Live State-of-Health Safety Monitoring for Safety-Critical Automotive Systems

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

***Abstract*—Autonomously driving vehicles require higher safety and reliability standards than traditional human-driven vehicles as they need to be able to handle safety-critical situations on their own. Therefore, these systems needs to demonstrate fail-operational behavior to ensure safety of the passengers by basic car controls. Especially silent failures of semiconductor devices can be critical from a safety point of view. Semiconductor devices fail abruptly and cannot be detected in advance.**

This paper presents a novel sensor approach to detect those kind of silent failures ahead of time and to ensure safety for future advanced driver-assistance systems (ADAS) such as LiDAR (Light Detection and Ranging). We have evaluated the design of our novel sensor concept in SystemC which will be implemented in a LiDAR system to mitigate silent failures as well as enable dynamic safety contracts.

***Keywords*-Safety, Safety Monitoring, Aging Monitor, Component Reliability, Safety Integrated Circuits, Live FIT Estimation**

I. Introduction

Autonomous driving is one of the next big steps of our society and is the key enabler of Smart Mobility [1]. Smart Mobility reinvents the urban environment by connecting infrastructure, vehicles and people to allow better quality of life, efficient energy usage and reduced costs for everyone. As a result, this era will disruptively change the daily routines of individuals as well as urban life [2]. 50 years ago, the idea of Smart Mobility started in Germany when Continental, a leading German automotive manufacturing company, tested tires on their test track Contidrom. Continental wanted to ensure constant conditions for testing and developed a self-driving car for this purpose [3]. This marked the beginning of autonomous driving. Nowadays, self-driving cars have already made their way to public streets. Tesla was the first company to release a semi-autonomous driving function called "Autopilot" [4]. Past accidents showed that it is hard to ensure safe semi-autonomous driving in urban environments by traditional methods [5]–[7]. Consequently, new Advanced Driver-Assistance Systems (ADAS) such as LiDAR (Light Detection and Ranging) need to be developed and combined with established systems. This is also the PRYSTINE (Programmable Systems for Intelligence in Automobiles" project's focus which aims at developing a comprehensive environment perception system by using LiDAR, radar and vision cameras as shown in figure 1 [1]. One of the key challenges of autonomous driving is safety and reliability of before mentioned systems. Traditional human-driven vehicles are fully - or supported by ADAS almost fully - controlled by the driver. Therefore, the system can return control and responsibility to the driver in critical situations. In future, vehicles with fully autonomous driving functionality will not have this possibility and need to be able to deal with critical situations on their own. That's one of the reasons why the impact of safety and reliability in the automotive domain is steadily increasing [8].

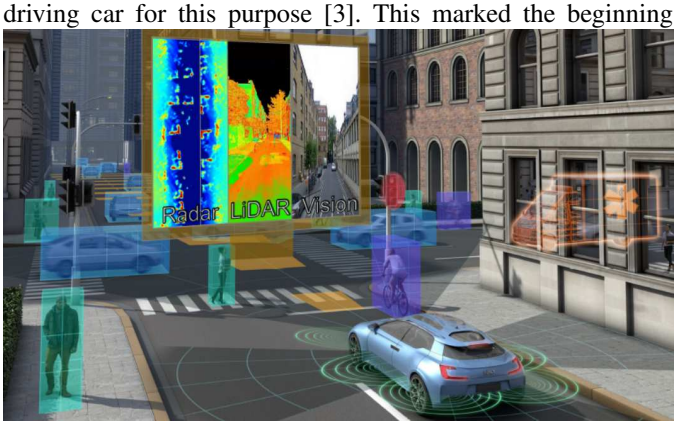

Fig. 1. PRYSTINE's concept view of a fail-operational urban surround perception system [1].

Nowadays, safety-critical automotive systems are developed in compliance with the ISO 26262 standard. This standard covers the development of electrical and electronic components for the automotive domain with a special focus on safe hardware and software components [9]. The standard added a guideline especially for semiconductor devices but does not support or cover dynamic safety functions such as "Conserts M" or "Ontology-Based-Run-time-Reconfiguration". Dynamic safety functions are necessary to establish resilience and flexibility to complex cyber-physical systems (CPS) [10]. Especially for future ADAS, such as the fail-operational urban surround perception system of the PRYSTINE project, this concept is vital to ensure fail-operational behavior during runtime.

Fail-operational systems require information about the common reliability and safe state of each system. Up to now, there is no possibility to retrieve live information about component reliability. Usually, components are designed for a specific utilization profile and safety is dimensioned for this profile. If there are substantial deviations to this profile, components could be undersized from a safety point of view [9]. It

would be beneficial to enable live monitoring of semiconductor devices' component reliability to communicate the state-of-health of individual components.

