# Unambiguous and Reliable Positioning in the vehicle in terms of Functional Safety and Cyber Security

*Ossmane Krini and Edgar Laile*

University of Lörrach, DHBW Lörrach, Germany
Department of Electrical Engineering, Functional Safety and Cyber Securtiy

**ABSTRACT:** Functional security and agile software development are two modern areas in product development, which initially have very opposite approaches. For example, formal tests are required by the relevant standards for the former, which must be documented very extensively. The agile software development, on the other hand, tries to come to its conclusion with as few documentation and flexible tests as possible. Also, the proof that testing and development are independent of each other for safety-critical projects is difficult in the context of the use of agile methods. However, taking the constraints of functional safety as given and taking advantage of the enormous flexibility of agile software development, e.g. With the use of Scrum, the Daily Team Meetings create new opportunities in product development. In contrast to previous positioning methods for linearly movable axles, a new developed approach for rear axle steering has not been used as an absolute value encoder, but a novel positioning concept has been researched and developed. Functional Safety first! A new safety concept must therefore be developed. The absolute value encoder, usually realized as an optical or magnetic bar-coded sensor, is used reliably but cost-effectively in a large number of systems. In order to save costs as well as space, the development of the new approach to the sensor will be dispensed with and the positioning will be realized via a new concept. The conventional concepts for position determination of axes is an absolute value encoder. However, this is not highly reliable and has no redundancy. With the new safety concept, the exact position of an axis can be determined and output with high accuracy by means of the various safety devices directly after switching on the system. As a result, the sensor system is hardly susceptible to errors. Here, a detailed error analysis has been carried out. Even after system crashes, there are enough detection points, which are constantly detected during normal operation and thus the plausibility check can be restored. The new explored approach allows the steering to work normally even in safe modes. However, the algorithms for protection have to take effect immediately if, for example, an expected index signal does not occur.

## 1 Introduction

### 1.1 Type area

Functional safety as well as cybersecurity have a great demand on the new concept. The main factors are determined by the following factors:

- Reliability terminal 30 (battery current)
- Reliability of non-volatile memory
- Gear slip
- Self-locking of the harness thread

However, the point of reliability terminal 30 also depends on the quality of the implemented memory algorithm since the reliability is only a minor factor due to an intelligent concept of position storage and restoration. Nevertheless, it is necessary to consider how frequently a voltage drop at terminal 30 can occur and what has the consequences for the Electronic Control Unit (ECU). Especially during the development period with an emergency stop in the test vehicle a frequent change of clamps can take place. Therefore, it must be ensured that the steering system is not subsequently initialized incorrectly, as otherwise, unexpected changes in the vehicle dynamics may occur.
The intention of this scientific paper is to introduce this new approach to the implementation of a specific functionality into an only partly existing software of an embedded control unit of an active rear axle steering. The sensor concept is a redevelopment for application of the different automobile manufacturers, and therefore must meet extensive, safety-related requirements. The implementation means using of an Index Sensor which should be used for location of the actuator. The sensor has to be implemented into the software so that values can be used safe and reliable for location.

Up to now, the main utility of concepts with rear axle steering is the controllability of large vehicles. As different models of automobile manufacturers are becoming more and heavier and longer, the agility is consequently getting worse. Nevertheless, to allow a good driving experience in situation with little scope, it is important that rear axle assists the steering process. However, the previous steering interventions are in the low single-digit range so that only minor corrections are possible.

The planned developments for different manufacturers include rear axles steering with double-digit setting angle for the future. This means that systems have to be further developed, particularly in terms of haptic, performance and security / reliability.
Besides, there must be a stronger focus on safety-relevant issues. Because of the high setting angle many other topics, which were not relevant by smaller setting angle, will become increasingly important now.

# 2 state of technology

## 2.1 Basics

By cars with only front axles steering, it is normal to use so-called one-track model for driving dynamics. This system is simple to simulate and fast comprehensibly. However, the system is not any longer to calculate reliable data of movement of the vehicle. It is necessary to develop more elaborate models.

Besides, the development of chassis and vehicle dynamics control is more complex and less transparency. Especially for luxury category, it is important to ensure a stable driving in all situation and in every possible rear axle position without any compromises. In order to meet requirements, it is important to calculate exactly the effects on rear axle steering.

