INTERNATIONAL DESIGN CONFERENCE – DESIGN 2020
https://doi.org/10.1017/dsd.2020.31

FAULT-TOLERANT DESIGN OF A GEAR SHIFTING SYSTEM FOR AUTONOMOUS DRIVING

R. Stetter [1,✉], R. Göser [1], S. Gresser [1], M. Witczak [2] and M. Till [1]

[1] University of Applied Sciences Ravensburg-Weingarten, Germany, [2] University of Zielona Góra, Poland
✉ ralf.stetter@rwu.de

Abstract

This paper reports the application of the methods and tools of fault-tolerant design to an automated shifting system and their reflection and extension. Fault-tolerant design has emerged in the last years and is generally understood as a collection of strategies, methods, algorithms, tools and insights which are intended to support the development of technical systems which are fault-tolerant because of their controllability but also their inherent fault-tolerant design qualities. The field of application is a shifting system for the gear system of a formula student driverless race car.

Keywords: design methods, design for x (DfX), design process, fault-tolerant design

1. Introduction

In the focus of this paper are the methods and tools of fault-tolerant design. These methods and tools are applied to an automated shifting system in order to reflect and extend these methods. The ultimate aim of the strategies, methods, algorithms, tools and insights summarized under the notion fault-tolerant design (FTD) is to support engineers to develop technical systems which are fault-tolerant because of their controllability but also their inherent fault-tolerant design qualities. For complex technical systems and complex application scenarios it is impossible to avoid faults, which can be defined as unpermitted deviations of at least one characteristic property or parameter of the technical system from the acceptable, usual, standard condition (Isermann, 2006), e.g. a malfunction of an actuator. It is important to distinguish faults from failures, which are permanent interruptions of the ability of a system or a component to perform an intended function under specified operating conditions and suggest a complete breakdown of a system. If one assumes that it is nearly impossible to avoid faults then it is extremely desirable to enhance the possibilities of system to accommodate such faults, i.e. their fault-tolerance. This paper intends to present a novel contribution which will support this endeavour. This intention is realised by applying fault-tolerant design to a shifting system for the gear system of a formula student driverless race car. The paper is structured as follows: the next two sections deliver a background describing the essentials of fault-tolerant design and the formula student driverless competition. The fourth section describes the newly developed gear shifting system. Section five is the core of the contribution and describes the application of fault-tolerant design to the gear shifting system. The paper concludes with the conclusions and an outlook.

2. Fault-tolerant design

As mentioned above, a fault can be defined as unpermitted deviations of at least one characteristic property or parameter of the technical system from the acceptable, usual, standard condition (Isermann, 2006). The capability of a technical system to accommodate the consequences of such faults and to allow a safe operation in a region of slightly degraded performance can be referred to as "fault-tolerance" (compare e.g. Rouissi and Hoblos, 2012). Over the last decade, powerful algorithms, methods and tools were developed for increasing the fault-tolerance by means of elaborate control systems (Witczak, 2014, 2019, 2020; Majdzik et al., 2016; Blanke et al., 2016; Stetter et al., 2018). The approaches for fault-tolerant control (FTC) can be distinguished in passive approaches, which are characterised by the fact that the system components and controllers are designed in a manner which enables them to be robust to possible faults up to a certain degree and active approaches which are characterised by the fact that the active FTC system includes an fault detection and identification (FDI) system and the fault handling is realised based on information on faults received from this FDI system.

In the last years, the concept of FTC was accompanied by the concept of fault-tolerant design (FTD). FTD intends to support the engineering design of technical systems in order to increase their fault-tolerance. The approaches for increasing the fault-tolerance of technical systems can target their observability and their controllability, but may also aim at intensifying their inherent fault-tolerant design qualities, e.g. by means of applying robust physical effects (Stetter, 2020). The importance of FTD is also emphasised by Rouissi and Hoblos (2012) and Dubrova (2013), who connect the capability of a system to accommodate faults to the quality of the design of this system.

Until today, scientific activities concerning FTD are sparse. The existing rich body of research concerning systematic design and the strategies, methods and tools of product development (Cross, 2008; Ehrlenspiel and Meerkamm, 2013; Ponn and Lindemann, 2011; Lindemann, 2009; Pahl et al., 2007) may present an excellent basis for the development of a FTD methodology; in these research activities FTD was however usually not a point of main emphasis. Additionally, the existing research results in the areas "Design for Monitoring" (DfM; Kukurowski et al. (2019), "Design for Control" (DfC; Stetter and Simundsson, 2017) and "Design for Diagnosis" (DfD; Stetter and Phleps (2011) can expand this basis, because FTD covers these three aspects. Several research activities are directly concerned with FTD, but are usually limited to a specific field of application. Rouissi and Hoblos (2012) remark that the ability of a system to tolerate one or more fault(s) must be achieved by means of designing the technical system. Oh et al. (2013) investigated fault-tolerant design approaches for nuclear power plants; they describe fault-tolerance and fault avoidance design approaches, e.g. the 2-out-of-4 (2/4) voting logic, redundant actuation devices and requirements towards process instrumentation. Lin and Yang (2009) apply the notion "fault-tolerant design" for the reliable design of wide area mobile networks. Shirazipourazad et al. (2014) use the same notion in the area of designing wireless sensor networks; they focus on approximation algorithms for improved fault-tolerance of gathering data from directional antennas. Hsieh et al. (2017) concentrate on the design of microelectronics; they recommend "Triple Modular Redundancy" (TMR - two additional copies of an intended design are additionally integrated in the chip and a voter is used - consequently the chip may work correctly if at least two of the copies can work). Vedachalam et al. (2016) developed some elements ("reliability modelling" and "redundancy analysis") of a fault-tolerant design approach; the scope is limited to frequency converters. To conclude, some elements of a fault-tolerant design methodology were already investigated, but no generally applicable structure was presented. A model, which is based on levels of abstraction of the product models (a distinction based on the level of abstraction is frequently used in product development methodology, compare e.g. Ponn and Lindemann, 2011) was presented by Stetter (2020); this model is shown in Figure 1.

