Active Monitoring Concepts for Safety-Critical Mirror Drivers of MEMS Micro-Scanning LiDAR Systems

Philipp Stelzer, Andreas Strasser, Philip Pannagger, Christian Steger
Graz University of Technology
Graz, Austria
Email: {stelzer, strasser, steger}@tugraz.at
pannagger@student.tugraz.at

Norbert Druml
Infineon Technologies Austria AG
Graz, Austria
Email: norbert.druml@infineon.com

Abstract*—In the future, more and more cars will be equipped with Advanced Driver-Assistance Systems (ADAS) like Adaptive Cruise Control (ACC), Collision Avoidance System and many more. Currently, the driver is held responsible by law to perceive the environment and take over control if it is required. But in foreseeable future highly automated vehicles or even fully automated vehicles will appear on the road; where the vehicle is responsible for perceiving the environment, operating the vehicle and intervening in hazardous situations. By then it will be necessary that systems must not fail unnoticed. Therefore, it is mandatory to monitor safety relevant components. For instance Light Detection and Ranging (LiDAR) Systems like the 1D Micro-Electro-Mechanical System (MEMS) Micro-Scanning LiDAR, which will be part of intelligent sensor fusion in future ADAS. As a matter of course various safety monitors and safety devices are installed in highly automated vehicles to ensure an appropriately high level of safety. To further increase the safety level of the entire environmental perception system, we propose our novel Monitors for the Safety-Critical MEMS Driver of the LiDAR part in the sensor fusion unit. In this publication, we introduce novel system architectures that are able to verify the correct operation of internal control systems in MEMS-based LiDAR systems respectively to assess the reliability of the MEMS-based LiDAR in the sensor fusion unit of the entire environment perception system. To evaluate the effectiveness of our novel monitoring approaches, we implemented the procedures on a 1D MEMS Micro-Scanning LiDAR prototype platform.

Keywords–ADAS; LiDAR; Signal Monitor; 1D MEMS Mirror; Safety Monitor

I. Introduction

With fully automated driving gaining more and more attention, industry and academia put a lot of effort into research in the field of sensor fusion and functional safety for sensors in the automotive domain. Key enablers of highly automated vehicles will be robust Radio Detection and Ranging (RADAR) and Light Detection and Ranging (LiDAR) solutions with additional support from vision cameras. Through fusion of sensor data and control functions enabling safe automated driving in rural as well as in urban environments is possible. In the project PRogrammable sYSTems for INtelligence in automobilEs (PRYSTINE) the consortium aims at a Fail-operational Urban Surround perceptION (FUSION) [2]. For years various Advanced Driver-Assistance Systems (ADAS), such as Electronic Stability Control (ESC) and Anti-lock Braking System (ABS) have been mandatory in new cars in the European Union [3]. ESC and ABS are ADAS, which are active safety components in contrast to passive safety components, such as seat belts and airbags [4]. For highly automated vehicles it is indispensable that ADAS are highly reliable and therefore ensure the safety for the driver, passengers and all other road users. Due to the increasing quantity and high reliability requirements of such ADAS and integrated systems the Society of Automotive Engineers (SAE) has introduced six levels of driving automation. A higher SAE level describes a higher level of driving automation of the vehicle. Due to the responsibilities that the systems take over the vehicle, it is possible to declare the SAE level of the vehicle [5]. Regardless of whether a vehicle, according to the manufacturer, would support higher automation levels, it is currently necessary in many countries that the driver continues to observe the environment and in an emergency takes over control [6]. For example, according to Article 8 of the Vienna Convention on Road Traffic, the driver must be able to continuously control the vehicle. The Vienna Convention on Road Traffic was ratified by the majority of EU member countries and several others. Large countries, such as the USA, China or England, are not among the signatories [7]. Due to legal and technical barriers driving automation levels

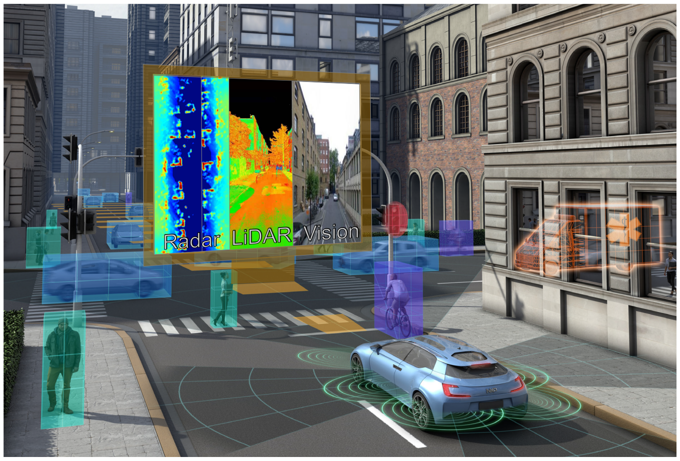

Figure 1. PRYSTINE concept view of a Fail-operational Urban Surround perceptION (FUSION) [2].

This publication is an extended Version of the "Monitor for Safety-Critical Mirror Drivers of MEMS Micro-Scanning LiDAR Systems" [1] publication, which was published in the Proceedings of the Tenth International Conference on Performance, Safety and Robustness in Complex Systems and Applications.

currently do not go beyond SAE level 2. From a legal point of view it will be necessary to adapt laws for introduction of vehicles with SAE Level 3 and greater in the future, as well as developing ADAS with higher levels of safety, reliability and availability. In projects like PRYSTINE, the goal is to develop components and systems for highly reliable and safe ADAS [2]. To ensure the proper functionality of systems it is mandatory to monitor said systems, especially parts which are safety critical. In case of a malfunction, the system has to be aware of its degraded state and in the worst case suspended its operation. Hence, these safety monitors are essential for ADAS in vehicles of SAE level 3 and above. Misbehaviour of a system is only detectable if the system is being monitored continuously. Therefore, we engaged in monitoring the Safety-Critical Mirror Driver of a 1D MEMS Micro-Scanning LiDAR System.

With our paper contribution we:

- Create a novel test opportunity for control loops.
- Ensure the detection of malfunctions during test run.
- Enable a reliability assessment of the LiDAR system.
- Allow for early warning about imminent failures of the LiDAR system.
- Enhance safety with diverse monitoring approaches.

Following aspects will be discussed: The overview on related work of MEMS-based LiDAR systems and several monitoring approaches are given in Section II. Architectures of novel safety monitors for the Safety-Critical Mirror Driver in a MEMS-based LiDAR System will be presented in detail in Section III and the achieved results including their discussion will be provided in Section IV. The summary and short discussion of the findings will conclude this paper in Section V.

II. Related Work

Currently available LiDAR technologies tend to be very bulky and cost intensive, such as the Velodyne HDL-64E [9]. Therefore, industry and academia put a lot of effort into the research of automotive qualified, long-range but low-cost LiDARs. Druml et al. introduced a 1D MEMS Micro-Scanning LiDAR, which is able to perceive the environment up to 200m, shall cost less than 200$ and is qualified for automotive applications due to its robustness [8]. The functional principle of the 1D MEMS-based LiDAR by Druml et al. is depicted in Figure 3. Several lasers are shot on the 1D MEMS mirror. A vertical laser beam is deflected by the mirror and sent into the scenery. This vertical line is moved horizontally across the Field-of-View(FoV) by oscillation of the mirror and the reflected light of the obstacle is captured by a stationary detector.

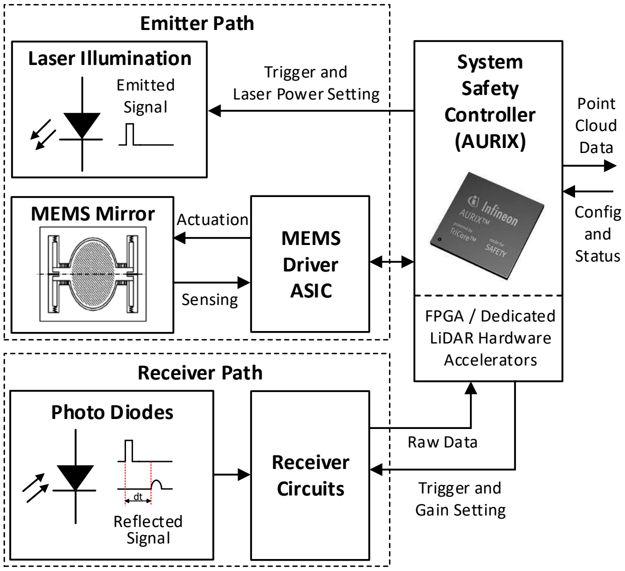

Figure 2. System concept of a 1D MEMS-based automotive LiDAR system by Druml et al. [8].