This paper will address the following research questions:

- Is it possible to detect component reliability of semiconductor systems during run-time?
- How can component reliability be measured for semiconductor devices?

II. Related Work

In general, detecting safety-related issues of mechanical components is rather trivial as it often involves vibration or noise during the operation [11]. For electrical or electronic components, detecting safety-related issues is much more complex. These systems fail silently and abruptly [9]. Especially for fully-autonomous vehicles, this fact poses a substantial risk as these systems need to handle every safety-critical situation on their own and any failure could trigger fatal road accidents. If we consider tucks carrying ecologically harmful substances, accidents may also lead to environmental disasters.

In general, designers of safety-critical semiconductor devices construct and dimension components for specific utilization profiles. These profiles cover the worst case utilization of the component to ensure component reliability during lifetime. Especially for semiconductor companies that design "Safety Elements out of Context", this design philosophy is difficult as they need to find the best compromise between cost and reliability. Overdimensioning hardware leads to higher costs, which may be the decisive factor for making business or not.

Nowadays, every semiconductor device contains additional safety-related monitoring circuits. For digital circuits, common monitors are error correction codes (ECC) or Built-In-Self-Test (BIST), analog circuits use monitors such as the Built-In-Current Sensor (BICS). These monitors mitigate specific problems: For instance, ECC control single event upsets (SEU), BIST checks correct functionality [9]. Shaheen et al. [12] describe common ECC practices in the automotive domain such as Parity Bit, Single Error Correction, Single Error Correction and Detection to detect and correct SEU during run-time [12]. Sargsyan [13] describes different BIST technologies that ensure correct functionality of digital semiconductor devices such as Production Mode Testing, Power-on Mode Testing and Mission Mode Testing. These tests are executed at startup or during idle time and compare the result with deposited patterns [13]. For analog circuits, Smith et al. describe the BICS that can detect current leakage [14]. Beckler et al. [15] introduce the On-Chip Diagnosis for early life and wear-out failures [15]. All these approaches only focus on testing the specific circuit's functionality in a specific moment and can not give any information on the current state-of-health. Therefore, it is necessary to have historical data about the device such as temperature, for instance. Szekely et al. [16] introduce a sensor for on-line temperature monitoring of safety-critical Integrated Circuits (IC). However, this sensor focuses on observing and communicating current temperature to external systems but does not cover temperature history [16]. Especially temperature history has a big impact on component reliability and needs to be considered from a safety point of view because higher temperature relates to higher component stress and this negatively influences the reliability.

Component reliability is one of the key requirements for safety-critical hardware devices. Nowadays, the automotive industry's approved safety methods are compiled in the ISO 26262 standard [9]. In general, these methods quantify hardware devices' component reliability in the failure in time (FIT) Rate. The FIT Rate represents the amount of failures that statistically arises within one billion operating hours. The FIT Rate is calculated or statistically determined by specific standards such as the IEC TR 62380 [17]. Usually, each semiconductor manufacturer publishes the specific FIT Rates for their devices in the component reliability data sheet [18]. These data sheets usually provide the FIT Rate for a specific test temperature which can be used to calculate equivalent FIT Rates for specific temperatures using the Arrhenius equation as seen in (1).

$$DF = e^{\frac{E_a}{k} \cdot (\frac{1}{T_{use}} - \frac{1}{T_{stress}}))} \tag{1}$$

where:

DF	is Derating Factor
E_a	is Activation Energy in eV
k	is Boltzmann Constant (8.167303 x 10^{-5} ev/K)
T_{use}	is Use Junction Temperature in K
T_{stress}	is Stress Junction Temperature in K

The Derating Factor (DF) represents the positive or negative feedback of the specific temperature on the semiconductor device and depends on the Junction Temperatures that need to be determined with equation (2).

$$T_j = T_{amb} + P_{dis} \cdot \theta_{ja} \tag{2}$$

where:

T_{amb}	is Ambient Temperature
P_{dis}	is Power Dissipation
θ_{ja}	is Package Thermal Resistance Value

Equation (2) shows that the component reliability depends on the power dissipation as well as on the ambient temperature of the integrated circuit. The Derating Factor can be used for calculating the specific FIT Rate for a specific temperature as seen in (3).

$$FIT_{Base} = DF \cdot FIT_{DS} \tag{3}$$

where:

DF	is Derating Factor as seen in (1)
FIT_{DS}	is Base FIT Rate of Component Reliability Data sheet

The idea of Beckler et al. [15] and Szekely et al. [16] with these equations could be used for live component reliability monitoring.