The most concrete level "geometry and material" consists of rather obvious concepts for enhancing the fault-tolerance such as redundancy. One example could be two optical sensors observing the same scene. Central insights on this level (compare Stetter, 2020) are that elaborate methods, algorithms and systems exist, which allow an optimum geometrical placement of sensors and actuators also with regard to fault-tolerance and that the fault-tolerance can be enhanced with redundant system elements. However, they may cause problems concerning the economic value and the performance and redundant elements may still fail, especially in the case of cold redundancy. Consequently, the respective redundant elements need to be consciously decided and concepts such as "over-actuation" and "overlap" also need to be considered. The well-known strategies of "Design for Safety" (DfS) such as "Safe-Life" and "Fail-Safe" may also increase the fault-tolerance; an adopted strategy "inherently fault-tolerant system configurations" may also be applied on this concrete level.

https://doi.org/10.1017/dsd.2020.31 Published online by Cambridge University Press

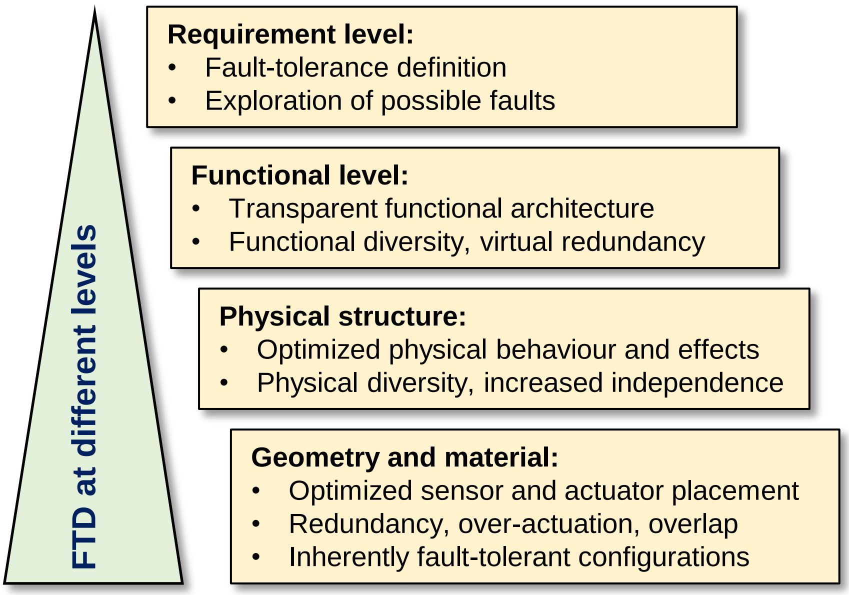

Figure 1. Fault-tolerant design on different levels

More independence can be achieved on the next higher level "physical structure". In the case of the example mentioned above, one optical sensor and another sensor relying on different physical effects, e.g. an ultrasonic sensor, can be applied and are less susceptible to certain sensor problems such as fog. Central insights on this level (compare Stetter, 2020) are that the conscious design of the physical behaviour of technical systems may be supported by the analysis of physical effects and lists with potential physical effects and that physical diversity can be identified as important means for increasing the independence of redundant system components and may consequently enhance the fault-tolerance of technical systems.

Even more independence can result from diversity on the functional level. One example would be to replace one real sensor by a virtual sensor, which works differently even in the functional domain. Central insights on this level (compare Stetter, 2020) are that an overview and understanding of the functional architecture of technical systems may be supported by function models and model-based function modelling and that functional diversity is the most elaborate form of redundancy and may increase the fault-tolerance of technical systems, if consciously applied.

A complete picture of design cannot be drawn, if the level of requirements is not considered, because requirements are a decisive factor in any industrial product development process (compare e. g. Bernard and Irlinger, 2016) and four of ten top risks in projects are connected with requirements (Hruschka, 2014). Central insights on this level (compare Stetter, 2020) are that the exploration of requirements should include the possible faults, the expected faults, the required level of fault-tolerance and the required form and amount of redundancy and that the exploration of requirements may be supported by fault tree analysis (FTA), failure mode and effects analysis (FMEA) and benchmarking as well as by model-based requirements management (compare Holder et al., 2017).

The different elements on the presented level were applied to a gear shifting system for a formula student driverless race car; this competition is characterised in the next section.

