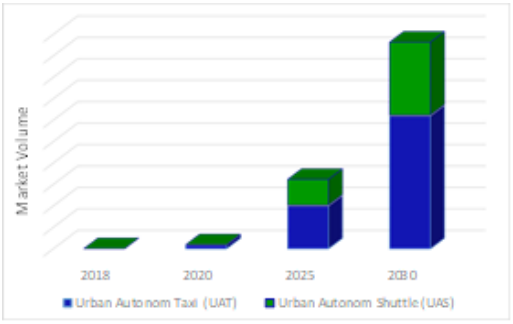


Figure 1: Market Volume Increase for UAS and UAT

Nowadays automated shuttles are already used on different university areas as well as in parks, e.g. in Dubai, Paris or Singapore. However, the operation still relies on a safety steward who is responsible to assure a safe stopping of the shuttle in the ego lane as well as to safeguard the passengers in case of a failure. To enable the shuttle operation without a safety steward and to reach the SAE automation level of 4 or 5 [5], we suppose that future systems for 2025 should be able to transit to a safe state in case of a failure on their own. For the fulfillment of these requirements, Bosch develops fail-operational powertrain solutions enabling a safe stop transition to the next safe state area. This is a more challenging design aspect compared to the state of the art powertrain systems enabling a stopping in ego lane only. In this paper, a new redundant powertrain capable to realize the transition to the next safe state area in case of a failure is proposed.

Fail-operational topologies need a certain amount of redundancy. This redundancy can be reached, for example, by the use of symmetrical topologies. However, a doubling of the complete powertrain is the most expensive solution in most cases. Instead, we target an intelligent modular system to reduce cost and weight without any performance constraints. Hence, Bosch has assessed and further developed different ideas in the broad solution range, covering (1) fail-operational powertrain topologies, (2) intelligent systems like predictive diagnosis and predictive control strategies for their control and (3) intelligent components for fail-operational e-drives and battery systems.

In this work, concepts of fail-operational powertrains for automated driving are presented and clarified by tangible examples.

2. Evolution of Powertrain/Powernet

The current Powertrain/Powernet Architectures in the market and the discussions about their future design are characterized by great diversity both on topology and component level. Main reason of this diversity are the OEM-specific specifications and drivers, which are reflected through the vehicle and Powertrain level in the Powernet architecture. Further, increasing electrification and interaction of the Powernet with the Powertrain leads to numerous requirements on the Powernets of today, (Figure 2) [3].

The roadmap of electrical Powernet from the past until today can be structured into four overlapping phases in Figure 3. In the 1960's the change from 6V to 14V electrical supply in passenger cars was largely seen. Main focus in the first phase was the optimization of components of the Powernet like belt driven 14V generator, battery and starter. In the second phase, the networking of functions and components started, e.g. load response function of the 14V generator, intelligent generator control and electrical energy management.

In phase three, as part of the Powertrain electrification, electrical subnets with different voltage levels were introduced, e.g. HEV, PHEV, BEV with high voltage subnets. Phase four of development is characterized by the increasing safety relevance of electrically powered functions. Future Automated Driving functions will have a strong impact on the Powernet architecture [3].