Therefore, this paper's contribution to existing research is:

- Developing a novel method for enabling live safety monitoring of safety-critical automotive systems.

- Implementing the novel method in SystemC to prove feasibility.
- Describing the integration of the novel method in a safety-critical LiDAR sensor system for autonomous driving.

III. Use Case Overview

Self-driving vehicles handle safety-critical situations on their own without any control of a driver. Consequently, a high safety and reliability standard is necessary to ensure fail-operational behavior. In the next few years LiDAR will become common in middle-class cars and will be an important part of self-driving functionality [19]. LiDAR is an environment perception systems in combination with Radar and Vision [1].

The 1D MEMS LiDAR system of Druml et al. [19] is a novel approach to develop an inexpensive ADAS that is suitable for the mass. Novel technologies are always related to unknown failures [11]. Especially in the domain of self-driving cars, these failures are not tolerable because they result in severe road accidents.

To increase the learning curve and to evolve safer and more reliable LiDAR systems as fast as possible, component reliability should be monitored live to get real-time data of a single vehicle as well as of a complete fleet. This will enable functions that increase the overall safety level of an individual driver as well as the overall road safety. Both scenarios will be described in our use case that is divided into two sections:

- Live Reliability Data for Customers
- Live Reliability Data for Original Equipment Manufacturer (OEM)/Suppliers

A. Live Reliability Data for Customers

The reliability data of a single vehicle can be used to determine the overall usage level of a specific system as well as of the complete car. This could be used for enabling predictive maintenance like in the aircraft industry. If a specific FIT Rate is reached and the safety-critical device is dropping in the Automotive Safety Integrity Level (ASIL), this could trigger the replacement of the specific device. Especially for self-driving cars this approach could ensure a specific safety level of all self-driving road vehicles.

Another use case is the review of the complete car if individual maintenance repairs are worth to accomplish. If a certain amount of systems has reached a specific FIT Rate, this would suggest that these systems will also fail in the next few months. This will support the customer during his decision, if a repair is useful or not.

B. Live Reliability Data for OEM/Supplier

For OEMs and suppliers, the reliability data is valuable to understand whether the systems are designed for their use cases and whether there are any problems that could arise during warranty time. By using real-time data, suppliers can interfere to adapt the software parts of the devices to ensure a specific FIT Rate until the end of lifetime.

Especially software updates are changing the behavior of devices and may have a big impact on the overall safety level. By collecting reliability data of these live monitors, it will be possible to investigate and evaluate changes of these updates from a safety point of view.

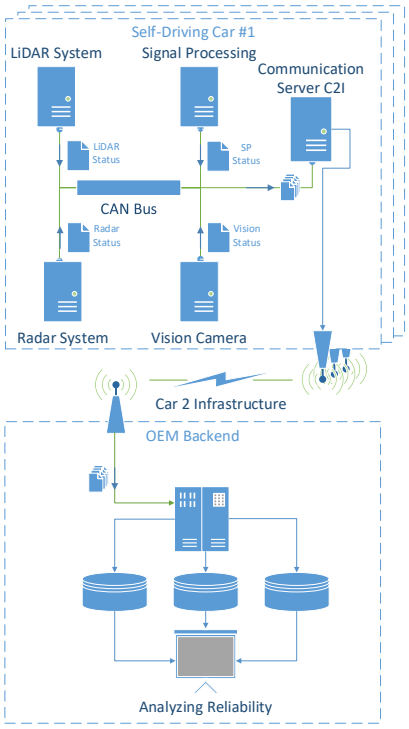

Fig. 2. Use case overview of the live FIT Monitor for safety-critical LiDAR sensor systems.

IV. RetroFIT - Live Safety Monitoring Sensor

$$DF = e^{\frac{E_a}{k} \cdot (\frac{1}{T_{use}} - \frac{1}{T_{amb} + P_{dis} \cdot \theta_{ja}})} \quad (4)$$

By combining both equations of the Related Work on component reliability, it becomes obvious that it is possible to calculate the theoretical FIT Rate for a specific temperature as seen in (3). However, component temperature is changing over time which results in different FIT Rates. Therefore, considering these temperature profiles as a time slice in a whole mission profile [9] will be used and integrated in our novel approach of live safety monitoring.

The idea behind our novel approach is to sample the power dissipation and the actual case temperature at a specific time interval. The power dissipation measurements are averaged and saved in a register which represents the average power dissipation of the whole lifetime. The temperature values are classified in a specific temperature range and integrated in a histogram. This histogram represents the whole temperature history of the integrated circuit during lifetime and can be used for further component reliability computations.