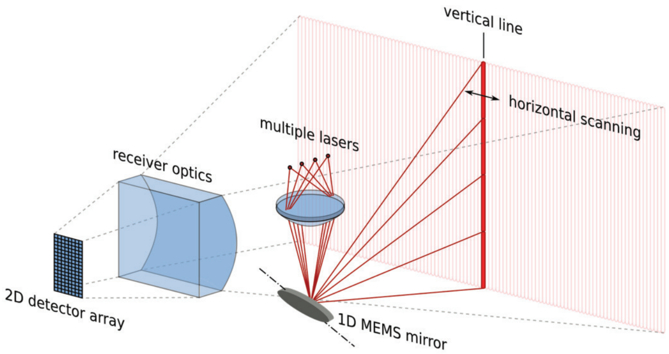

Figure 3. Functional principle of a 1D micro-scanning LiDAR [8].

A. *1D MEMS Micro-Scanning LiDAR*

In this section, the 1D MEMS-based LiDAR System by Druml et al. is presented. The system concept of the MEMS-based LiDAR is depicted in Figure 2. Generally Druml et al.'s system consists of an emitter path, a receiver path and the System Safety Controller (AURIX). The emitter path includes a laser illumination unit, the MEMS mirror and the actuation and sensing unit of the mirror, the MEMS Driver ASIC. Within the receiver, an array of photo diodes and the receiver circuitry is included. The System Safety Controller is the central unit, which is responsible for monitoring, controlling and signal processing. Regarding the signal processing part, the task of the System Safety Controller is to compute and provide a 3D point cloud for dedicated ADAS [8]. Due to the dependence of correct position, direction and verification signals from the mirror, the Driver ASIC, which is responsible for the actuation and sensing of the MEMS mirror, is described in particular. The MEMS Driver provides crucial signals to the System Safety Controller. Thereby it is mandatory that the delivered information is reliable. By reference to the correctness of these crucial signals, the System Safety Controller will create a plausible 3D point cloud with the raw data from the receiver circuits. If the crucial signals were corrupted, the 3D point cloud would be useless due to wrong assumptions of the reflected laser origin.

In Figure 4, the crucial signals are illustrated, which are provided by the MEMS Driver ASIC. These signals are needed to monitor the current status of the MEMS mirror during operation. The POSITION_L represents whether the mirror is aligned to the left or to the right side; logical high means an alignment to the left and logical low to the right. DIRECTION_L indicates in which direction the movement is directed; logical high means moving to the left and logical low to the right. Precise and high-frequent phase information of the current mirror position is provided by a PHASE_CLK signal that counts from 0 to n_{max} in equal time steps during one mirror oscillation. Furthermore, an ANGLE_OK signal is available in addition to the tracking signals. This ANGLE_OK signal notifies the System Safety Controller when the Driver ASIC operates according to the programmed specification (e.g., angle setpoint is reached). To be able to ensure functional-, eye-, and skin-safety this notification is mandatory: MEMS mirror's current position and MEMS Driver ASIC's internal position information must match to allow the laser to be emitted [8].

B. Test Facilities

One of the major objectives of the automobile industry is to evolve individual traffic. The coexistence of partially, highly and fully automated cars will be the reality in the near future. In conventionally equipped vehicles, the driver is responsible for environmental perception, operation of the vehicle and intervention in hazardous situations. In prospective automated cars more and more competences will move from the driver to the car. Based on information, which is obtained from ADAS, the vehicle will make decisions. Therefore, it is obviously necessary that this information is reliable. To ensure safe and reliable operation of ADAS and their embedded components like LiDAR, it is mandatory to test the behavior for correctness. BISTs and a wide variety of safety monitors can be used for this purpose.

1) Built-In Self-Test:

A Built-In Self-Test (BIST) operates simultaneously with the circuit and is monitoring or checking the output of a circuit to check its validity. The BIST needs a strategy for generating input signals for the circuit and has to know how to evaluate the correlated output. The circuit or device which is tested is called the Circuit Under Test (CUT). A basic BIST architecture is shown in Figure 5. A realization of a BIST fundamentally needs to implement four new functions within the existing system. First of all, there is the Test Pattern Generator (TPG), which is responsible for generating the input signals for the test. The test pattern consists of multiple sets of test cases, which theoretically simulate all possible combinations of input signals. The complement to the TPG is the Output Response Analyzer (ORA). Its task is to know every correct output response of the CUT and decides whether the current output is faulty or valid. To create a meaningful and valid test it is important to isolate the test from any other input. Therefore, the Input Isolation Circuitry (IIC) is implemented. Its task is to decouple all input signals, which are commonly provided to the CUT and replace them with test-signal coming from the TPG. Last, but not least to synchronize the behaviour of the TPG, ORA and IIC the Test Controller is implemented. First it initializes a specific test, then decouples the System Inputs and finally activates the ORA which then outputs a Fail or Passed signal [10][11].

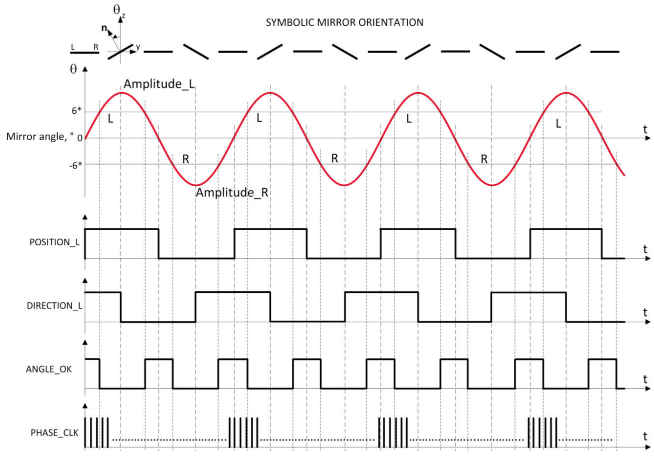

Figure 4. Crucial signals of the MEMS Driver ASIC from Druml et al.'s LiDAR system [8].

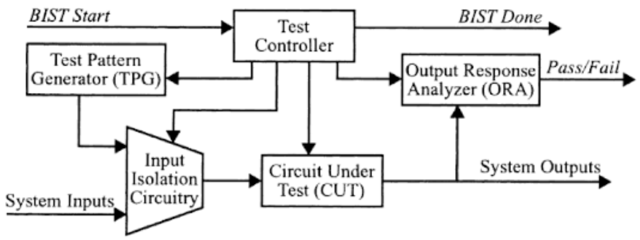

Figure 5. A basic Built-In Self-Test Architecture [10].

2) Safety Monitor Approaches:

Beside BISTs there are also other monitors, which verify the behavior of circuits and whole systems. Schuldt et al. [12], for example, strive to test and validate ADAS efficiently by referencing systematically generated virtual test scenarios. The idea hereby is to identify the factors that affect the assistance system. Hence, the test scenarios will be generated. By reference to the test scenarios a test will be executed and due to the variety of scenarios an evaluation of the results can be done. Another approach to monitor ADAS is presented by Mauritz et al. [13]. With this approach, results obtained from simulations are transferred to road scenarios. They ensure a consistent behavior of the ADAS in both worlds due to a simulation of realistic driving conditions and by utilization of a set of runtime monitors. Furthermore, Meany [14] illustrates that Integrated Circuits (IC) provide the basis for all modern safety-critical systems. According to Meany, besides redundant and diverse development, it is necessary to monitor the ICs to achieve fault-tolerance. There are several ways to monitor the IC during operation. Meany addresses several opportunities of IC diagnostics in his paper.