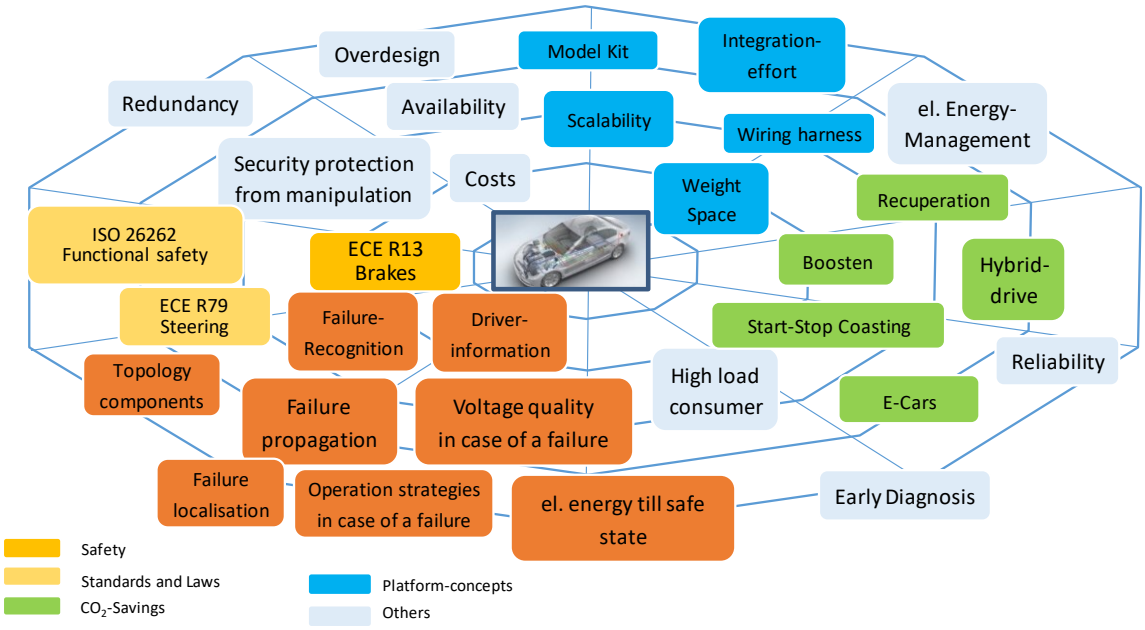


Figure 2: Demands/Requirements to Powertrain/Powernets [3]

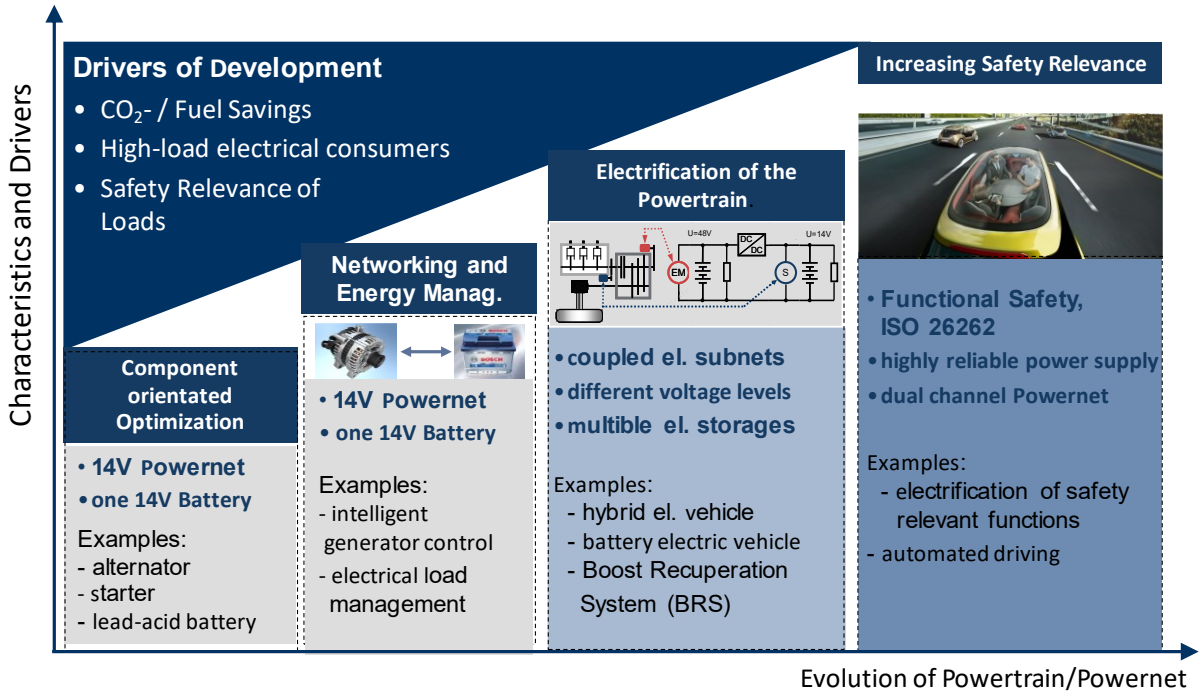


Figure 3: Development phases of Powertrain (Powernet) [3]

3. Requirements

For the development of future powertrain topologies and components, first the requirements with relevance to powertrain at vehicle level must be analysed and a representative use cycle must be defined. These inputs can then be further used for the analysis and derivation of the requirements at powertrain level [2].