3. The formula student driverless competition

For the past 2 years, a competition for the further development of autonomous driving ("Formula Student Driverless") has taken place within the framework of the design competition "Formula Student". The team of the University of Applied Sciences Ravensburg-Weingarten was able to start with an autonomous vehicle as early as 2018. The autonomous driving vehicle even earned the first place in the category "Driverless Overall" at the "Fomula Student" competition in Spain. The driverless formula student race was initiated in order to confront students with and to educate them in the upcoming field of autonomous driving. Autonomous driving is a current topic of the future in the

https://doi.org/10.1017/dsd.2020.31 Published online by Cambridge University Press

entire automotive industry and aims at a drastic improvement of traffic safety and driving comfort, especially in high traffic density. The requirements for autonomous vehicles are enormous:

- they must recognize all aspects of the environment and also moving objects in real time,
- they have to localize themselves in the environment and record their own driving condition with position, speed and acceleration,
- they have to identify possible driving manoeuvres and driving routes,
- they have to plan suitable and safe driving manoeuvres and driving routes and
- they have to implement and monitor driving manoeuvres and driving routes.

A team can only compete in this competition, if the team members are innovative. This competition requires a high level of energy efficiency and lightweight construction, therefore innovative ideas can be very important. A performant and robust shifting system is required in order to compete in the challenging drive events. The automated gear shifting system which was developed in the last two years is described in the next section.

4. Automated shifting system

In the race car, a motor bike combustion engine with integrated sequential gear box is used (from a Honda CBR 600). The gear box is usually manually operated by means of a foot lever. For formula student driverless an automated shifting system has to be adapted to this gear box. The newly developed design was based on an earlier pneumatic shifting, which also allowed automated shifting (Figure 2)

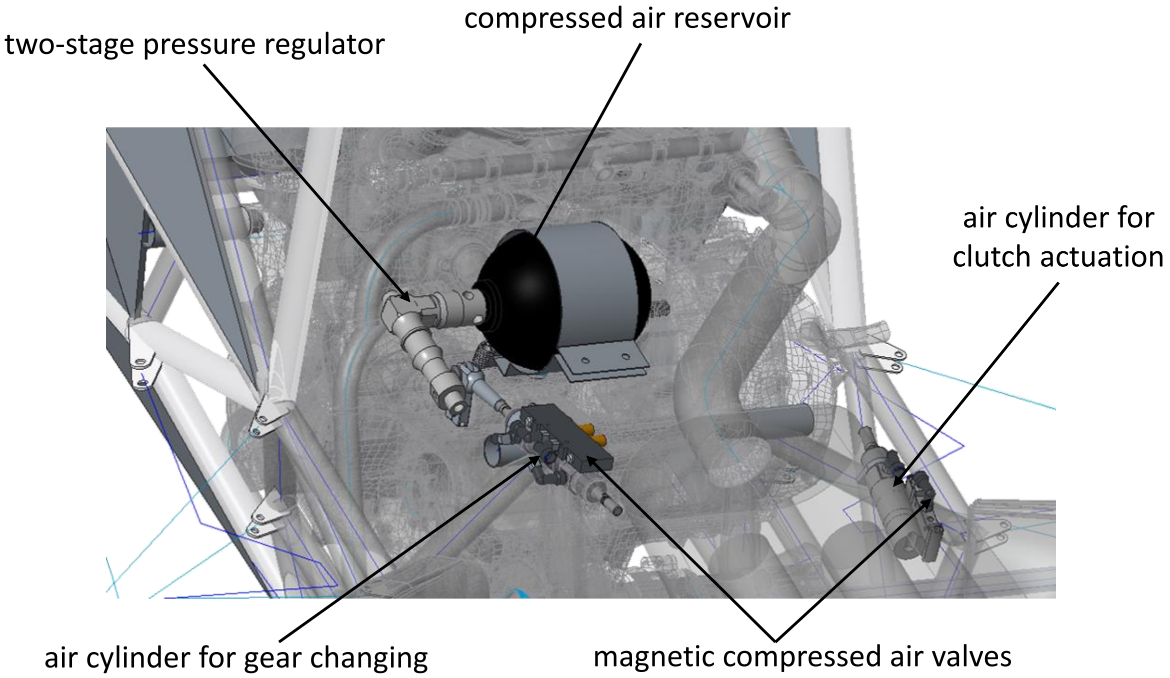

Figure 2. Prior pneumatic gear shifting system

The newly developed gear shifting system is shown in Figure 3. The pneumatic gear system consumed a lot of space, is rather heavy and is relatively slow. The pneumatic system can only achieve shifting times of approx. 300ms (the newly developed electromechanical system described in the next section is able to achieve 45ms). Due to the deficiencies concerning space, weight and speed, it was decided to develop a new, electromechanical gear shifting system. The core of this system is an electrical motor, which is equipped with an incremental encoder. After a predefined initialization run (for instance for the 1st gear a position value of 22100 inc is assigned - this corresponds to 138,7° at the gear exit and 60° at the shift drum), this encoder will obtain the exact rotary position of the motor shaft. Via a long shaft and a pair of spur gears the motion is transferred to the slightly modified shift

https://doi.org/10.1017/dsd.2020.31 Published online by Cambridge University Press

drum, which will cause a movement of sleeves, which will enable to select a gear, as usual for motor-bike gear sets. At the end of the shift drum a potentiometer is fixed which will deliver a certain analogous resistance depending of the rotary position of the shifting drum. The rationale of this design with regard to fault- tolerant design will be explained in the next section.