3) On-Board Diagnostic Systems:

The California Air Research Board (CARB) was established in 1967 as commission of experts to draw up legislative proposals for control of air pollution. The idea of On-Board Diagnostic (OBD) systems for vehicles was then born on the one hand by CARB and on the other hand by the car manufacturers themselves in the 1970s. McCord [15] explains in his book, how it came about from the establishment of this agency in 1967 to the OBD protocols that are standardised today. OBD-I, all standards before OBD-II was introduced, dealt with engine malfunctions and emission equipment malfunctions. OBD-I and OBD-II are well described in several publications [15], [16], [17]. In difference to the OBD-I regulations in which only a limited number of components had to be monitored, the current OBD-II regulations include monitoring of a wide range of components and systems that in turn also monitor components. The fundamental strategy behind the OBD II system is unchanged from the OBD-I system: OBD-II systems

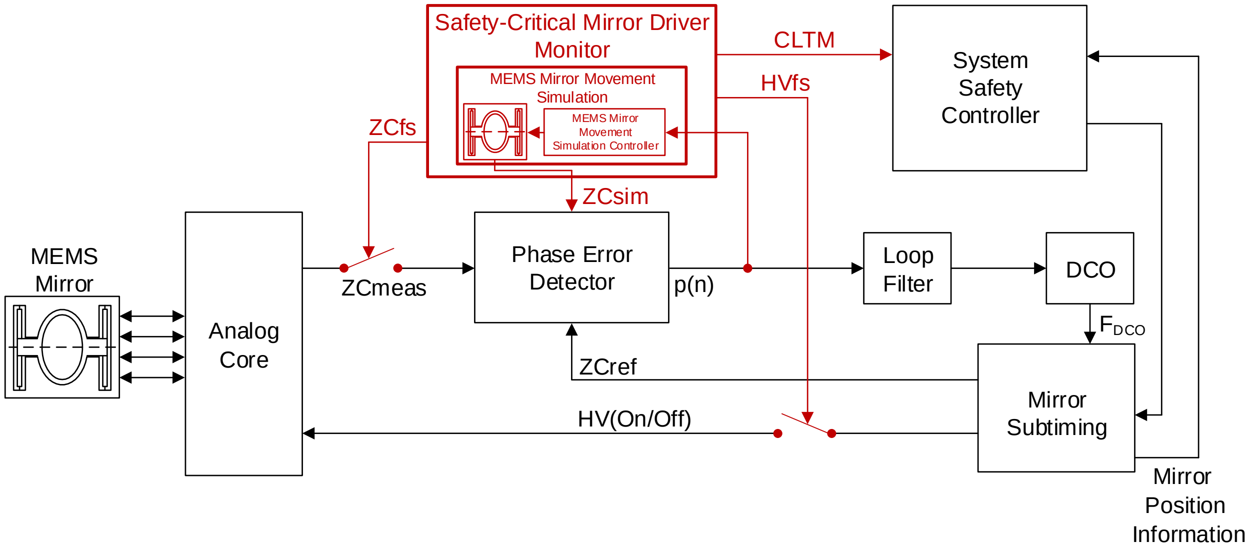

Figure 6. Block diagram of a PLL architecture with the novel adaptions to include a Safety-Critical Mirror Driver Monitor module in the system.

monitor emission-related components. When a problem is detected, the driver of the vehicle is alerted by the illumination of the so-called Malfunction Indicator Light (MIL) on the dashboard. The MIL can be triggered under a variety of conditions, as Durbin et al. [18] described in their publication. In the case of sporadic faults (e.g., due to a loose contact), the MIL may turn off after the fault has disappeared or after the next engine start. Otherwise, this can only be done by reading out and clearing the fault memory at the workshop. This approach can also be pursued for other monitors. For highly automated vehicles, a system degradation can be logged and further examined with similar approaches.

III. Core Concepts and Architectures

In this section, we present our concepts and architectures for novel safety monitors of MEMS-based LiDAR systems. The reliability of the Driver is a sensitive topic. Therefore, it is indispensable to monitor and test the Driver extensively and diverse. Thus, we introduced novel procedures to enable testing and monitoring the Driver component.

A. Novel Safety-Critical Mirror Driver Monitor

The first procedure, we present in our publication is a novel safety monitor for the Driver to check the functionality of the phase-locked loop (PLL) control. It is a procedure to evaluate the correct operation of a control loop, while the system is not in use. For deeper insight into this concept of the procedure, the architecture and process flow will be described in the following. At first, the architecture modifications are highlighted and described. Furthermore, we go through the process flow of the monitoring and test period. With this new monitor there is another possibility to detect faults in the Driver module at an early stage and to take appropriate measures beforehand. In case of detected faults, for example, the System Safety Controller will be informed and the LiDAR system can be degraded or disabled accordingly. Due to the diversity of the testing module it should be possible to prevent prior undetectable faults even better.

In Figure 6, the modified block diagram is illustrated. In principle, it is a common PLL, which is essential for the MEMS mirror actuation, the System Safety Controller, the MEMS mirror and our novel Safety-Critical Mirror Driver Monitor (SCMDM). The HV(On/Off) signal sets the points in time in the internal schedule at which the High Voltage (HV) is switched on or off. This internal schedule is managed by the Mirror Subtiming block. How fast or slow this schedule is processed depends on the PLL and therefore we aimed at testing the PLL on its functionality. For this purpose we designed a SCMDM and adapted the existing architecture and integrated our novel monitor. The core of the SCMDM consists of a mirror simulation part and a decision part. The decision part is responsible to evaluate the test run and notify the System Safety Controller. With the begin of the test run and the accompanying monitoring of the system, it is also necessary to decouple the Driver from the physical MEMS mirror. Hence switches for the Zero-Crossing measured (ZCmeas) and High Voltage On/Off (HV(On/Off)) signals were implemented. To start the test run the SCMDM block disables the switch for ZCmeas signal by Zero-Crossing forwarding stop (ZCfs) signal and the switch for HV(On/Off) signal by High Voltage forwarding stop (HVfs) signal. Furthermore, the SCMDM notifies the System Safety Controller of the test run by the Control Loop Test Mode (CLTM) signal.

After a test run is started the Zero-Crossing simulated (ZCsim) signal is forwarded to the Phase Error Detector (PD) block instead of the ZCmeas signal. A test run can be started at a vehicle startup or even while stopping in front of a traffic light. In case of a vehicle startup, the frequency of the simulated MEMS mirror movement is set to a random but plausible frequency. Otherwise, the frequency is set to a different frequency than the actual mirror swing to test and monitor the behaviour of the MEMS Driver during control operation. To be able to adapt the simulated frequency to the Zero-Crossing (ZC) a MEMS Mirror Movement Simulation Controller (MMMSC) is implemented in the simulation part of the SCMDM. By reference to the PLL error this controller is adapting the simulated MEMS mirror frequency and works contrary to the PLL. Due to the characteristics of the MEMS mirror in regard to acceleration and deceleration, the control loop of the simulation must take these into account. This is necessary to be able to emulate the physical MEMS mirror's behavior after frequency increase respectively decrease. The