3.1 Requirements at vehicle level

Our target is to define a quantified specification for a fail-operational powertrain system and the underlying components. To achieve this, the requirements at vehicle level must be analyzed first. For a systematical and structured derivation of all relevant requirements, two main sources are typically considered in automotive sector, namely (1) laws [6], standards and regulations (e.g. ECE-R, StVZO, ISO, …) and (2) voice of customer and market (e.g. OEM, individuals, cities, …) [2].

3.1.1 Legal requirements at vehicle level

From the legal perspective, two main drivers for the requirements can be identified, namely (1)

vehicle safeguarding in the case of a failure and (2) the type approval regulations. With respect to the today's driver obligation to safeguard the vehicle, its passengers and the surrounding traffic in case of a failure, a breakdown in a traffic lane (ego lane) is tolerated. Nevertheless, the vehicle should be taken out of the active traffic as soon as possible according to the UNECE Vienna Declaration. Also the current legal regulations in Germany (StVO, StVZO) require a driver to secure the vehicle and safeguard the passengers and other traffic participants in case of a vehicle breakdown. The impact of these legal requirements to the automated driving systems must be clarified. In fully automated vehicles, no person responsible for these tasks is present, since the passengers might not be trained in driving a vehicle or be aware of the traffic rules (e.g. children). Therefore, the allocation of the responsibility for safeguarding of the vehicle, passengers and surrounding traffic in case of a breakdown must be clarified [2].

3.1.2 Voice of customer and market requirements

Currently discussions considering the required location to be reached by automated vehicles in case of a failure are ongoing by customers as well as by official committees like the German "Ethics Commission on Automated Driving". We introduced a new metric of so called safe stop levels (SSL) to be able to quantify the needed performance at vehicle level, which contains the definition of the safe stop location to be reached and the functionality of the required subsystems. An overview about the seven safe stop levels is depicted in Figure 4. The main distinguishing parameter of these levels is the intended safe stop location or destination, starting with today's emergency braking (SSL G) and ending up with driving home for mission complete (SSL A). Besides the safe stop location, in Figure 4 the required functionality of the four subsystems driving, steering, braking and battery (energy) involved into vehicle motion. Also the needed energy demand to assure each level is characterized schematically. In case of SSL A (driving home) a high residual energy has to be available as well as fail-operational driving, steering and braking subsystems. For SSL G (emergency braking), only a fail-operational braking system would be sufficient to bring the vehicle to a standstill [4].