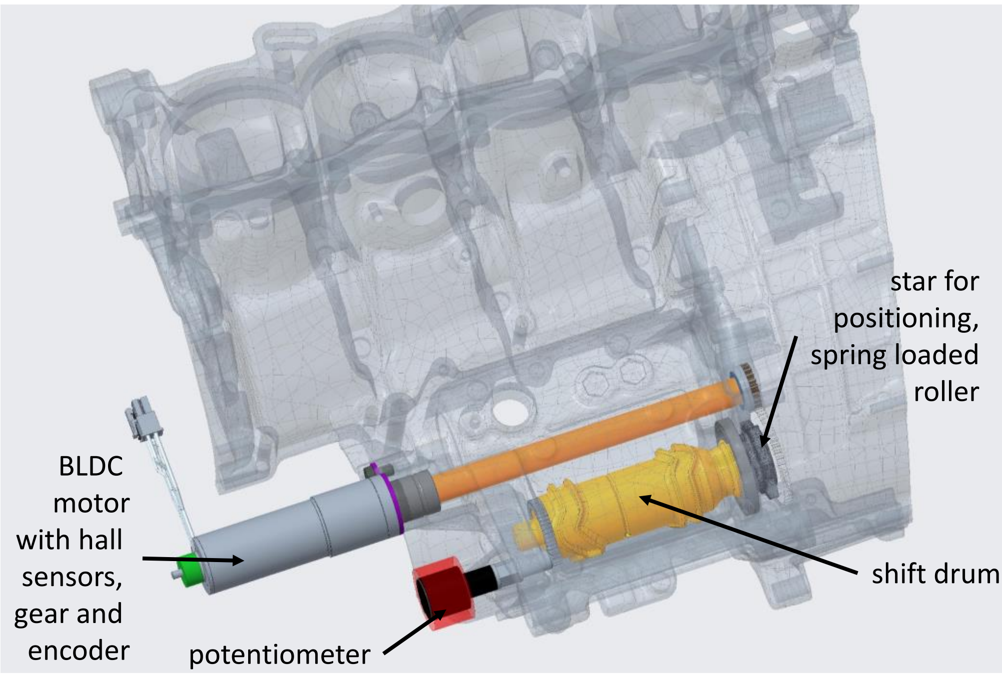

Figure 3. Newly developed electromechanical gear shifting system

5. Fault-tolerant design of the shifting system

This section explains the fault-tolerant design of the shifting system; the subsections reference to the model shown in Figure 1.

5.1. Measures on the geometrical and material level

Concepts to increase the fault-tolerance can be realized on the most concrete level "geometry and material". In the given case two instances of redundancy and the principle "over-actuation" were realised. The system is driven by an electrical motor (maxon EC-i 30 Motor with gear GP 32 C) which is controlled by an electronic position control (maxon EPOS4). This motor is also equipped with an incremental encoder (maxon ENX 16 EASY). This motor drives a shaft going to the other side of the gear system housing. At the end a spur gear is fixed which transfers the torque by means of another spur gear to the shifting drum. Close to the second spur gear, an element is fixed which is formed similar to a star. At this star, a spring loaded roller forces the shift drum to rotary positions which conform to the gears of the gear system. On the shift drum, geometrical elements as shown in Figure 6 are integrated which can move shift forks which are responsible for fixing the gear wheels for certain gear to one of the shafts. The position of the shift drum is monitored by a potentiometer.
The first example of redundancy is the use of two different sensors for the position information - an incremental encoder directly mounted at the electrical motor and a potentiometer gathering the position of the shift drum. As these two redundant sensors also rely on different physical principles, they are discussed in section 5.2. The second example of redundancy is the switching star with a spring loaded roller, which was mentioned above. This switching star assures in the motor-bike that the shift drum is kept in the optimum position for each gear. In the automated shifting system this switching star is theoretically not necessary, because the self-locking gear at the electrical motor (ratio 14:1) will by itself guarantee that a gear will be held, if it was once engaged. In testing it was found that the star is not impairing the control quality and speed and that it gives additional safety for holding a gear that was selected. Additionally, this redundant system eases the so-called "teaching" of

https://doi.org/10.1017/dsd.2020.31 Published online by Cambridge University Press

the motor positioning system, as optimum positions for each gear are guaranteed mechanically. Even more, it is possible to save electrical energy because of the switching star, because it is not necessary to energize the motor permanently.
Over-actuation can either be the usage of more actuators than necessary or the use of stronger actuators than necessary (Stetter, 2020). Over-actuated systems dispose of the advantage of an improved controllability and can enhance fault-tolerance, because the potential of over-actuation may be used to compensate the effects of faults (Stetter and Simundsson, 2017). In the given example, over-actuation could be realized in the motor itself. Measurements using a wrench for driving the shaft made clear that a torque of about 1,5 Nm is necessary in order to engage a gear safely and quickly. The applied motor with the gear system is able to achieve up to 6 Nm (for a short time, but definitely long enough for the shifting process and also for multiple shifting processes). This was found to lead to fast shifting times and to lead to a good control quality.