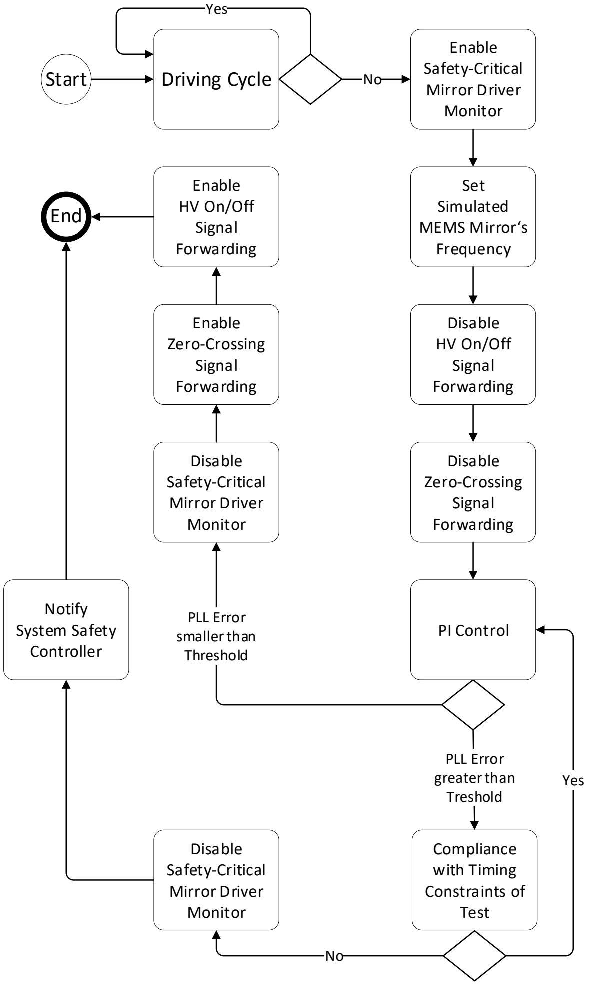
Yes
Start
Driving Cycle
No
Enable Safety-Critical Mirror Driver Monitor
End
Enable HV On/Off Signal Forwarding
Set Simulated MEMS Mirror's Frequency
Enable Zero-Crossing Signal Forwarding
Disable HV On/Off Signal Forwarding
Disable Safety-Critical Mirror Driver Monitor
Disable Zero-Crossing Signal Forwarding
Notify System Safety Controller
PLL Error smaller than Threshold
PI Control
PLL Error greater than Treshold
Yes
Disable Safety-Critical Mirror Driver Monitor
Compliance with Timing Constraints of Test
No

Figure 7. Process flow of the Safety-Critical Mirror Driver Monitor module.

acceleration of the mirror requires more energy effort than its deceleration. Thus, the integrator values have to be chosen accordingly to that fact. An overview of the process flow of this procedure is depicted in Figure 7. The test cycle and monitoring procedure is divided into the following steps:

1) **Checking for Driving Cycle**

   The operational state of the vehicle is continuously examined whether the vehicle is in the driving or not. A stopped driving cycle is, for example, a vehicle stop before a traffic light or a vehicle start. A test cycle with subsequent mirror restart is usually shorter than one second. In both cases, traffic light stop and vehicle start, there is at least 1s time to perform the test and monitoring cycle. Hence, the SCMDM is started after a stop of the driving cycle is detected.

2) **Enable Safety-Critical Mirror Driver Monitor**
   After the driving cycle check green lights the test the SCMDM is enabled and notifies the System Safety Controller via the CLTM signal about the test cycle. The next step is to adjust the frequency for the simulated mirror.

3) **Frequency Adjustment**
   On the basis of a simulated mirror movement the adequate and orderly function of the MEMS Driver ASIC's PLL shall be proven. Therefore, it is necessary to set a start frequency for this simulated mirror with a significant difference to the actual frequency of the physical MEMS mirror. In case of a vehicle start it is only necessary to choose a frequency within given limits of the physical MEMS mirror. If the MEMS mirror has already been in operation, the frequency to be set must then be selected within plausible limits and the selected frequency must also be sufficiently different from the actual mirror frequency. After the initial frequency of the mirror simulation is set the system has to be decoupled from the physical MEMS mirror during the test cycle.

4) **Decoupling**
   Switches have been integrated into the existing architecture to decouple the system from the MEMS mirror. By means of HVfs the HV(On/Off) signal is decoupled from the physical mirror and thus prevents an unintended mirror actuation. During the test phase, the mirror is actuated in an open loop mode with the HV(On/Off) value, which is configured before the test is started. In order to prevent a disturbance of the control loop during test mode by the ZC of the physical mirror, the ZCmeas signal is switched off. Thereby pnly the ZCsim signal is forwarded to the PD block and the PLL is not affected due to two different, actual and simulated ZC, signals.

5) **PI Control**
   Afterwards the control of the PLL and the simulated mirror frequency starts. The PLL is operating as usual and tries to match the internal adjusted frequency with the simulated mirror frequency. The simulated mirror is also adapting the frequency with respect to the specifics of the acceleration and deceleration of the physical mirror. By reference to the obtained PLL error the MEMS Mirror Movement Simulation (MMMS) part is informed whether an acceleration (frequency increase) or a deceleration (frequency decrease) has to be simulated. It is necessary to know whether the simulated mirror needs to be accelerated or decelerated because the integrator values of acceleration and deceleration differ. Due to the difference in energy consumption between acceleration and deceleration. This regulation happens until either the simulated mirror has the desired frequency or a time limit is reached.

6) **End of PI Control**

   a) **Control Success**
      After the control process was successful, the SCMDM is disabled and the physical MEMS mirror is integrated into the control system again instead of the simulated one. To re-integrate the MEMS mirror, the ZCmeas signal is forwarded to the PD block and the HV(On/Off) signal of the Mirror Subtiming block is forwarded to the Analog Core that connects to the physical mirror.

   b) **Control Abort**
      In case the control is aborted by reaching the time limit, the SCMDM is also disabled. In contrast to successful control, however, a notification of failure is transmitted to the

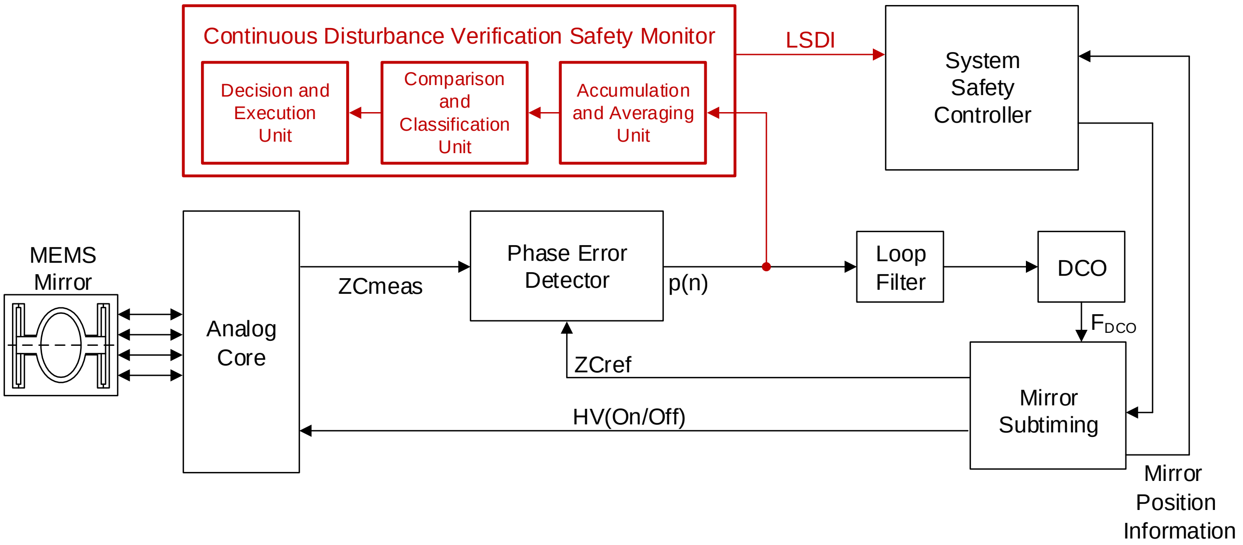
Continuous Disturbance Verification Safety Monitor
Decision and Execution Unit
Comparison and Classification Unit
Accumulation and Averaging Unit
LSDI
System Safety Controller
MEMS Mirror
Analog Core
ZCmeas
Phase Error Detector
p(n)
Loop Filter
DCO
F_{DCO}
ZCref
Mirror Subtiming
HV(On/Off)
Mirror Position Information

Figure 8. Block diagram of a PLL architecture with the novel adaptions to include a Continuous Disturbance Verification Safety Monitor module in the system.

System Safety Controller. The System Safety Controller is then responsible for further measures. Such measures could be a further test run or a degradation of the system.