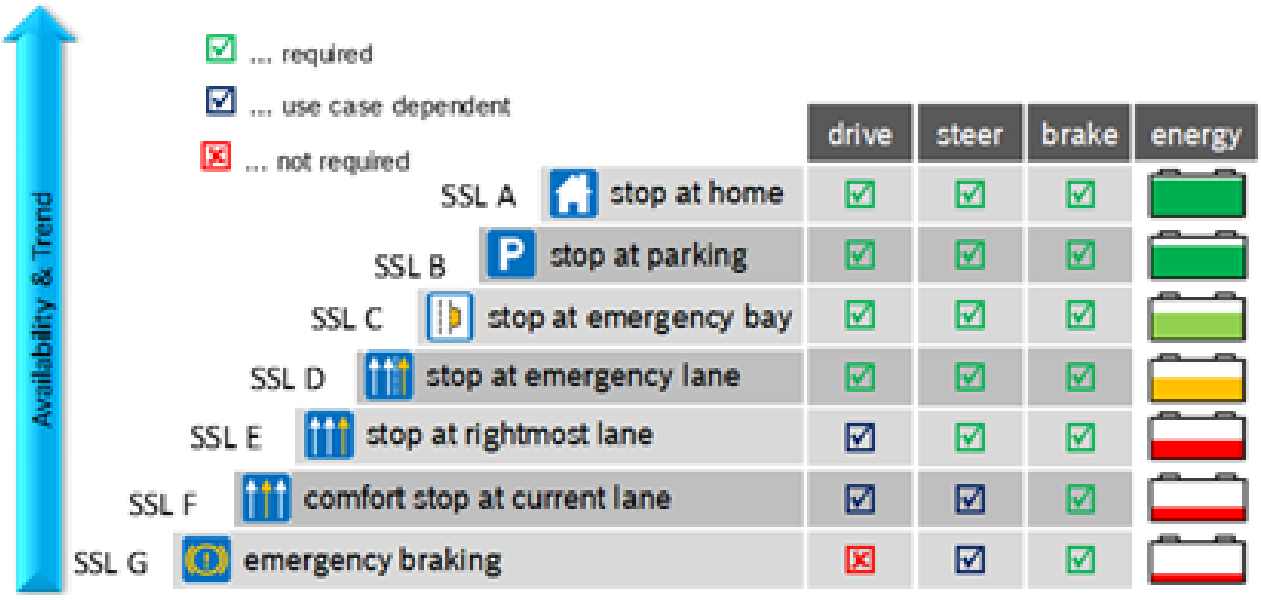


Figure 4: Metric for new safe state definition of automated vehicles using safe stop levels (SSL).

4. Design of Fail-Operational Powertrain

Target is to develop an intelligent, scalable and modular fail-operational powertrain in order to fulfill the requirements derived from the use cycles, OEMs, laws & standards as well as market demands, different approaches starting with full system redundancy to a topology with minimum cost for component redundancy can be used. Using a morphological box, two different topologies depicted in Figure 5 were developed.

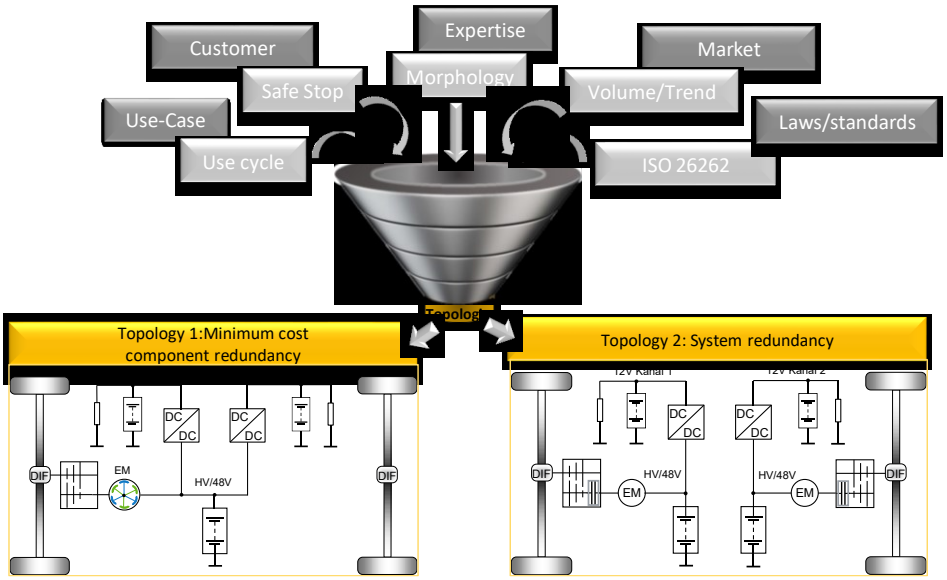


Figure 5: Topologies for fail-operational powertrain

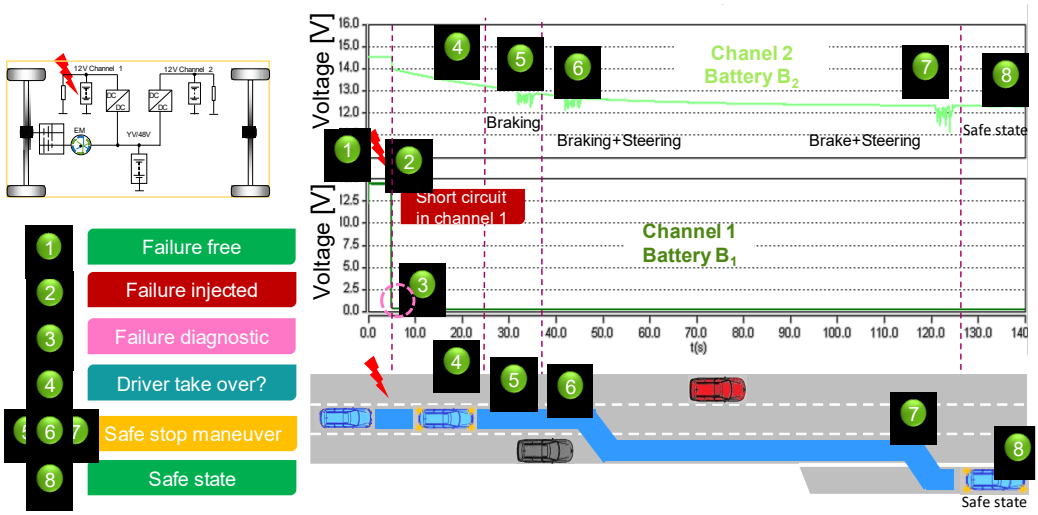


Figure 6: Failure simulation for defines topology [8]