The current state of technology based on products currently being used by different automobile manufacturers. At the end of the 20th century, the promoted main development is an all-wheel steering for private vehicles which caused certain products and methods. The construction methods involved can be separate in following three categories:

- Mechanical rear axle steering
- Hydraulic rear axle steering
- Electromechanical rear axle steering

Besides, there is a difference between centralized actuator and decentralized actuator (one at each wheel), because hydraulic or electromechanical systems are flexible in require flexible on the assembly line.

There is the option to install a big centralized actuator on the rear axle for both wheels or to install the actuator on two smaller places, closed to the wheel but with less power.

## 2.2 Mechanical actuator

Mechanical actuators were the basic for the first approaches of all-wheel steering. With the help of a gear, the movement was shift from the front steering axle to the rear axle. The power assistance of the front axle is thus also pressing the steering of the rear axle.

So, a second actuator is not required. In regards to used steering assistance via hydraulic, this technology was very workable approach. Besides, it could be achieved a practicable steering through a revolutionary construction. With a reverse rotation of a planetary gear, it was possible to achieve a distinction of steering angle.

For example, the Honda Prelude (1987) is able to differentiate between small and large steering angles. By smaller angles at the front axle, the rear axle steering moves minimal in the same direction, while in the case of larger steering angles the rare axle takes in the opposite direction, see figure 1. So, the maximum steering angle of the rare wheels of 5.3° can be achieved by steering angle of 450° in the different direction.

A disadvantage of this mechanical solution is that the independence of speed. If, despite high speed, a large steering wheel angle must be adjusted, an extremely dangerous yawing moment can arise because of the opposite movement of the rear wheels.

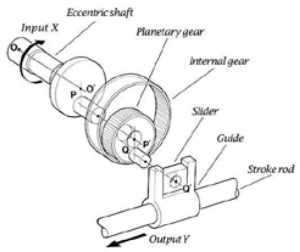


Figure 1. Illustration of the mechanical rear axle actuator

A disadvantage of this mechanical solution is that the independence of speed. If, despite high speed, a large steering wheel angle must be adjusted, an extremely dangerous yawing moment can arise because of the opposite movement of the rear wheels.

## 2.3 Hydraulic motor controller

Hydraulic motor controller based on pressure differences in one cylinder to affect to adjusting axis for one moment. The system consists of the cylinder, one-cylinder control in the form of one or more other valves and one pumps for the used liquid. The advantage of the used oil is that it has no high viscosity and so the containers are easier to seal up by high pressure ratios. Besides, all mechanical components are permanently lubricated. Consequently, there is a lower wear of all components. The hydraulic steering system gets robust in this way and it never loses its power, provided the oil circulation works.

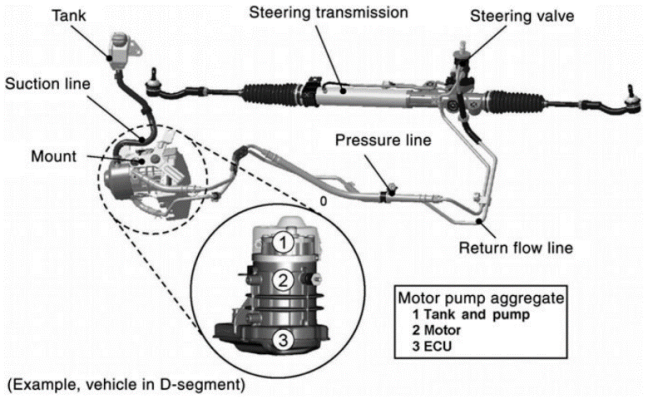


Figure 2. Representation of components of hydraulic steering

In figure 2 the components are marked individually. The power transmission takes places in the marked “Steering transmission” cylinder. Depending on rotation angle of the steering wheel, the steering valve is so twisted that the oil flow is directed in one part of the cylinder. Consequently, the pressure increases in this part and an additional moment supports this steering movement of the driver.

This principle works also as only electronically controlled system. Thereby, an “Electronic Control Unit” (ECU) controls the valve and so it creates an ideal motion of the steering axle.

### 2.4 Electro mechanics motor controller

The motor controller for prototype is an electro mechanic system of the current generation of EPS steering systems which is adjusted to give of a rear axle steering. This system is able to move the steering axle without any complex mechanic or hydraulic.

It uses a simple engine and a power transmission in linear direction. The activation of the described engine happens about a standard value in degree which is sent via the vehicle bus to the electronic control unit of the motor controller.

The angle set value is a specialty of the rear axle steering, because a moment is normally awarded by an Electronic Power Steering (EPS). This moment serve the servo support and is calculated at the handlebar with the help of a torque sensor. In order to prevent a servo support during the rear axle steering, but to have an autonomous steering movement, it takes place an absolute position setting.

