Enabling Fail-Operational Behavior and Degradation for Safety-Critical Automotive 3D Flash LiDAR Systems

Andreas Strasser†, Philipp Stelzer†, Felix Warmer†, Christian Steger† and Norbert Druml*
†Graz University of Technology, Graz, Austria
email:{strasser, stelzer, warmer, steger}@tugraz.at
*Infineon Technologies Austria AG, Graz, Austria
email:{norbert.druml}@infineon.com

***Abstract*—Advancing the current Advanced Driver Assistance Systems (ADAS) is coupled with introducing novel technologies into the automotive domain such as Light Detection and Ranging (LiDAR). LiDAR is attributed as a key-technology that will be one of the key enablers for safe and reliable automated driving. Considering the fact that vehicles nowadays rely on the driver in safety-critical situations leads to the problem that in a fully-automated driving scenario the vehicle needs to control every possible situation on its own. This increases the requirements and the overall safety level of the system but also for each component and needs a gradual transition from fail-safe to fail-operational behvior at least as long as the occupants and other road participants could be endangered.**

This publication introduces a novel system architecture of a fail-operational 3D Flash LiDAR System that enables dynamic system degradation during run-time as well as internal built-in self-test (BIST) for automated failure injection tests. The novel fail-operational system architecture is able to handle critical temperature ranges as well as long-term memory faults.

***Index Terms*—Automotive LiDAR, Fail-Operational, Degradation, Dynamic Safety, Memory Faults**

I. Introduction

The concept of fail-safe behavior is one of the key methodologies that is used in the automotive domain for safety-critical systems to handle failures during run-time [2]. However, this concept will not fullfill the requirements of future fully-automated driving vehicles because of the need of a human driver as a fall-back scenario who is able to control the vehicle. Future fully-automated driving vehicles that are able to provide driving services at SAE Automated Driving Level 4 or 5 will control all possible driving scenarios on their own, including situations in which safety-critical systems partly fail [4]. This fact will force a paradigma change and requires a transition from fail-safe behavior to fail-operational behavior. Especially sensors that are responsible for providing environmental perception data needs to be highly robust and safe. This key requirement for future automated driving systems has already been identified by the European research project PRYSTINE (Programmable Systems for Intelligence in Automobiles). One of the key goals of PRYSTINE is introducing a novel Fail-Operational Urban Surround perception (FUSION) which is based on LiDAR and RADAR sensors as seen in Figure 1. FUSION will be an enabler for safe automated driving in urban and rural environments [1].

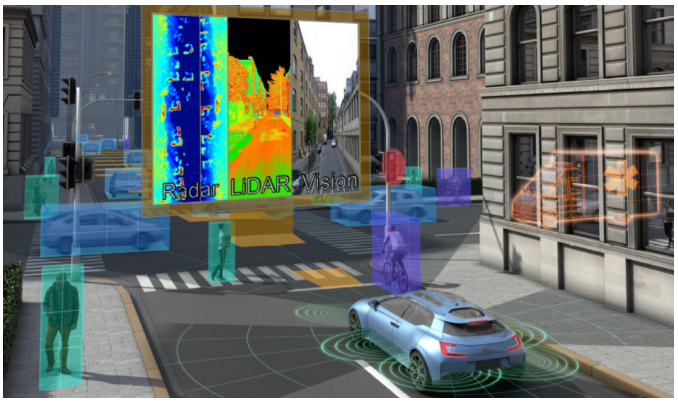

Fig. 1. PRYSTINE's concept view of a fail-operational urban surround perception system [1].

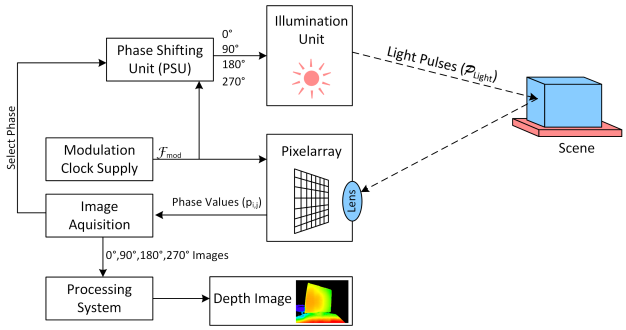

Fig. 2. Conceptional overview of a 3D Flash LiDAR system [3].