5.2. Measures on the physical level

In product development methodology, the analysis of physical effects is recommended for fostering a better understanding of the technical system and for developing innovative solutions, which use different physical principles (Ehrlenspiel and Meerkamm, 2013). An in-depth analysis of innovative break-through products even resulted in the insight that such products in most cases rely on different physical principles. In recent years the analysis of physical effects was expanded in order to include uncertainties in form of disturbances (Mathias et al., 2011). The analysis of elementary physical effects leads to effect chains describing the physical phenomena (Figure 4).

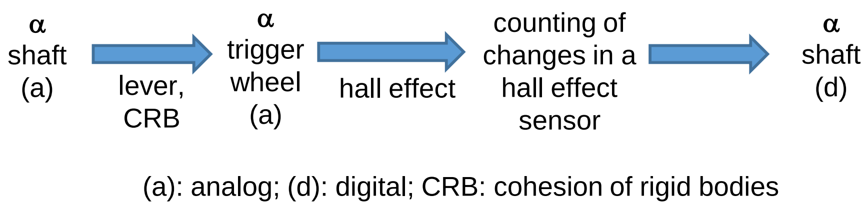

Figure 4. Physical effect chain incremental encoder

In this effect chain, the physical effects which allow the function of the incremental encoder on the motor shaft are visible. It was found that this analysis fosters a deeper understanding of the physical phenomena and eases the communication in the design team.
The most important design principle on this level concerns physical diversity. Physical diversity is the use of system elements which apply different physical effects for achieving certain goals (Stetter, 2020). For instance, airplanes achieve their high level of fault-tolerance by applying a combination of hydraulic power lines and hydraulic actuators together with electrical power lines and electrical actuators (Charrier and Kulshreshth, 2007). As mentioned above, two sensors were applied which essentially share one intention: to monitor the position of the shift drum in order to allow a position control of the motor and ensure a safe engaging of the gears. The incremental encoder at the motor shaft in combination with a gear system with transmission ratio of 14:1 allows to distinguish 57.344 positions (1024 (pulses per channel per revolution) * 4 (resolution) * 14 (gear reduction)) within the whole possible movement. Figure 5 shows the information gathered by the motor potion control unit (EPOS 4) from the incremental encoder on the motor shaft respectively from the motor control itself. The figure shows an error analysis when switching from the neutral (0 inc) to the first gear (22100 inc).
In Figure 3 it is obvious that some kind of redundancy is already given by the unit electrical motor, incremental encoder and motor position control (EPOS). The EPOS can determine a motor rotary position at certain instances of time. This determination is based on information from the encoder. Additionally, it can determine the motor velocity at certain instances of time, by means of combining information form the encoder with a numerical differentiation and information form the hall sensors of the motor (which existence also leads to another instance of redundancy). Finally, the EPOS delivers electrical current to the motor in order to trying to achieve a desired position. It is important to note that a PID control loop is realised within the motor controller.

https://doi.org/10.1017/dsd.2020.31 Published online by Cambridge University Press

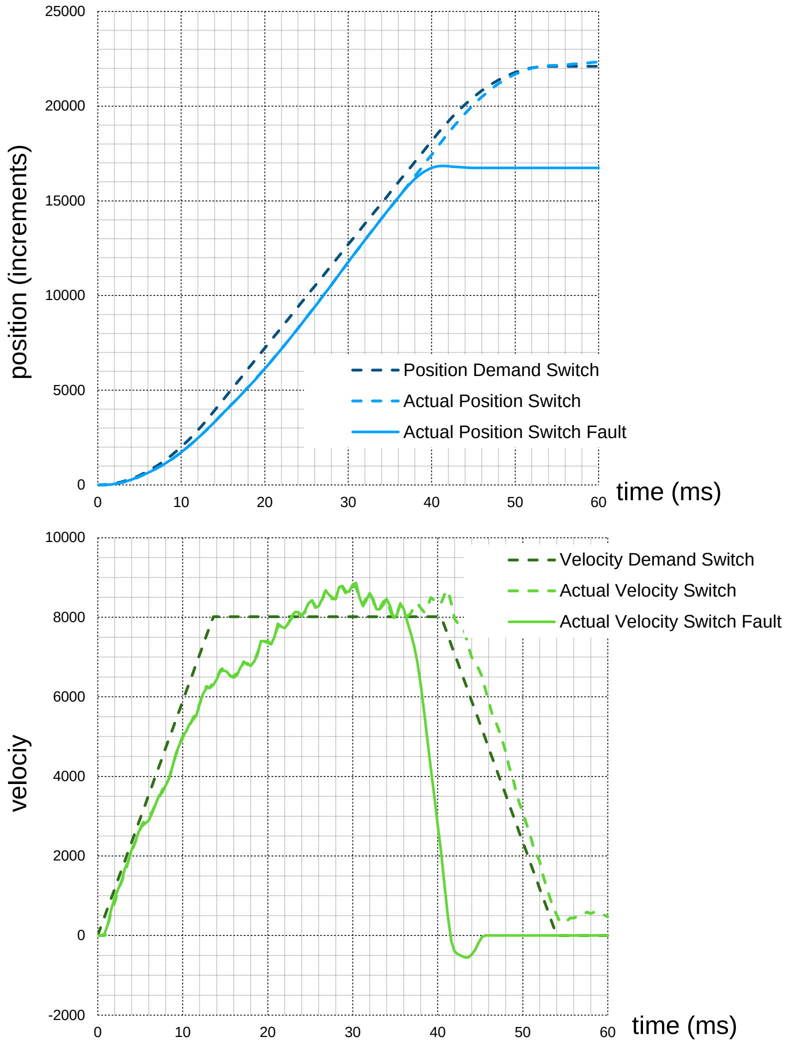

Figure 5. Position over time (top) and velocity over time (bottom)