Figure 3. Representation of a steering

The used control unit have a processor with the implemented software for implementation of the activation as well as various other factors. Besides, it includes the full power electronics for the engine and diverse analogue and digital inputs for I/O tasks in the ECU. The analysis of sensors as well as the power supply of all active components of the steering system are managed within the ECU, see figure 3.

The power transmission takes place in a thread which transfer rotation of the motor in a linear movement of the steering axis. This thread can be implemented by different methods.

## 3 New development of a safety-oriented sensor concepts

### 3.1 Concept in terms of functional safety

In the scope of new development of rear axle steering, a safety-oriented sensor concept will be rethought and developed. The necessity results from a cost and competitive advantage. Possible competitors can be outcompeted via price advantage. Besides, the savings by the new sensor concept can be used to improve the performance and haptic of the motor controller so that it is also possible to achieve highly dynamic large angles by heavy axles.

The conventional sensor concepts with linear sensors will be replaced through new and safety-oriented index sensor concepts. The ranking algorithms is only concentrated on the values of the rotor position sensor and on the further processing of these values taking account of the gear coefficient.

A new concept must be developed for initialization of the position, recovery after loss and ensuring the reliability. On the one hand, the challenge is the functional safety and calibration of the position on the other hand.

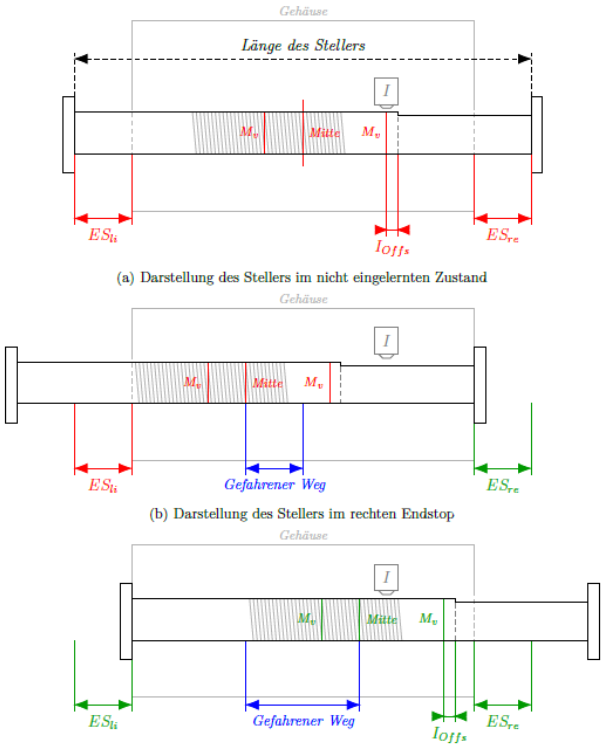


Figure 4. Views of the actuator during initialization

Figure 4 shows the starting position after first start of the control device. To simplify the graphic, the motor controller is shown in the exact center position (unlikely in reality).

For the algorithm, the starting position is not relevant because movement during the initialization is calculated relatively in regard to the starting position. This is necessary, because there are no values about positioning.

In the described starting position, the index sensor is active, because in this case the offset to the middle is negative. This means that the index edge is on the x-axis and is shifted to the right relatively to position of sensor by the distance IOffs.

If the algorithm has to work as quickly as possible but also has to required certain safety levels, then the driving direction has to be selected accordingly value of index sensor.

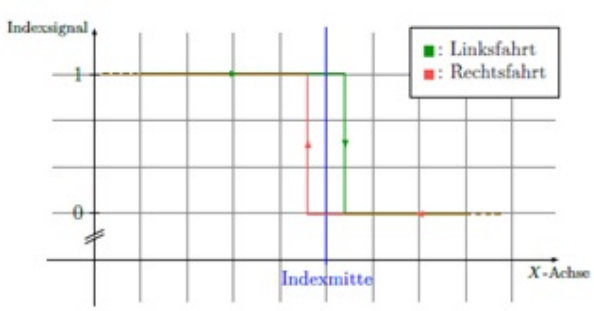


Figure 5. Index sensor flanks on crossing

As you can see in figure 5, the senor is above the left part of the handlebar by active sensor signal. To ensure to have an index signal previous to the end stop and to ensure the plausibility of the measurement, it is compulsory that the algorithm drives leftwards.