7) **Encoupling**
After the test run is finished, the physical mirror is coupled back into the system. This works in principle similar to the start-up procedure. The physical mirror in open loop mode is put back into closed loop mode by activating the PLL. This completes the test run and the system continues to operate as usual.

With this novel procedure there is the possibility to check the function of a control loop for MEMS-based LiDAR systems. Especially for safety-critical components in environmental perception systems, it is important due provide diversity in addition to redundancy of tests and monitoring. The most important thing is to ensure the correct operation of the systems that provide information for ADAS and other sensor fusion components. Section IV discusses and explains the results of the novel monitor approach.

B. Continuous Disturbance Verification Safety Monitor

The second procedure, we present in our publication, is a novel safety monitor for the MEMS Driver to continuously check the system for disturbances. This procedure is focused on disturbances in the control loop, which can be detected via the provided PLL error during the system runtime. To obtain a more detailed understanding of this concept of the procedure, the architecture and process flow will be discussed in the following. First of all the architectural changes are highlighted and described. Furthermore, the process flow of the monitoring and degradation steps will be illustrated. Another possibility for disturbance detection and the corresponding degradation measures is made possible by this new type of monitor. For example, if a reoccurring disturbance is detected, measures can be taken depending on the severity of the disturbance, ranging from partial degradation to complete degradation of the LiDAR system. As a result it should be possible to degrade supposedly malfunctioning MEMS-based LiDAR systems in sensor fusion units of environment perception systems.

Figure 8 shows the block diagram of a common PLL architecture with the modifications for the integrated **Co**ntinuous **D**isturbanc**e** Ver**i**fication **S**afety M**o**nitor (CodeIso) and the System Safety Controller. The PLL is responsible for matching the frequencies of the MEMS mirror and the MEMS Driver. With a constant low PLL error, the frequencies of the MEMS mirror and MEMS Driver are approximately equal. If the PLL error increases, this may be due to several reasons. It can be caused, for example, by an frequency adaption during the adjustment phase to the new frequency or by a massive shock. Or due to physical problems with the MEMS mirror such as ageing or other signs of wear. Therefore, we designed a CodeIso and integrated this novel monitor into the existing architecture. The CodeIso is essentially composed of an Accumulation and Averaging Unit (AAU), a Comparison and Classification Unit (CCU) and a Decision and Execution Unit (DEU). The AAU is responsible for accumulating the absolute PLL error values over a specified number of Mirror Half Periods. These accumulated absolute PLL error values will afterwards be averaged and forwarded to the CCU. In the CCU, the PLL error mean value obtained will be compared with a PLL error mean value set by an authorised mechanic or technician during the last maintenance in the repair shop. Depending on the deviation of the obtained PLL error mean value from the preset PLL error mean value, the measurement is classified into a Degradation Level. The classified Degradation Level will then be stored as a histogram. This histogram is subsequently forwarded to the DEU to be able to validate the Overall Degradation Level of the LiDAR system. In the DEU a validation of the Overall Degradation Level takes place. According to the results of this validation, further action can be taken. In any case, the System Safety Controller will be informed of the Level of System Degradation Indicator (LSDI) of the current Degradation Level of the LiDAR system. The System Safety Controller is the interface between the LiDAR system and the sensor fusion unit in the entire environmental perception system. With this information the LiDAR system is then degraded by the System Safety Controller in the sensor fusion unit of the environment perception system when the LSDI indicates a necessary degradation. Such Degradation Levels can either change again during runtime or, under certain circumstances, only be altered after the system has been inspected, repaired if necessary respectively replaced and finally released. This monitor is used to observe the system and does not take corrective action. The purpose of this procedure is to ensure that any disturbances are detected and the environment perception system can be alerted accordingly. The procedural flow is depicted in Figure 9. The monitoring procedure is divided into the following steps:

1) **Checking for System Degradation**
After startup the LiDAR system first checks whether the system is fully degraded or not. If the system is fully degraded, the CodeIso is not enabled. The CodeIso can only be re-enabled after the system has been inspected, repaired respectively replaced and released. Otherwise, the CodeIso is started after the system startup and operates during the whole system runtime until the system is degraded or the system is shut down.
2) **Enable Continuous Disturbance Verification Safety Monitor**
When the degradation check shows that the system is not fully degraded and therefore not neglected in the sensor fusion, the CodeIso is enabled. The CodeIso is now active as long as there is no full system degradation. The system is monitored during operation by the CodeIso.
3) **PLL Error Accumulation**
As soon as the CodeIso is active, the absolute PLL error value accumulation starts. For each Mirror Half Period, a PLL error is measured that occurs between the actual ZC of the MEMS mirror and the ZC reference signal. This PLL error is then used as an absolute value to average the PLL error values over a certain measuring period and is cached. Until the desired number of PLL error values per Mirror Half Period is reached, these absolute PLL error values are constantly accumulated.
4) **Averaging Accumulated PLL Error**
After the accumulation of the absolute PLL error values is complete, the PLL Error Mean Value (PEMV) is formed.

$$PEMV = \frac{1}{n}\sum_{i=1}^{n}|PEV_i| \qquad (1)$$

In Equation (1), the PEMV is calculated by reference to the sum of the individual absolute PLL error values and the quantity of PLL error values. PEV$_i$ represents the PLL error value of measurement i. This PEMV is then forwarded to the CCU to compare and classify the state of the system.
5) **Compare and Classify PLL Error Mean Values**
During maintenance, the system is inspected and a mean value of the measured absolute PLL error values during proper operation is formed. This Maintenance PLL Error Mean Value (MPEMV) is compared with the previously calculated PEMV. Depending on the deviation from the MPEMV, the PEMV is classified into a Degradation Level.
6) **Creation of Histogram**
The histogram is afterwards filled with the previously classified Degradation Levels. Depending on the level of degradation, the entry in the histogram is weighted. For example, for Degradation Level 0, each Degradation Level 0 entry is increased by 1. For Degradation Level 1 it is increased by 1.5 and for Degradation Level 2 by 2. According to how significant a Degradation Level should be, you can change the weighting. The histogram is filled up

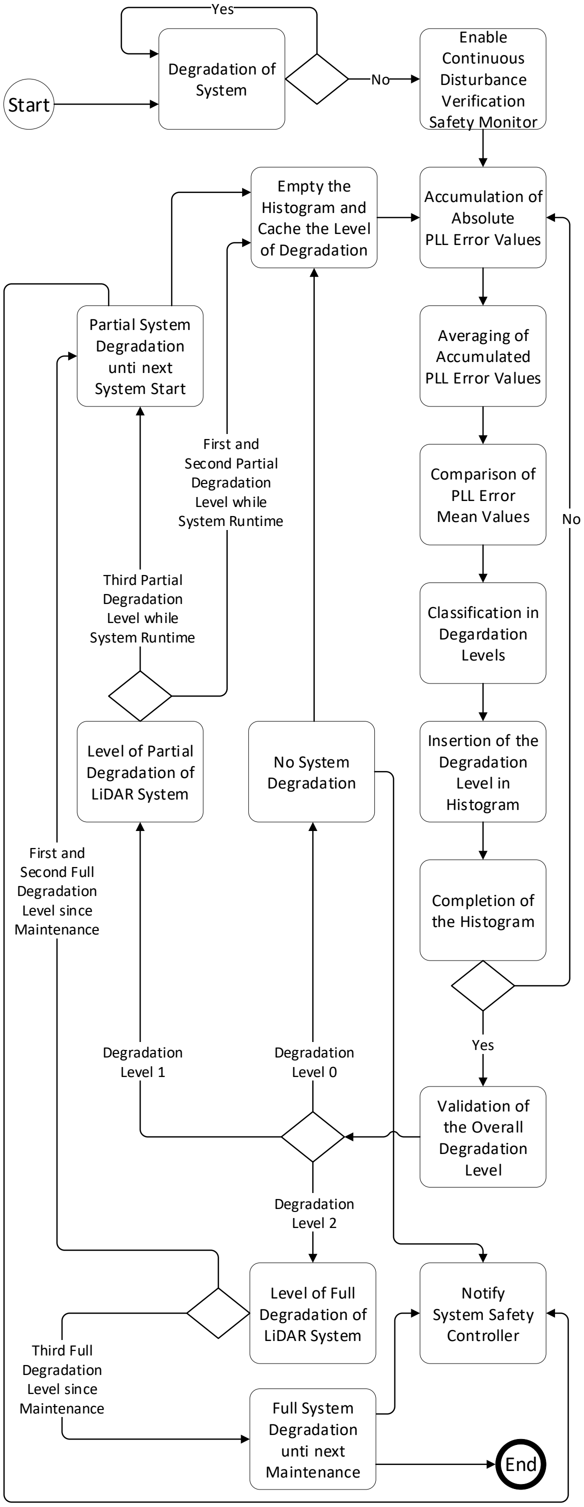
Yes
Start
Degradation of System
No
Enable Continuous Disturbance Verification Safety Monitor
Empty the Histogram and Cache the Level of Degradation
Accumulation of Absolute PLL Error Values
Partial System Degradation unti next System Start
Averaging of Accumulated PLL Error Values
First and Second Partial Degradation Level while System Runtime
Comparison of PLL Error Mean Values
No
Third Partial Degradation Level while System Runtime
Classification in Degardation Levels
Level of Partial Degradation of LiDAR System
No System Degradation
Insertion of the Degradation Level in Histogram
First and Second Full Degradation Level since Maintenance
Completion of the Histogram
Yes
Degradation Level 1
Degradation Level 0
Validation of the Overall Degradation Level
Degradation Level 2
Level of Full Degradation of LiDAR System
Notify System Safety Controller
Third Full Degradation Level since Maintenance
Full System Degradation unti next Maintenance
End