As mentioned above, another sensor was also applied which essentially shares the intention to monitor the position of the shift drum - a potentiometer driven by the shift drum. The potentiometer will deliver an analogous resistance, which is evaluated in the superordinate control unit and not in the position control of the electrical motor. Consequently, the superordinate control may know the engaged gear, even if the electrical motor or the motor position control would be faulty. In this case, the car could continue the race in the given gear. For slow speeds, it is possible to open the clutch in order to avoid stalling the engine. It could even be possible to start the car form standstill in other gears than the first gear, if the clutch characteristic is adapted, because in the race courses there are only small inclinations. In the formula student competition it is extremely important to finish a course even in the case of a fault, because for early retirement no points at all are awarded (did not finish (DNF)). Consequently, in this example an increased fault-tolerance by means of conscious design can lead to enormous advantages in the competition.

5.3. Measures on the functional level

Figure 6 shows a part of function model of the gear shifting system. This model is based on the integrated function modelling framework (IFM), which has received increasing attention in the last years (compare Eisenbart et al., 2016; Ramsaier et al., 2017; Elwert et al., 2019). Here only the state view is shown (upper left part of an IFM model). It is obvious, that some of the fault-tolerant qualities of the developed design are visible in the function model, such as the redundancy between encoder and potentiometer. Also, the operands energy and signal are clearly visible in this model.

https://doi.org/10.1017/dsd.2020.31 Published online by Cambridge University Press

position control	el. motor	shaft and gear pair	shifting drum	encoder	potentiometer	energy	signal	
receives signal from encoder	initial position	initial position	initial position; sleeve unmoved	initial position motor	resistance of position bef.	at input positon control	initial position motor	*initial state*
P1				condition for P1		P1	P1	*process*
control enabled	initial position	initial position		position motor aft.		at input el. motor	position motor aft.	*state*
	P2					P2		*process*
	regulated postion	initial position				at input shaft and gear pair		*state*
		P3				P3		*process*
		regulated postion			resistance of position bef.	at input shifting drum	initial position drum	*state*
			P4		process state of P4	P4	P4	*process*
control enabled	regulated postion	regulated postion	regulated postion; sleeve moved	position motor aft.	resistance of position aft.	moving sleeve	position drum aft.	*final state*
Actors						*Operands*		

Figure 6. Part of a IFM model of the gear shifting system (state view)

The fault-tolerant design aspects on the functional level focus on the fault "tooth-on-tooth". Figure 7 shows the information from the motor position control which can be used together with a rather simple theoretical model (virtual sensor) in order to detect this fault and to define countermeasures.

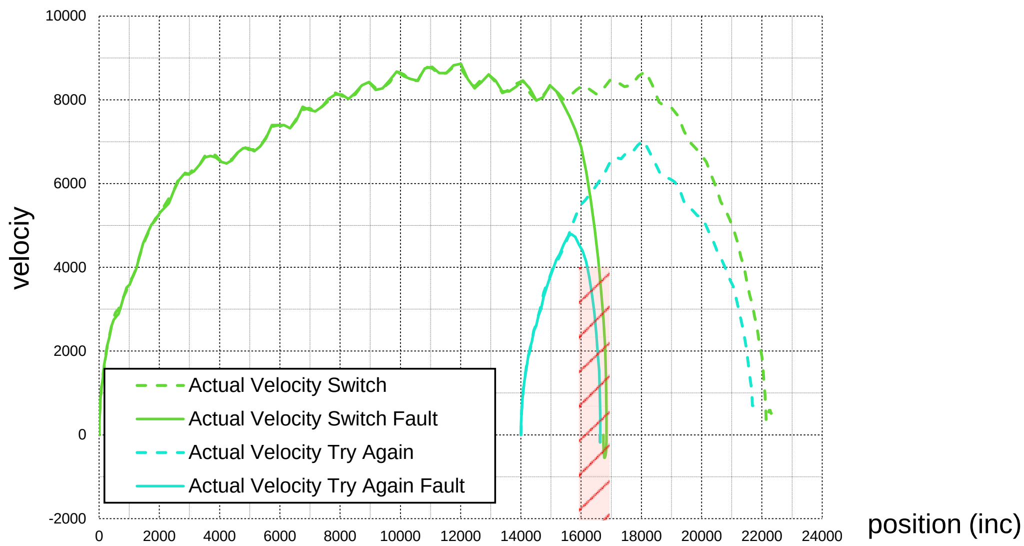

Figure 7. Velocity over position

The most common fault of the shifting system is a so-called "tooth-on-tooth" situation; in this kind of situation the gear cannot be applied, because two side surfaces of the switching toothing are just opposite to each other and hinder a sideward movement of the shift forks which would engage the switching toothing. It is obvious that this fault can be detected, if the velocity over position reaches a certain region (shown in red hatched in Figure 7). This zone can be understood as the fault signature of the fault "tooth-on-tooth". If the second kind of available information is present, which is the current over position, it is rather sure that the respective fault is present.