In contrast to RADAR, which is already widely used in the automotive domain for ADAS such as Adaptive Cruise Control (ACC), is LiDAR not very common in the aumototive domain yet because of the high costs of the current mechanical spinning LiDAR systems [5], [6]. One possible key changer could be the novel 1D MEMS Micro-Scanning LiDAR system concept, as seen in Figure 2, by Druml et al. which will reduce the costs to approximately 250 Dollar and enables robust and safe automated driving functionalities for middle class vehicles [7]. This novel system is based on a scanning technology

which is enabled by an oscillating MEMS mirror. On the other hand there are also non-scanning LiDAR systems such as the diffuse light cone Flash LiDAR system as seen in Figure 2 that are already available on the market.

This publication describes a novel fail-operational, safety-critical Automotive 3D Flash LiDAR system architecture that enables degradation of specific functions to guarantee the correct behavior of the system in case of failures. Our provided solution makes the following fundamental contributions:

- Describing 3D Flash LiDAR degradation possibilities that enables correct data for other ADAS and ensures safe driving.
- Providing a prototype that proves feasibility of a novel fail-operational 3D Flash LiDAR system architecture that enables degradation from a safety point of view.
- Introducing a novel test platform that is able to verificate the novel introduced degradation functions of the 3D Flash LiDAR prototype.

This paper is structured as follows. Section I gives a short introduction into the topic and what research output is provided by this publication. In Section II, we are providing information about current challenges and other related work in the topic of fail-operational 3D Flash LiDAR systems. Section III introduces our novel fail-operational 3D Flash LiDAR system architecture that enables degradation of safety-critical functions. The evaluation and results can be seen in Section IV such as the Graphical Control Interface that enables the testing of the novel degradation functions of the implemented prototype. Finally, we concluded our results in Section V.

II. Related Work

The change from traditional controlled vehicles by the driver to autonomous driving vehicles requires higher safety standards. The discontiunation of the driver as a control backup in case of a failure will enforce a disruptive change of designing safe and robust vehicles [8]. Any failure that appears during driving must be handled by the system itself and is also known as fail-operational behavior [9], [10]. For this purpose, specific functions must be degraded to a point at which the vehicle still can operate in a safe way that decreases the probability of an accident to the lowest possible limit.

In the next few years, Light Detection and Ranging (LiDAR) will be one of key sensors for environmental perception in automated driving vehicles [1], [7]. LiDAR scans the front scene of the sensor by emiting a laser pulse that is reflected by the objects of the scenery and is received by a photo diode. The measurement range from the LiDAR system is primary defined from the output power of the laser. Because of eye-, and skin-safety the laser must guarantee a specific maximal output power. For that reason, the maximal possible distance is already limitied through that safety specification and can not be extended by increasing the laser power [7]. One negative side effect is that the output power of a laser is affected by the overall temperature. Yulianto et al. [11] described that with a Distributed Feedback Laser (DFL) with an operation wavelength of 1550 nm the slope of the output power was -0.33 mW/°C. Additionally, also the wavelength is varying by the laser temperature with a slope of 0.094nm/°C. Transfer to the automotive LiDAR system would result in a possible decrease of the maximum operation distance. In the worst case, this would vary during operation based on the current temperature that is mostly influenced by the current weather conditions.

Volatile Memory such as Random-Access Memory is necessary to cache sensor data as well as computation results. Especially for LiDAR big on-chip memory arrays are needed [12]. Maksymova et al. [13] described that the amount of data that needs to cached depends on several key parameters of the LiDAR system such as image and range resolution, frames per second, sampling frequency, and others. The last trend in the automotive domain is to use for highly computational tasks consumer modified hardware components such as the Intel Atom A3900 [14]. In the A3900 datasheet [15] the supported memory technology are DDR3L/ECC and LPDDR4. The DDR3L/ECC technology is the same technology that are used in business servers. For Dynamic Random Access Memory (DRAM) technology several research studies are already available that are describing potential soft errors, transient errors and failures in these modules and counter measures [16]–[19]. Especially the large-field study of Schroeder et al. [19] must be emphasized that describes a study of DRAM errors within two years considering multiple vendors, generations, technologies and capacities. Most of the annual incidence errors that appeared were corrected by the internal Error Correction Code (ECC) but there were about 1.3% of uncorrectable errors per machine and 0.22% uncorrectable errors per DIMM. An interesting fact is that temperature does not impact the incidence of memory errors but utilization does [19]. This results in the requirement to consider the utilization of the volatile memory module of the LiDAR system.