Figure 9. Process flow of the Continuous Disturbance Verification Safety Monitor module.

with the Degradation Levels of the PEMVs until the specified number of histogram entries is reached. Once the histogram is filled, the validation of the Overall Degradation Level is performed.

7) **Validation of Overall Degradation Level**
The validation of the Overall Degradation Level is done by evaluating the individual classes of the Degradation Levels in the histogram. The class that has the largest amount is selected as the Overall Degradation Level. Depending on the resulting Degradation Level, the further steps can be taken. In principle it leads to one of the following actions:

   a) **Degradation Level 0**
   In case the validation results in a Degradation Level 0, then the system is considered reliable and will not be degraded. The histogram is cleared and the Degradation Level is cached and reported to the System Safety Controller via the LSDI. Afterwards the monitoring process restarts with accumulation of absolute PLL error values.

   b) **Degradation Level 1**
   If the monitoring process leads to a Degradation Level 1, then there is not necessarily a system degradation. Until the 3rd time, the system is treated as at Degradation Level 0. Therefore, the histogram is cleared and the level of degradation is cached. But unlike Degradation Level 0, the System Safety Controller is not informed about a new level of degradation. However, if it happens for the 3rd time during system runtime that a Degradation Level 1 results, the system will be partially degraded. The System Safety Controller will be informed via the LSDI and gets a lower priority in the sensor fusion of the environment perception system. Afterwards, the histogram is cleared and the Degradation Level is cached, just like before. The monitoring process starts again.

   c) **Degradation Level 2**
   Should a Degradation Level 2 occur during the monitoring process, there are two possibilities, similar to the Degradation Level 1. For the first two occurrences of Degradation Level 2 after a performed maintenance the system is partially degraded. Here, it is the same as for the 3rd time of Degradation Level 1. The systems priority in sensor fusion is downgraded, until the next system restart and the System Safety Controller is informed via the LSDI. Then the histogram is cleared again and the level of degradation is cached. The monitoring process starts again. However, if there is a 3rd occurrence of Degradation Level 2 since maintenance, the system is completely degraded and the System Safety Controller is informed via the LSDI. The system remains degraded until the next maintenance. The system degradation can then only be removed by an authorized technician or mechanic after the system has been inspected and, if necessary, repaired respectively broken components replaced.

This new monitoring procedure creates another possibility for early detection and reaction to disturbances in MEMS-based LiDAR systems. The system can then be degraded in order to avoid transmitting any erroneous data to the environment perception system. This procedure can help detection of imminent MEMS mirror failures due to aging or MEMS mirror fractures caused by massive shocks and to early initiate required maintenance. Section IV discusses and explains the results of the novel CodeIso approach.

IV. Results

In this section, we provide the measurement results and analysis of our novel monitoring procedures, which have been introduced in Section III.

A. *Novel Safety-Critical Mirror Driver Monitor Evaluation*

Figure 10 shows the start of the novel monitor procedure. After 427 Mirror Half Periods, the frequency of the simulated mirror is changed. The Angle_Ok signal can be used as an indicator for a frequency shift between mirror and driver, because it indicates whether the angle setpoint is reached or not. At the beginning of the frequency mismatch, this indication is also clearly visible in the ZC measurement. The red signal corresponds to the ZC reference signal of the MEMS mirror Driver and the blue one to the ZCsim signal. After the 427th Mirror Half Period it is clearly visible that the reference and the simulated ZC signal are no longer synchronous. The exemplary course of the mirror is recorded at Mirror Angle. The red curve indicates the course of the mirror at the same frequency and the blue curve looks like the course when the new frequency is set for the simulated mirror. Figure 11 shows that the frequency of the mirror has been adjusted again and that the angle setpoint has been reached again from the 1709th Mirror Half Period onwards. Here the Angle_Ok signal is essential for detecting whether the angle setpoint has already been reached again. The frequencies of mirror and Driver are equalized before the 1709th Mirror Half Period. The exemplary courses of the mirror overlap almost completely, reference and simulated ZC signal also occur again almost simultaneously.

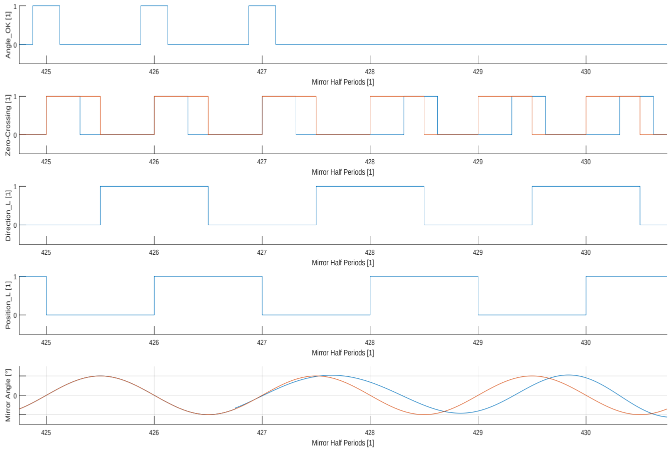

Figure 10. Measurement with the initial frequency adaption of the simulated MEMS mirror.

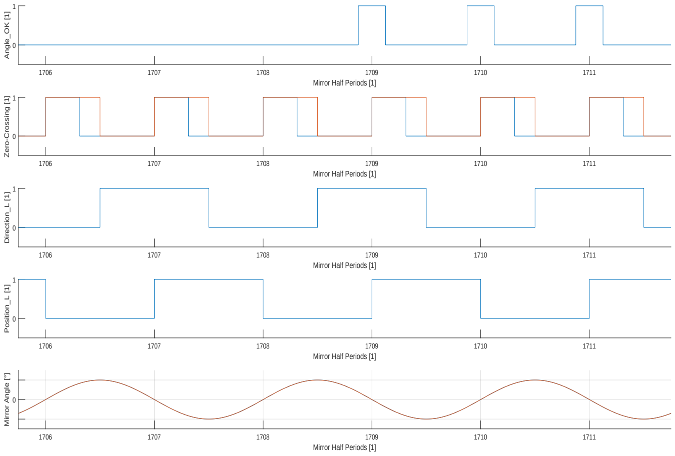

Figure 11. Measurement with the frequency match of the simulated MEMS mirror and the MEMS Driver.