The first measure of fault-tolerance is to move the electrical motor just a bit in the opposite direction and then to try again to engage the switching toothing. In most of the cases, this new approach will be enough to be able to allow the complete movement of the sleeve and to engage the gear. In this case only 10 to 20 microseconds are lost. Additionally, if a faulty shifting is detected, the superordinate system can slightly attach the clutch in order to realize a small rotation in order to generate a non "tooth-on-tooth" situation.

Additionally, the developed fault-tolerant design can also lead to an improved performance of the whole race car in term of real shifting times (also including the time the engine needs to be able to deliver again the full power after the ignition cut-off during switching). Through the combined position, and current detection, it is possible to be sure that a gear will be engaged, even before the final position is reached. In this case the superordinate control can already reconnect the ignition and

https://doi.org/10.1017/dsd.2020.31 Published online by Cambridge University Press

increase the petrol injection quantity of the engine. In this case the so-called gear-cut control for shifting is overruled, i.e. the combustion motor acceleration is initiated even before the final position of the shift drum is sensed.

6. Conclusions and outlook

In this paper, the application of the methods and tools of fault-tolerant design to an automated shifting system for a formula student race car was described. On the three different levels of abstraction "geometry and material", "physical structure" and "functional level" concrete measures were explained in detail, which are intended to improve the fault-tolerance of this system. Additionally, some measures also contributed to an increase of the overall performance of the superordinate system - the race car. It is important to point out that the intelligent measures only lead to the addition of one element (a potentiometer) and did not cause excessive consequences in terms of space, weight and money. Most of the examples are possible by a combination of an intelligent mechanical and electromechanical design together with elaborate diagnosis and control systems. In the age of ubiquitous computing, one can expect that the possibilities for fault-tolerant design (FTD) and fault-tolerant control (FTC) will be further increasing in the near future. A positive influence from the application of the methods and tools of product development methodology such as integrated function modelling and a conscious analysis of physical effects could be observed. It is obvious from the example, that FTD is able to support engineers to develop technical systems which are fault-tolerant because of their controllability but also their inherent fault-tolerant design qualities. Obvious is as well that a large potential to increase the fault-tolerance of technical systems stems from a combination of FTD and FTC. It is important to point out that the experience in the presented project indicated a lack of guidance in current literature. The existing knowledge base concerning fault-tolerant design is still incomplete. The presented research aimed at contributing to the expansion of this knowledge base. One future aim is the development of further guidelines and tools, which will help designers to synthesize fault-tolerant products. In addition it was found that a conclusive metric for assessing the fault-tolerance of technical systems is not yet existing. The development of this kind of metric is an important part of the intended future research activities. Additionally, further research is planned which will expand FTD and will concentrate on technical systems with different sets of requirements, application scenarios and levels of complexity.

Acknowledgement

The work was partially supported by the National Science Centre, Poland under Grant: UMO-2017/27/B/ST7/00620 and in the scope of the project "digital product life-cycle (ZaFH)" which is supported by a grant from the European Regional Development Fund and the Ministry of Science, Research and the Arts of Baden-Württemberg, Germany (www.rwb-efre.baden-wuerttemberg.de).

References

Bernard, R. and Irlinger, R. (2016), "About watches and cars: winning R&D strategies in two branches", *Presentation at the International Symposium Engineering Design – The Art of Building Networks*; Garching, April 4th.

Blanke, M. et al. (2016), *Diagnosis and Fault-Tolerant Control*, Springer. https://doi.org/10.1007/978-3-662-47943-8

Charrier, J.-J. and Kulshreshtha, A. (2007), "An electric actuation for flight and engine control system: Evolution, current trends and future challenges". In: *Proceedings of the 45th AIAA Aerospace Sciences M. & Exhibit*. https://doi.org/10.2514/6.2007-1391

Cross, N. (2008), *Engineering Design Methods: Strategies for Product Design*. John Wiley and Sons Ltd.

Dubrova, E. (2013), *Fault-Tolerant Design*, Springer. https://doi.org/10.1007/978-1-4614-2113-9

Ehrlenspiel, K. and Meerkamm, H. (2013), "Integrierte Produktentwicklung", Denkabläufe, Methodeneinsatz, Zusammenarbeit. Carl Hanser. https://doi.org/10.3139/9783446436275

Eisenbart, B. et al. (2016), "A DSM-based Framework for Integrated Function Modeling: Concept, Application and Evaluation", *Research in Engineering Design*, Vol. 28 No. 1, pp. 25-51. https://doi.org/10.1007/s00163-016-0228-1

Elwert, M. et al. (2019), "Holistic Digital Function Modelling with Graph-Based Design Languages", In: *Proceedings of the Design Society: International Conference on Engineering Design*, Vol. 1 No. 1, Cambridge University Press, pp. 1523-1532. https://doi.org/10.1017/dsi.2019.158

Holder, K. et al. (2017), "Model-Based Requirements Management in Gear Systems Design Based On Graph-Based Design Languages", In: *Applied Sciences*. Vol. 7, p. 1112. https://doi.org/10.3390/app7111112

Hruschka, P. (2014), *Business Analysis und Requirements Engineering: Produkte und Prozesse nachhaltig verbessern*. Hanser, https://doi.org/10.3139/9783446438620