Topology 1: One possible solution for realization of fail-operability in case of a single failure in the traction drive could be a single electric machine (EM) with internal redundancy by using a dual three-phase concept (Figure 5, topology 1). In case of a failure of one phase such an electric machine will still be able to provide the necessary torque enabling degraded vehicle motion.

Topology 2: Another approach for realization of fail-operability of propulsion function is to use a full system redundancy (Figure 5, topology 2) which can be symmetrical using equal components or diverse by using different technologies for the single components.

5. Fault Injection Simulation

The goal of the fault injection simulation is to analyses the impact of the failure classes on the power net behaviour as well as to verify the defined fault reactions. Figure 6 exemplifies the procedure of the fault injection simulation for the failure class “short circuit to ground in channel 1” [7, 8].

The simulation starts with a failure free condition (point 1). At point 2, the failure is injected into the power net and the battery voltage in channel 1 immediately drops to 0V. It is assumed that the system needs several seconds to detect this failure. After detection of the failure at point 3, the automated driving system will stop the vehicle immediately at the current lane without any driver interaction in case the failure is emergent. If the failure is not emergent, but the automated driving system still needs to be stopped, the system will request the driver to take over the vehicle control and wait for a defined period of time at point 4. If the

driver does not take over the control, the automated driving system will then complete the safe stop maneuverer (points 5, 6, 7) defined in the safety concept in the automated mode. In the example shown in figure 5, the vehicle will change the lane twice and stop automatically at the emergency lane (point 8: safe state) [8]

6. Summary

- A new mobility solution is required due to the increasing of the person and goods transportation as well as the growing of urbanization.
- Automated driving is a fast evolving technology in a fast growing, evolving market and required a new powertrain concept.
- Automated driving requires new powertrain concepts for safety-related functions and for achieving a safe state location.
- Requirements for future powertrain systems and automated driving are discussed and summarized, for example legal requirements, voice of customer and market requirements.
- New fail-operational electrical powertrain system and components for automated driving was briefly presented in this paper
- Based on the derived requirements a methodology for a systematic development of fail-operational powertrain topologies and required subsystems for automated driving are presented.
- This work presents a simulation-based method for dimensioning the powertrain topologies and components. Based on the simulation results, the reliability of the power net is quantified, the optimal dimensioning of the power net components is determined and new functional requirements are derived.

7. References

1. Roland Berger, CEO agenda for the (r)evolution of the automotive ecosystem. Roland Berger GmbH, Munich, Germany, 2016.
2. Kilic A., Fassnacht J., Shen T., Thulfaut C., "Der Antrieb von Morgen", Springer Vieweg, 221-236, 2019.
3. Augier J.-L., Huck T., Kilic A., Müller W., "Efficient, Safe and Reliable Powernet for AD, in Elektrik/Elektronik in Hybrid- und Elektrofahrzeugen und elektrisches Energiemanagement VII", Expert Verlag, 398-411, 2016.
4. Kilic A., Fassnacht J., Shen T., Thulfaut C., "Fail-operational Powertrain for Future Mobilit", MTZ - Motortechnische Zeitschrift, Ausgabe 9/2019, 66-69, 2019.
5. SAE International, J3016 SEP2016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, United States: SAE International, 2016.
6. Regelung Nr. 13-H der Wirtschaftskommission für Europa der Vereinten Nationen (UN/ECE) — Einheitliche Bedingungen für die Genehmigung von Personenkraftwagen hinsichtlich der Bremsen 2015-2364, 2015.
7. https://www.synopsys.com. Cited, 04 05 2017.
8. Shen T., Kilic A., Gorelk K., "Dimensioning of Power Net for Automated Driving", in Proceedings of EVS30 - Electric Vehicle Symposium & Exhibition, 2017.