For our measurement, the control required 1282 Mirror Half Periods to adjust the frequencies. That was approximately 220 ms for the frequency range from about 2300 Hz to about 2400 Hz. Depending on the frequency difference between mirror and Driver, this control time can be extended or shortened. Finally, the results of the frequency adaption duration are summarized and shown in Table I.

TABLE I. MEASUREMENT RESULTS of SCMDM

	Begin	End	Time in ms
Duration of Frequency Adaption	427	1709	∼ 220

B. Continuous Disturbance Verification Safety Monitor Evaluation

To test the CodeIso, different scenarios were examined and evaluated. The CodeIso accumulates PLL error values of 100 Mirror Half Periods per test run. The first recorded measurement, which is shown in Figure 12, was recorded without any influence. Here one can see that the PLL error value is close to zero and the frequency remains constant. As shown in Table II, the first measurement results in an average of the absolute PLL error values of 3.42. The classification is determined in advance. In our evaluation of the CodeIso, we defined the limits of the different classes exemplarily to show how the division into the specified classes happens. Degradation Level 0 is divided from 0 up to MPEV plus 10, Degradation Level 1 from MPEV plus 10.01 to MPEV plus 50 and Degradation Level 2 from MPEV plus 50.01. Since a reference measurement, which we consider as the maintenance measurement, was calculated to be an average of the absolute PLL error values of 3.38, it is clear that the measurement in Figure 12 belongs to the Degradation Level 0 class. The classification of the different measurements during a CodeIso run is also shown in Table II.

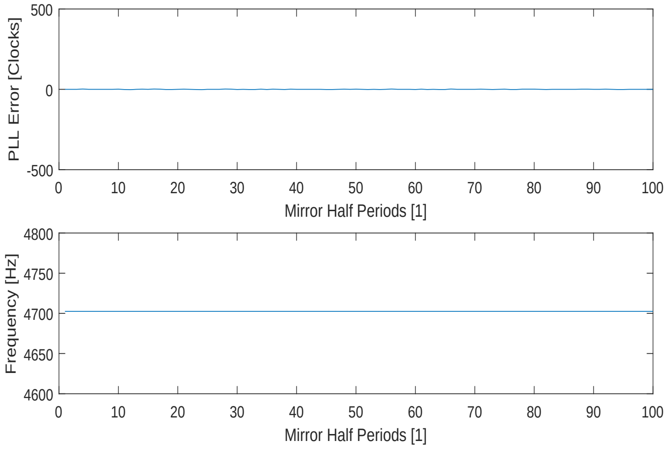

Figure 12. Measurement of the PLL error value accumulation of the CodeIso without any abnormalities.

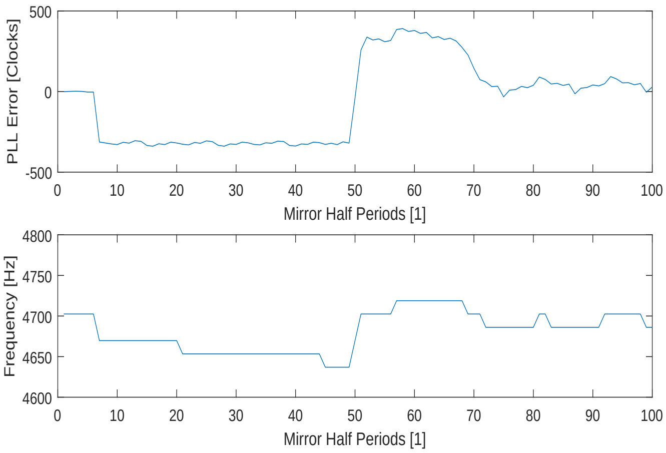

Figure 13. Measurement of the PLL error value accumulation of the CodeIso with an injected massive shock.

TABLE II. MEASUREMENT RESULTS of CODEISO

Measurement	PLL Error Mean Value	Classified Degradation Level
Maintenance	3.82	
1.	3.42	0
2.	215.93	2
3.	24.23	1
4.	10.98	0
5.	198.58	2
6.	28.04	1
7.	6.09	0
8.	7.53	0
9.	5.32	0
10.	206.45	2

Figure 13 shows the 2nd measurement. Here a massive

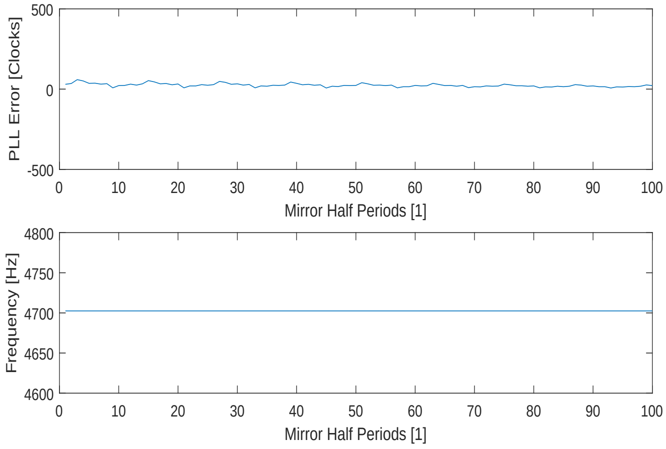

Figure 14. Measurement of the PLL error value accumulation of the CodeIso with effects of the injected massive shock in the measurement before.

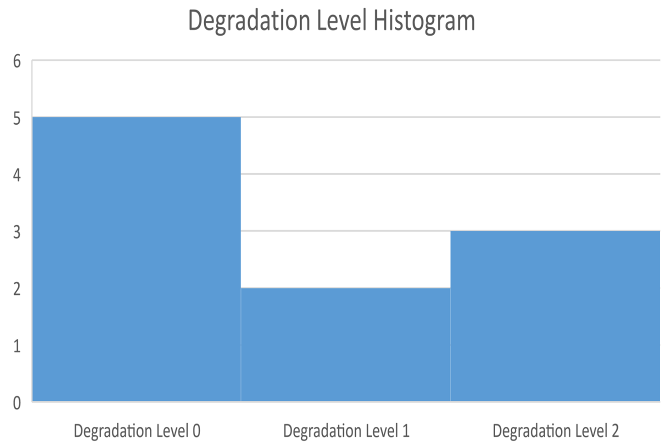

Figure 15. Histogram of a CodeIso iteration with 10 accumulation runs of absolute PLL error values.

shock was injected, simulating a massive shift between MEMS mirror frequency and MEMS Driver frequency. Besides the large PLL error, the unstable frequency clearly shows that the system has been heavily affected. If such a measurement result is obtained, it is clear that it must be noted as Degradation Level 2 in the histogram. As mentioned before, the absolute PLL error value is compared with the MPEV. With 215.93 the PLL error mean value is clearly in the Degradation Level 2 class, because it exceeds MPEV plus 50.01. However, if a majority of such results are obtained, it can be concluded that there are either age-related problems with the MEMS mirror or that the MEMS mirror has been sustainably damaged by a previous massive shock. Furthermore, the 3rd measurement is shown in Figure 14. Here you can see the effects of the previous measurement with the injected massive shock. The frequency is constant again, but the PLL error has not yet settled. Due to the previously defined limits, the 3rd measurement with an absolute PLL error average of 24.23 is slightly in the Degradation Level 1 class. After ten iterations, the histogram shown in Figure 15 is filled with the classified Degradation Levels from Table II. This histogram is now used to validate the Overall Degradation Level. For this purpose, the number of occurrences in the different classes is multiplied by the respective, previously defined factor. A single Degradation Level 2 will not be decisive for the degradation. Depending on the selected factors, more or less of such Degradation Level 2 ratings will be needed to fully degrade the system. The class that contains the highest value will be used as the Degradation Level for the entire LiDAR system. In our case we chose factors 1, 1.5 and 2 for Degradation Level 0, 1 and 2. Figure 16 shows the result for validation. With the highest class value of 6 marked in red, the LiDAR system is set to full degradation. Since we injected a massive shock in three measurements and therefore simulated a heavy damage, respective impairment of the system, it is the result we expected. In case two classes have the same value, the higher Degradation Level is always taken.