In general, fail-operational behavior of safety-critical embedded systems can be achieved by introducing redundant subsystem design and diversity, as described in the IEC 61508 safety standard of Electronic systems [20]. Fail-Operational behavior is particularly important for systems that do not have the possibility of a mechanical fallback. For that specific systems novel system design approaches have been introduced such as the 2-out-of-3 architecture. In this case, three independent systems perform the same tasks and a voting system decides about the correctness of the output [9]. But there are also researchers in the field of fail-operational systems that are enabling this function by introducing a dynamic configuration of their system [21], [22]. For that reason, we are inclined to take the path of dynamically reconfiguring the 3D Flash LiDAR system during operation, in case of failure, and enable a continuous performance of the system to keep up the overall automated driving service as long as needed to prevent any fatal damages. Additionally, we want to decrease the possibility of material fatigue of the components and increase the mean-time-between failures. This will increase the overall safety of the whole system as well as decrease possible costs caused by guarantee services.

III. Fail-Operational 3D Flash Lidar System

This Section gives an overview about the novel developed fail-operational 3D Flash Lidar system architecture that supports automatic degradation in failure cases as well as to take care of safety-critical hardware parts to extend lifetime.

The main focus of the novel system architecture is to determine on a safe behavior in any possible situation. For this purpose, we identified that one of the worst scenarios is driving with high speed on a highway, fully-autonomous and the driver is distracted while the Lidar system is losing environmental perception. In this particular situation, the vehicle is not able to recover from this situation on its own. Traditionally developed vehicles that rely on the driver as a backup system would cause a crash with all consequences such as harmed passengers or worse. Modern vehicles with functionalities that consider self-driving behavior such as Adaptive Cruise Control (ACC) require higher standards for safety-critical components such as fail-operational behavior. For this reason, we decided to develop a novel system architecture for an environmental perception system that is based on Lidar that fulfills the requirement of a fail-operational behavior and is able to degrade functions in specific context such as driving in an overcrowded city or on a highway.

A. System Architecture

In Figure 4 an overview of the novel fail-operational 3D Flash Lidar system architecture can be depicted. The system is divided in two main parts:

- **System Control**
  This sub-system is handling the configuration of the overall system as well as controlling the overall fail-operational processes and application.
- **Memory Manager**
  The Memory Manager is responsible for storing data on the memory and continously checks integrity of individual memory blocks.

The system receives raw input data from the 3D Flash Lidar system to the Memory Manager. The Memory Manager is able to disable specific memory blocks in case of failures and this allows a longer lifetime of the system because faulty memory blocks can be disabled and does not infect higher layers of the processing chain. This data is processed by the application that is fetching the data from the memory. The system controller can be configured by external configuration with focus on preserving memory faults and temperature caused faults. To achieve these targets the control system is able to modify frames per second of the output data, frequency of the processor or resolution of the output image.

1) Preserving Memory Faults: As we have described the common problem with worn out EMMC chips from Tesla vehicles in the Section about Related Work clearly depicts that memory faults could be one of the most common faults for future fully-autonomous vehicles that are using centralized computation platforms for computational tasks [23]. To prevent this circumstance the novel system architecture focuses on this specific problem by enabling an automatic degradation mode for memory faults.