This enables the recording of the index edge and determination of first reference to actual position. So, it can be prevented an uncontrolled driving in the direction of the end stop.

### 3.2 Possible problems and restrictions

By various mechanical qualities of the system, it could be possible that their problems in the execution of the automatically calibration. Unusual mechanical resistors can occur in using the method for recognition of end stops and would lead to measurement errors.

Therefore, concepts, restrictions or error detection has to be evolved which identify these problems and if possible solve these problems. Throughout the self-locking trapezoidal thread as power-transmitting link in the motor controller it has to be consider the mechanical blockade by the adjusting axis so that the so-called effect of screws substance can be caused an establishment of the engine by to high mechanical torques.

If the axis is mechanically blocked and the engine is simultaneously able to drive the thread with a further relative high torque, it can be possible that the thread anchored itself and can only be resolved with a lot of effort. If this required effort is larger as the maximum torque that can be applied by the engine, the motor controller has to repeat by hand. Therefore, the recognition of the end stops and the speed by which is driven in direction of the end stop has to be exactly determined and reviewed.

In case of limited controller adjustment, a mechanical blockade can be possible by fast acceleration or suddenly stopping. A completely determination of the system is unrealistic.

However, smaller blockades could lead to high power consumption and some high mechanical constraints. There are acoustical and haptical consequences which is why acceleration and braking techniques with special functions have to be evolved to enable a gentle modification of acceleration. If the functionality is tested outside the laboratory conditions, first the new conditions for measurement has to be perform to establish the current limit for identification of the end stops.

In the case of calibration of steering in the vehicle, this has to be performed under previously exactly determined conditions.

Throughout tire pressure, tire marking and soil condition the variation of the engine torque and closely linked motor current happen. Even on a jack in a workshop it is possible that different environmental conditions as large wheels can slightly change the streamlines of the motor. This can be caused inaccurate values or as the dangers already listed.

### 3.3 Reaction by error detection

A case of failure must be assumed if the identified index edges are not a part of the calculated rack position or do not fit with stored motor angle or index edges cannot be detected by the expected position.

In those cases, the necessary corrections could be:

- A downtime in the completely EOL procedure or in the workshop,
- A reduced training time procedure during the drive or at a downtime or,
- A new calculation of the positions and an evaluation and correction of the caused tilted position under consideration of the newly identified index edges and the old value for index offset

For the first two variants, the driver must get a warning by infotainment system. This warning includes an announcement about the following autonomous movement of steering system or must demand a service visit in the next workshop.

These warnings integrate in the comfort of the driver and is only acceptable in an emergency case. The second variant can be happened while driving because it does not disturb the driver because an adaptive teach-on algorithm is used. From the current position, it should be continue to implement the parking request. Of vehicle with reduced speed.

By recognition of an end stop or index edge, these factors are to be registered as by complete calibration. As soon as both end stops are achieved by normal steering requirements, the system should be completely programmed.

It is doubtful whether this state can be achieved by a normal driving situation within a foreseeable time period. Therefore, this method is not safe and reliable. If possible, it should be always use the third method. It is not possible to resolve mechanical defects but a shifting of index edges have rarely serious mechanical defects as a causal factor.

An electronic sensor error or a strap leap is more likely. Throughout the EOL invited indexoffset, it can be calculated and corrected, via the determined indexoffset, the tilted position.

Is the stored value e.g. around +90° motor angle and a new offset around +20° could be measured by the index middle, the motor can be moved to achieve the center. A decision is taken on how to proceed with the new indexoffset and this has to be set in a safety concept.

The system must be verified for mechanical defects before the old system will be overwritten.

## 4 Validation and testing

Firstly, static software module tests were performed for testing the software to check the compliancy of standards as well as measurement of different assessment parameters. In safety-relevant development processes, these are compulsory components in any effective software development process. The module tests take place after implementation of individual modules. This happens after the standards of the V-module of software development after ISO 26262, which is shown in figure 6. This module is used for development process for control unit software in the automotive industry and is adjusted on respective in-house processes of producers and suppliers.

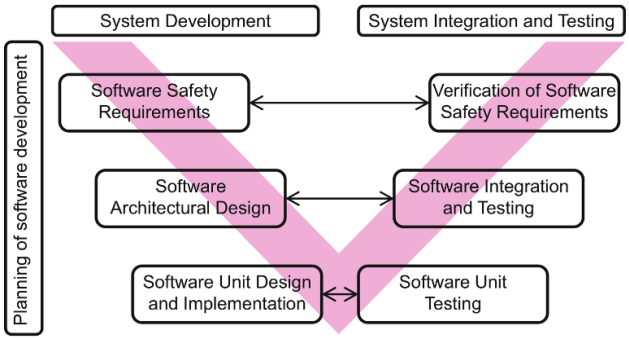


Figure 6. V-development model according to ISO 26262

For first review of the safety functionality, the program code is tested in a SiL setting. After that the function is integrated in the prototype software and will be tested on correct functionality together with remaining hardware at the laboratory space.