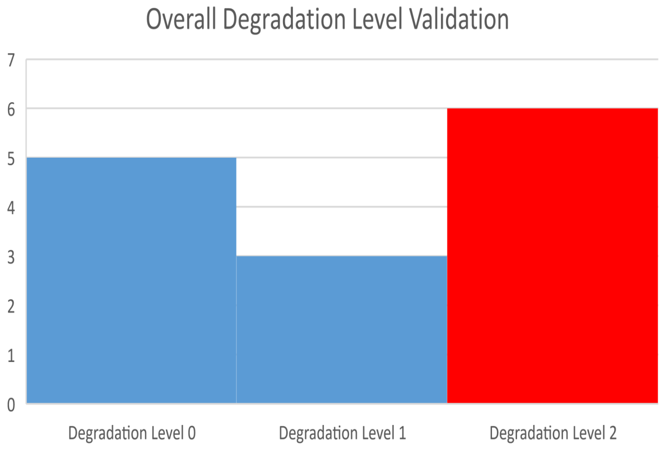

Figure 16. Validation of the Overall Degradation Level by reference to the completed histogram.

V. Conclusion

In our paper, we introduced two novel safety monitor architectures for a Safety-Critical Mirror Driver. With the first monitor we suggest a new possibility to test the control of a MEMS-based LiDAR system and to monitor the functionality of the Driver during the test cycle. The diversity of system monitor options is further increased with this new SCMDM, along with BIST and other diagnostic variants, further reducing the probability of malfunctions remaining undetected. With a duration of around 220ms, this test run is also well under 1s. Therefore, it is unproblematic to perform this procedure during the start of the vehicle or at a vehicle stop in front of a traffic light. Even if the traffic starts to move again, not even 1s passes until the LiDAR system is operational again. Due to the speed at which the vehicle starts to move (usually a slow start), it is only a few centimetres at most that the vehicle does not receive any information from the LiDAR. By further optimizing the parameters, the time required for the test run can probably be shortened considerably. Our intention was to show that in principle it is possible to simulate the mirror and thus create a further possibility for MEMS Driver monitoring by means of the novel monitor. The second monitor we suggest, is a new possibility to continuously check the system for disturbances in the PLL control loop. The CodeIso is used during continuously throughout system operation and is supposed to inform the system of the different Degradation Levels. The absolute PLL error mean values over a given measurement period are used to obtain classified entries in a histogram. After the histogram is filled with the given number of measurements an Overall Degradation Level is determined. In case the MEMS mirror is operated in a frequency range from about 2300 Hz to about 2400 Hz, a statement on the Overall Degradation Level can be made after approximately 10 ms. The weight factors for the Overall Degradation Level were determined exploratory and can also be adapted to get an earlier system degradation or later. Its intention was to design a monitor that detects disturbances in the PLL early and alerts the environment perception system accordingly. With the full degradation of the LiDAR system by this monitor, maintenance of the system becomes necessary. Furthermore, this monitoring procedure extends the diversity of the safety monitors. Monitors as presented here will be even more important in the future for highly automated vehicles than they already are in safety-critical vehicle components. The top priority is to ensure the safety and reliability of the ADAS in the vehicles and also to check whether this is the case.

Acknowledgment

The authors would like to thank all national funding authorities and the ECSEL Joint Undertaking, which funded the PRYSTINE project under the grant agreement number 783190.

PRYSTINE is funded by the Austrian Federal Ministry of Transport, Innovation and Technology (BMVIT) under the program "ICT of the Future" between May 2018 and April 2021 (grant number 865310). More information: https://iktderzukunft.at/en/.

References

[1] P. Stelzer, A. Strasser, P. Pannagger, C. Steger, and N. Druml, "Monitor for Safety-Critical Mirror Drivers of MEMS Micro-Scanning LiDAR Systems," The Tenth International Conference on Performance, Safety and Robustness in Complex Systems and Applications (PESARO 2020), 2020, pp. 7–12.

[2] N. Druml, G. Macher, M. Stolz, E. Armengaud, D. Watzenig, C. Steger, T. Herndl, A. Eckel, A. Ryabokon, A. Hoess, S. Kumar, G. Dimitrakopoulos, and H. Roedig, "PRYSTINE - PRogrammable sYSTems for INtelligence in AutomobilEs," in 2018 21st Euromicro Conference on Digital System Design (DSD), Aug 2018, pp. 618–626.

[3] European Road Safety Observatory, "Advanced driver assistance systems," https://ec.europa.eu/transport/road_safety/specialist/observatory/analyses/traffic_safety_syntheses/safety_synthesies_en, retrieved: October, 2019. [Online]. Available: https://ec.europa.eu/transport/road_safety/sites/roadsafety/files/pdf/ersosynthesis2018-adas.pdf

[4] M. Lu, K. Wevers, and R. V. D. Heijden, "Technical Feasibility of Advanced Driver Assistance Systems (ADAS) for Road Traffic Safety," Transportation Planning and Technology, vol. 28, no. 3, 2005, pp. 167–187. [Online]. Available: https://doi.org/10.1080/03081060500120282

[5] SAE, "SAE International Standard J3016 - Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems," SAE International, Standard, January 2014.

[6] C. Brünglinghaus, "Wie das Recht automatisiertes Fahren hemmt," ATZ - Automobiltechnische Zeitschrift, vol. 117, no. 4, Apr 2015, pp. 8–13. [Online]. Available: https://doi.org/10.1007/s35148-015-0039-0

[7] United Nations Conference on Road Traffic, "19 . Convention on Road Traffic," https://treaties.un.org/pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XI-B-19&chapter=11&Temp=mtdsg3&clang=_en, retrieved: October, 2019. [Online]. Available: https://treaties.un.org/pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XI-B-19&chapter=11&Temp=mtdsg3&clang=_en

[8] N. Druml, I. Maksymova, T. Thurner, D. Van Lierop, M. Hennecke, and A. Foroutan, "1D MEMS Micro-Scanning LiDAR," in The Ninth International Conference on Sensor Device Technologies and Applications (SENSORDEVICES 2018), 09 2018.

[9] Velodyne LiDAR, "HDL-64E," 2016.

[10] C. E. Stroud, A designers guide to built-in self-test. Springer Science & Business Media, 2006, vol. 19.

[11] E. J. McCluskey, "Built-In Self-Test Techniques," IEEE Design Test of Computers, vol. 2, no. 2, April 1985, pp. 21–28.

[12] F. Schuldt, F. Saust, B. Lichte, M. Maurer, and S. Scholz, "Effiziente systematische testgenerierung für fahrerassistenzsysteme in virtuellen umgebungen," 2013, retrieved: October, 2019. [Online]. Available: https://publikationsserver.tu-braunschweig.de/receive/dbbs_mods_00052570

[13] M. Mauritz, F. Howar, and A. Rausch, "Assuring the Safety of Advanced Driver Assistance Systems Through a Combination of Simulation and Runtime Monitoring," in Leveraging Applications of Formal Methods, Verification and Validation: Discussion, Dissemination, Applications, T. Margaria and B. Steffen, Eds. Cham: Springer International Publishing, 2016, pp. 672–687.

[14] T. Meany, "Functional Safety for Integrated Circuits," July 2018, retrieved: November, 2019. [Online]. Available: https://www.analog.com/en/technical-articles/a54121-functional-safety-for-integrated-circuits.html

[15] K. McCord, Automotive Diagnostic Systems: Understanding OBD I and OBD II. CarTech Inc, 2011.

[16] B. Shinde, D. S. Kore, and D. S. Thipse, "Comparative Study Of On Board Diagnostics Systems-EOBD, OBD-I, OBD-II, IOBD-I and IOBD-II," International Research Journal of Engineering and Technology (IRJET), 2016.

[17] P. Baltusis, "On Board Vehicle Diagnostics," SAE Technical Paper, Tech. Rep., 2004.

[18] T. D. Durbin and J. M. Norbeck, "The effects of repairs on tailpipe emissions for On-Board Diagnostics II-equipped vehicles with the malfunction indicator light illuminated," Journal of the Air & Waste Management Association, vol. 52, no. 9, 2002, pp. 1054–1063.