The novel memory monitoring system can be depicted in Figure 5 and is storing the raw data from the 3D Flash Lidar system into the memory block according the index array. Any fault inside the memory block that gets detected triggers

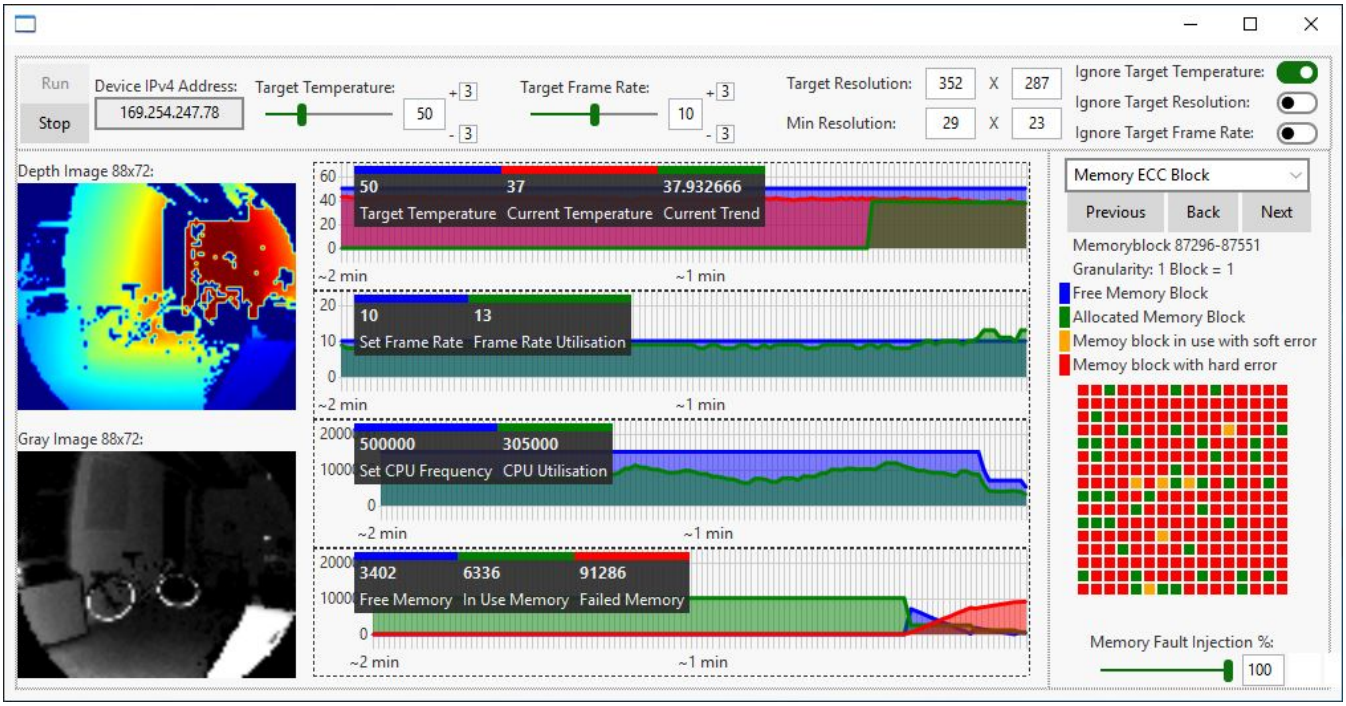

Fig. 3. Graphical Control Interface that depicts the current live camera data, settings, and current monitoring data.

the automatic memory degradation algorithm that is deciding about the further processing of the faulty memory block. For this purpose, the algorithm is introducing a generation based memory management. In the first generation are memory blocks without any occuring error. The second generation are memory blocks that are classified as suspicious and the memory blocks get verified more frequently. This prevents that memory blocks are getting excluded because of external events such as soft errors. In the third generation are memory blocks placed that are not reliable enough anymore and are excluded from storing data.

2) Efficient and Effective Resolution Adaption: One of the most effective ways of reducing computational utilization is about reducing raw pixel data. For this purpose, the novel system architecture is reducing the amount of pixels by skipping a specific amount of pixels as depicted in Figure 6. The system is able to automatically degradate the resolution between the factor one to four. The main focus from a safety point of view was to still provide enough information inside the image that computer vision algorithm are still able to interpret the data in a correct way as seen in Figure 7. Additionally, the system is not able to reduce the resolution in each situation. In specific situations, such as driving in an overcrowded city the system should not be able to reduce the pixels on purpose. Just in emergency cases, if the system would otherwise result in a total failure a degradation is allowed. In other non safety-critical cases like driving on a highway the system is allowed to reduce the resolution on purpose. This guarantees a safe behavior for passengers as well as other road participants.