Before installation in a vehicle (this test is not for this functionality), further tests are required, e.g. endurance runs, exposure measurements, "measurement of clearness" in the hardware in the loop (HiL).

In the same time, module tests are made for each new software standard to ensure the best possible code quality and reliability. The so arising procedure can be described as follows:

- Addition of a new test case / adaption of new test case on the code,
- Work through module tests,
- Perhaps performance of a code adjustment to successfully complete module tests
- Again, work through module tests until tests are successfully completed,
- SiL or HiL testing of functionality in line with the development progresses and
- Adaption of the code

The software module tests are separated in different tests which have special requirements for the software and verify the code of an isolated module of these requirements. The tests are implemented by different programs and results are presented in an overview. During the tests of a special modules, is this module separated from the rest of software and is invoked by generated signals.

The developer or software tester determine these signals and has to choose realistic standards. The aim is to achieve the best possible results as well as including of intentionally faulty signals to test the reaction of software. Throughout these so-called "Regression-testing", errors can be recognized which can be caused by software changes.

For a moment, these changes may appear marginal. A regression testing can detective frequently serious mistakes that otherwise would not have been recognized. Through sorting of test signals in different test cases, it is possible to test individual modules according to special cases or requirements.

This is important because in many cases it is not necessary to do complete regression testing but merely separate test scenarios should be applied. Besides, there is a complexity reduction of the tests. Many different scenarios must be test, because of the high complexity of the software.

## 5 Summary and reflection

The development of a new safety-oriented functionality for an HAL-prototype and the development of an innovative sensor concept for the positioning of a motor controller lead to a successful result.

The redevelopment functionality for calibration for an HAL-prototype are also utilized and serves the purpose of calibration with reliability and precision. Further tests in this area are planned. The results of these tests and also further benchmarks under laboratory conditions are used to refine the functionality. Thereby, the safety requirements for this security concept are completely fulfilled. In the area of speed exists optimization work, because there are still outstanding regulator polls? The general safety-oriented functionalities are in place and are perfectly matched to the rest of the software modules, so that the automatic calibration of the motor controller can be achieved.

Besides, the renewed initializing after a clamps-30-loss uses values which are measured by automatic calibration. The development of this functionality based on several electronic and mechanical properties and was linked with a lot of research and analytical work as well as with testing of different approaches and methods.

The parallel development and elaboration of the new sensor concept can benefit from the presented results.

## REFERENCES

1. J. Misra. A Discipline of Multiprogramming: Programming Theory for Distributed Applications. Monographs in Com puter Science. Springer New York, 2001.
2. W. Oswald. Mercedes-Benz Personenwagen: 1886 - 1986. Motorbuch-Verlag, 1986.
3. C. P. Pfleeger. „State Reduction in Incompletely
4. Specified Finite-State Machines". In: IEEE Transactions on Computers C-22.12 (Dez. 1973).
5. A.Percy, I. J. Spark und M. Y. Ibrahim. „On-line determination of wheel angles and speeds for manoeuvrable gantry tractor comprising a " chorus line" of synchronized modules".
6. In: 2009 IEEE Iternational Conference on Industrial Technology. Feb. 2009, S. 1–6.
7. Miroslaw Staron und Per Johannessen. „Functional Safety of Automotive Software". In: Automotive Software Architectures: An Introduction. Cham: Springer International Publishing, 2017, S. 201–222.
8. Michel-François Rossignol und Jean-Paul Yonnet. „Permanent magnets". In: Magnetism: Materials and Applications. Hrsg. von Étienne du Trémolet de Lacheisserie, Damien Gignoux und Michel Schlenker. New York, NY: Spriger, New York.
9. René Linssen, F. Uphaus und J. Mauss. „Software-in-the-Loop at the junction of software development and drivability calibration". In: 16. Internationales Stuttgarter Symposium: Automobil- und Motorentechnik. Hrsg. von Michael Bargende, Hans-Christian Reuss und Jochen Wiedemann. Wiesbaden: Springer Fachmedien Wiesbaden.