Hsieh, T.-Y., Li, K.-H. and Chung C.-C. (2017), "A fault-analysis oriented re-design and cost-effectiveness evaluation methodology for error tolerant applications", *Microelectronics Journal*, Vol. 66, pp. 48-57, https://doi.org/10.1016/j.mejo.2017.05.018

Isermann, R. (2006), "Fault Diagnosis Systems". *An Introduction from Fault Detection to Fault Tolerance*. Springer-Verlag, New York. https://doi.org/10.1007/3-540-30368-5

Kukurowski, N., Stetter, R. and Witczak, M. (2019), "Design for Monitoring of a Research Vehicle", In: *Proceedings of the Design Society: International Conference on Engineering Design*, Vol. 1 No. 1, Cambridge University Press, pp. 1523-1532. https://doi.org/10.1017/dsi.2019.290

Lin J.-W. and Yang, M.-F. (2009) "Fault-tolerant design for wide-area mobile ipv6-networks", *The Journal of Systems and Software*, Vol. 82, pp.1434-1446. https://doi.org/10.1016/j.jss.2008.07.021

Lindemann, U. (2009), *Methodische Entwicklung technischer Produkte*, Springer. https://doi.org/10.1007/978-3-642-01423-9

Majdzik, P. et al. (2016), "A fault-tolerant approach to the control of a battery assembly system", *Control Engineering Practice*, Vol. 55, pp. 139-148. https://doi.org/10.1016/j.conengprac.2016.07.001

Mathias, J. et al. (2011), "Selection of Physical Effects Based on Disturbances and Robustness Ratios in the Early Phases of Robust Design", In: *Proccedings of the International Conference on Engineering Design*, Iced11, Technical University of Denmark.

Oh, Y.G. et al. (2013), "Fault-tolerant design for advanced diverse protection system", *Nuclear Engineering and Technology*, Vol. 45 No. 6, pp.795-802. https://doi.org/10.5516/net.02.2013.526

Pahl, G. et al. (2007) *Engineering Design: a Systematic Approach*. Springer. https://doi.org/10.1007/978-1-84628-319-2

Ponn, J. and Lindemann, U. (2011), "Konzeptentwicklung und Gestaltung technischer Produkte", Springer. https://doi.org/10.1007/978-3-540-68563-0

Ramsaier, M. et al. (2017), "Digital representation of product functions in multicopter design", In: Maier, A. et al.: *Proceedings of the 21st International Conference on Engineering Design (ICED 17) Vol 1: Resource Sensitive Design, Design Research Applications and Case Studies*, Vancouver, Canada, 21-25.08.2017, pp. 369-378. https://doi.org/10.1016/j.procir.2016.06.008

Rouissi, F. and Hoblos, G. (2012), "Fault tolerant sensor network design with respect to diagnosability properties". In: *Proceedings of the 8th IFAC Symposium on Fault Detection*, Supervision and Safety of Technical Processes (SAFEPROCESS), pp. 1120-1124. https://doi.org/10.3182/20120829-3-mx-2028.00067

Shirazipourazad, S., Sen, A. and Bandyopadhyay, S. (2014), "Fault-tolerant design of wireless sensor networks with directional antennas", *Pervasive and Mobile Computing*, Vol. 13, pp. 258-271. https://doi.org/10.1016/j.pmcj.2014.03.004

Stetter, R. (2020), "Fault-Tolerant Design and Control of Automated Vehicles and Processes", *Insights for the Synthesis of Intelligent Systems*. Springer. https://doi.org/10.1007/978-3-030-12846-3

Stetter, R. and Phleps, U. (2011), "Design for diagnosis". In: *Proceedings of the 18th International Conference on Engineering Design (ICED 11)*, Vol. 5, pp. 91-102.

Stetter, R. and Simundsson, A. (2017), "Systematic Product Development of Control and Diagnosis Functionalities", In: *Proceedings of the 21st International Conference on Engineering Design (ICED 17) Vol. 4: Design Methods and Tools*, pp 149-158. https://doi.org/10.1088/1742-6596/783/1/012063

Stetter, R., Witczak, M. and Pazera, M. (2018), "Virtual Diagnostic Sensors Design for an Automated Guided Vehicle", *Applied Sciences*, Vol. 8 No. 5, p. 702. https://doi.org/10.3390/app8050702

Vedachalam, N., Umapathy, A. and Ramadass, G.A. (2016), "Fault-tolerant design approach for reliable offshore multi-megawatt variable frequency converters", *Journal of Ocean Engineering and Science*, Vol. 1, pp. 226-237. https://doi.org/10.1016/j.joes.2016.06.001

Witczak, M. (2014), "Fault Diagnosis and Fault-Tolerant Control Strategies for Non-Linear Systems", *Analytical and Soft Computing Approaches*. Springer. https://doi.org/10.1007/978-3-319-03014-2

Witczak, M. et al. (2019), "Interval max-plus fault-tolerant control under resource conflicts and redundancies: application to the seat assembly", *International Journal of Control*, pp. 1-13. https://doi.org/10.1080/00207179.2019.1630749

Witczak, M. et al. (2020), "A Fault-Tolerant Control Strategy for Multiple Automated Guided Vehicles", *Accepted for publication in the International Journal of Manufacturing Systems*.