B. Integrated Testing Functions

1) Realistic Scenario Simulations: Testing is necessary to provide information about reliability and utilization of hardware components. Nowadays, most of these tests are performed by statistical tests in which specific road types are mapped to a specific time. In the near future, these tests can be advanced to more sophisticated real data scenarios that can be obtained by using data from the European eCall system or similar systems that are able to provide GPS data. These data sets can be used to test the real utilization of the hardware components and enable more precise optimization of specific components with the positive side-effects of reducing ressource usage and costs.

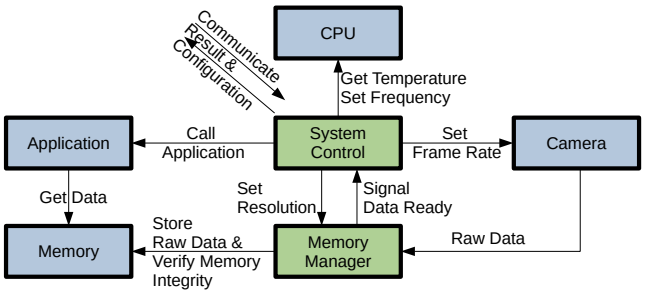

Fig. 4. Overview of the novel fail-operational 3D Flash Lidar system architecture.

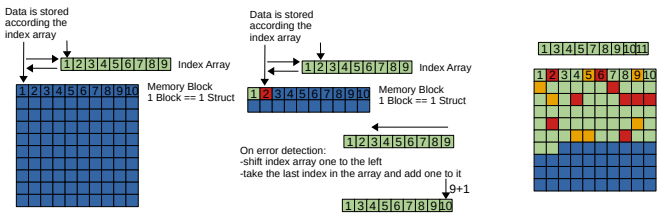

Fig. 5. Concept of the preserving memory fault system architecture that has been integrated in the novel fail-operational 3D Flash Lidar platform.

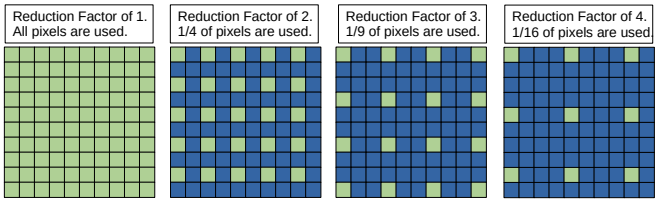

Fig. 6. Overview of the efficient and effective resolution adaption algorithm that is implemented in the novel fail-operational 3D Flash Lidar system.

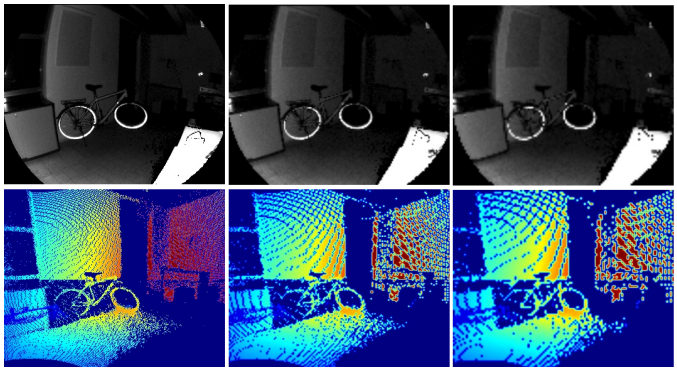

Fig. 7. Adaptive resolution example containing grey images and depth information images of the 3D Flash Lidar system of a bicycle scene. The resolution is reduced from 352x287 (left photo) to 118x96 (right photo).

For this reason, our novel system architecture is able to test real-life usage scenarios in which road trips can be defined and virtually driven. The system will automatically change the configuration of the 3D Flash Lidar system based on the actual road type. This enables the testing of the system in real scenarios to increase the trustiness of the resulting reliability estimation.

2) Memory Fault Injection: Memory is necessary to store data from the sensors as well as computational results. The integrity of the stored values inside volatile memory is crucial for correct computation and reliable quality of the output results. If individual memory blocks get corrupted over time results in an unpredictable behavior of the whole system. For that reason, the novel system architecture has built-in a memory fault injection module that is able to disable a variety of memory blocks as seen in Figure 5. This enables us to verify the degradation and fail-operational behavior functions of the novel system.

C. Graphical Control Interface

The novel system-architecture offers a TCP/IP interface which offers a service providing environmental perception data

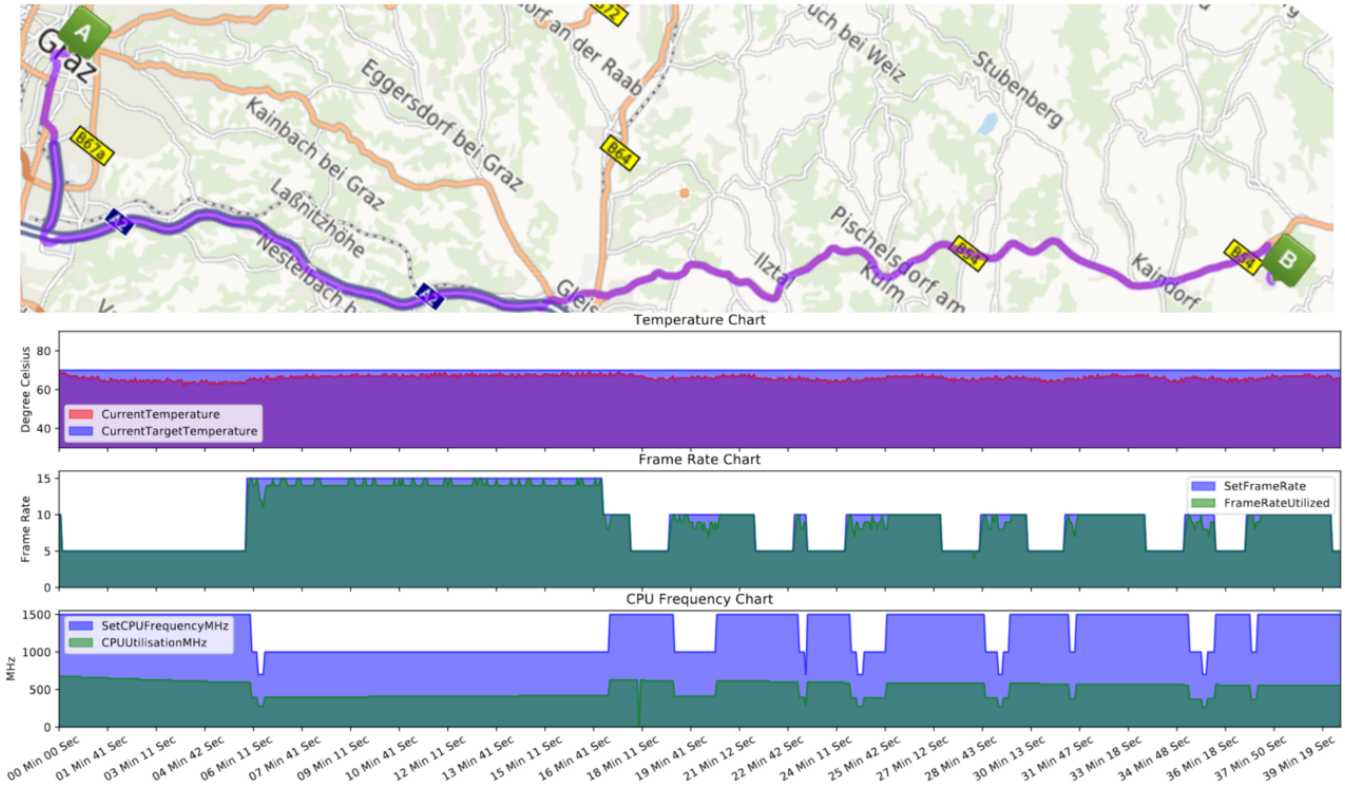

Fig. 8. Test run of a an average commuter route between Graz and Hartberg and the related monitoring data.

as well as monitoring data to external systems. As a client we have developed a Graphical Control Interface (GCI) as seen in Figure 3 that displays the current live data from the 3D Flash LiDAR system as well as current safety-critical sensor values such as temperature, frame rate, memory usage, and CPU frequency. The GCI also provides settings for testing specific usage scenarios of the whole platform to derive behavioral patterns such as temperature trends and CPU throttling.

IV. Results

This Section describes the results of the novel fail-operational 3D Flash Lidar system architecture that enables the degradation of the environmental perception functionality and enables a safe driving for SAE Automated Driving Level 4 vehicles.

Figure 3 clearly depicts the graphical monitoring system of the novel implemented system-architecture. On the left side, the current environmental perception data (Depth Image and Gray Image) can be seen and is continously updating with a specific frame rate. The target frame rate can be specified in the upper section of the GCI as well as the maximal targeted temperature and the preferred resolution including the minimum allowed resolution. This resolution can be adapted according driving scenarios such as urban areas or highways. Additionally the framework allows to ingore individual parameters such as temperature, resolution or frame rate. In the middle section of the GCI the current sensor values of the overal system architecture temperature, frame rate of the live 3D Flash LiDAR data, CPU frequency and memory usage can be seen. On the right side is the memory fault injection module that is able to disable a specific amount of memory blocks for testing degradation and fail-operational behavior considering memory faults.

The novel system architecture was tested with the integrated realistic scenario simulation with a virtual test run between Graz and Hartberg. The route was separated into specific sections with meta information about road type and speed limit. Generally these values would be provided by additional ADAS that are common available in middle-class cars nowadays.

In Figure 8 the route is shown on a map as well as the resulting monitoring results of the test run. The main focus in this scenario was the strict adherence of the specific system architecture temperature of 70°C because temperature is one of the most crucial parameters for reliability. Higher temperature directly results in lower reliability and higher FIT Rates. Higher FIT Rates could potentially degrade the overall Automotive Safety Integrity Level. The temperature diagram clearly depicts that this limit was strictly adhered by the system architecture by dynamically adapting the CPU frequency of the computation platform as well the frame rate of the 3D Flash LiDAR sensor.

V. Conclusion

In this publication we have introduced a novel fail-operational 3D Flash LiDAR system architecture. The architecture enables the system to dynamically adapt specific

parameters to strictly adhere safety-critical parameters such as temperature.

In Section III we have described the general system-architecture and implemented built-in self tests. Considering the last trends in the automotive industry of using EMMC memory and the resulting faults [23] we have integrated a memory fault injection module that is able to simulate faults in multiple memory blocks to test the direct and indirect impacts of these failures. The resulting degradation of the system by adapting the environmental perception data resolution shows that the scene still could be properly interpreted by higher level computer vision algorithms as seen in Figure 6.

The test scenario of an average commuter route test run between Graz and Hartberg that is described in Section IV clearly indicates the effective performance of the dynamic degradation of the platform considering specific safety-critical parameters. In this case, we have set the limit of the general system architecture temperature range because this is one of the most crucial parameters for reliability for hardware components.

In the next few years, vehicles will perform the transformation from SAE Automated Driving Level 3 to 4 and this will require higher safety standards because of the absence of a human driver that is able to retake the driving control. For this reason, reliability and fail-operational behavior will become to the most important parameters for the general safety of road vehicles. The novel introduced fail-operational 3D Flash LiDAR system architecture proves feasibility and gives an overview of a possible solution for safety-critical environmental perception sensors such as LiDAR.

VI. Acknowledgments

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] 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.

[2] I. n. E. ISO, "Draft 26262 2nd Edition: Road vehicles-Functional safety," *International Standard ISO/FDIS*, vol. 26262, 2018.

[3] H. Plank, T. Egger, C. Steffan, C. Steger, G. Holweg, and N. Druml, "High-performance indoor positioning and pose estimation with time-of-flight 3d imaging," in *2017 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, Sep. 2017, pp. 1–8.

[4] J. Dokic, B. Müller, and G. Meyer, "European roadmap smart systems for automated driving," *European Technology Platform on Smart Systems Integration*, p. 39, 2015.

[5] S. Tokoro, K. Kuroda, A. Kawakubo, K. Fujita, and H. Fujinami, "Electronically scanned millimeter-wave radar for pre-crash safety and adaptive cruise control system," in *IEEE IV2003 Intelligent Vehicles Symposium. Proceedings (Cat. No. 03TH8683)*. IEEE, 2003, pp. 304–309.

[6] J. Hecht, "Lidar for self-driving cars," *Optics and Photonics News*, vol. 29, no. 1, pp. 26–33, 2018.

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

[8] M. Kyriakidis, J. C. de Winter, N. Stanton, T. Bellet, B. van Arem, K. Brookhuis, M. H. Martens, K. Bengler, J. Andersson, N. Merat *et al.*, "A human factors perspective on automated driving," *Theoretical Issues in Ergonomics Science*, vol. 20, no. 3, pp. 223–249, 2019.

[9] A. Kohn, M. Käßmeyer, R. Schneider, A. Roger, C. Stellwag, and A. Herkersdorf, "Fail-operational in safety-related automotive multi-core systems," in *10th IEEE International Symposium on Industrial Embedded Systems (SIES)*, June 2015, pp. 1–4.

[10] N. Druml, O. Veledar, G. Macher, G. Stettinger, S. Selim, J. Reckenzaun, S. E. Diaz, M. Marcano, J. Villagra, R. Beekelaar, J. Jany-Luig, M. M. Corredoira, P. Burgio, C. Ballato, B. Debaillie, L. van Meurs, A. Terechko, F. Tango, A. Ryabokon, A. Anghel, O. Icoglu, S. S. Kumar, and G. Dimitrakopoulos, "Prystine - technical progress after year 1," in *2019 22nd Euromicro Conference on Digital System Design (DSD)*, Aug 2019, pp. 389–398.

[11] N. Yulianto, B. Widiyatmoko, and P. S. Priambodo, "Temperature effect towards dfb laser wavelength on microwave generation based on two optical wave mixing," *Int. J. Optoelectron. Eng.*, vol. 5, no. 2, pp. 21–27, 2015.

[12] I. Maksymova, C. Steger, and N. Druml, "Extended delta compression algorithm for scanning lidar raw data handling," *International Conference on Intelligent Robots and Systems*, 2019.

[13] I. Maksymova, N. Druml, and C. Steger, "Review of lidar sensor data acquisition and compression for automotive applications," in *Multidisciplinary Digital Publishing Institute Proceedings*, vol. 2, no. 13, 2018, p. 852.

[14] S. Han, Y. Wang, S. Liang, S. Yao, H. Luo, Y. Shan, and J. Peng, "Reconfigurable processor for deep learning in autonomous vehicles," 2017.

[15] Intel, "Intel Atom Processor E3900 and A3900 Serie Datasheet," 2019.

[16] R. Baumann, "Soft errors in advanced computer systems," *IEEE Design Test of Computers*, vol. 22, no. 3, pp. 258–266, May 2005.

[17] C.-L. Chen and M. Hsiao, "Error-correcting codes for semiconductor memory applications: A state-of-the-art review," *IBM Journal of Research and development*, vol. 28, no. 2, pp. 124–134, 1984.

[18] A. H. Johnston, "Scaling and technology issues for soft error rates," 2000.

[19] B. Schroeder, E. Pinheiro, and W.-D. Weber, "Dram errors in the wild: a large-scale field study," *ACM SIGMETRICS Performance Evaluation Review*, vol. 37, no. 1, pp. 193–204, 2009.

[20] I. E. Comission, "IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems," 2009.

[21] T. Ishigooka, S. Honda, and H. Takada, "Cost-effective redundancy approach for fail-operational autonomous driving system," in *2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC)*, May 2018, pp. 107–115.

[22] F. Oszwald, J. Becker, P. Obergfell, and M. Traub, "Dynamic reconfiguration for real-time automotive embedded systems in fail-operational context," in *2018 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*, May 2018, pp. 206–209.

[23] T. Nardi, "Worn Out EMMC Chips Are Crippling Older Teslas," Oct 2019. [Online]. Available: https://hackaday.com/2019/10/17/worn-out-emmc-chips-are-crippling-older-teslas/