For calculating the FIT Rate at a specific time, the following steps are necessary:

1) Calculate FIT Rate for each Histogram Bin
2) Determine the time span percentage of each Histogram Bin
3) Calculate the FIT Rate for each Histogram Bin

4) Sum up each individual Bin FIT Rates to the overall FIT Rate
5) Determine and check with theoretical lifetime FIT Rate

A. Calculate FIT Rate for each Histogram Bin

Each Histogram Bin represents a specific temperature. In our case, we chose a temperature range between $0°C$ and $140°C$. For each Bin, the specific FIT Rate can be calculated by using equation (3) and (4). These FIT Rates represent the statistical lifetime FIT Rate assuming this device would run on this specific temperature for the whole lifetime.

B. Determine the time span percentage of each Histogram Bin

As a first step, the run-time of the device until this moment is determined. For this purpose, all samples of the whole Histogram are summed up as seen in (5).

$$T_{OR} = \frac{\sum n \cdot T_{SR}}{3600} \tag{5}$$

where:

T_{SR} is sampling rate of the measurements.

The overall run-time can be used to determine the specific amount of run-time for each Histogram Bin as seen in (6).

$$T_{Run} = \frac{T_{SR}}{3600 \cdot T_{OR}} \cdot n \tag{6}$$

where:

T_{SR} is sampling rate of the measurements.
T_{OR} is the whole run-time of the device as calculated in (5).

The equation (6) is used to calculate the run-time for each Histogram Bin. In the next step, the specific FIT Rate considering the specific run-time is calculated.

C. Calculate the FIT Rate for each Histogram Bin

In the next step, the FIT Rate of the whole lifetime of each Histogram Bin is calculated.

$$FIT_{Bin} = \frac{FIT_{RB}}{T_{EL}} \cdot T_{Run} \tag{7}$$

where:

FIT_{RB} is FIT Rate of the specific temperature of the Bin as calculated in (4).
T_{Run} is the whole run-time of the device as calculated in (5).
T_{EL} is the expected lifetime of the semiconductor device that has been selected during design phase.

D. Sum up each individual Bin FIT Rates to the overall FIT Rate

In the last step, all individual FIT Rates of the Bins are summed up to an overall FIT Rate.

$$FIT_{TS} = \sum FIT_{Bin} \tag{8}$$

where:

FIT_{Bin} is FIT Rate of each Bin as calculated in (7).

This value represents the FIT Rate to this specific timestamp and can be compared to the theoretical FIT Rate up to this timestamp as well as the theoretical FIT Rate until the end of the expected lifetime.

E. Determine and check with theoretical lifetime FIT Rate

In the last step, we observe if the FIT Rate of the current timestamp exceeds the theoretical FIT Rate that was chosen during design phase.

$$FIT_{TTS} = FIT_{DS} \cdot \frac{T_{OR}}{T_{EL}} \tag{9}$$

where:

FIT_{DS} is theoretical FIT Rate for a specific temperature as seen in (4).
T_{OR} is run-time of the device until this timestamp as seen in (6).
T_{EL} is the expected lifetime of the semiconductor device that has been selected during design phase.

The ratio between the theoretical FIT Rate and the calculated FIT Rate gives a tendency about the usage of the device and whether there should be any concern due to predicted over-stress until the end of the lifetime.

$$FIT_{Ratio} = \frac{FIT_{TS}}{FIT_{TTS}} \tag{10}$$

Ratios that are greater than one indicate that the device was used too extensively and that there could be over-stress until the end of the expected lifetime. This also increased the theoretical amount of failures until the end of the lifetime. The amount of statistical failures can be determined with equation (11).

$$FIT_{LT} = FIT_{TS} \cdot \frac{T_{EL}}{T_{OR}} \tag{11}$$

where:

FIT_{TS} is the calculated FIT Rate for a specific timestamp as seen in (8).
T_{OR} is run-time of the device until this timestamp as seen in (6).
T_{EL} is the expected Lifetime of the semiconductor device that has been selected during design phase.

V. Results

We will implement the "RetroFIT" method in a LiDAR system as seen in Figure 3. To evaluate the functionality and behavior of this methodology we implemented this approach in SystemC.

In Figure 4 the architecture of the implemented FIT Monitor can be seen. The architecture consists of the "Environmental and Integrated Circuit Simulation Model" that contains the temperature profile (as seen in Figure 5) curve that will stimulate the FIT Monitor. The histogram will save each sampled value of the temperature as well as the average power dissipation. The last part is the signal processing where the FIT Rates are calculated as described in Section IV. In Figure 5 the upper diagram is showing temperature profile that have been

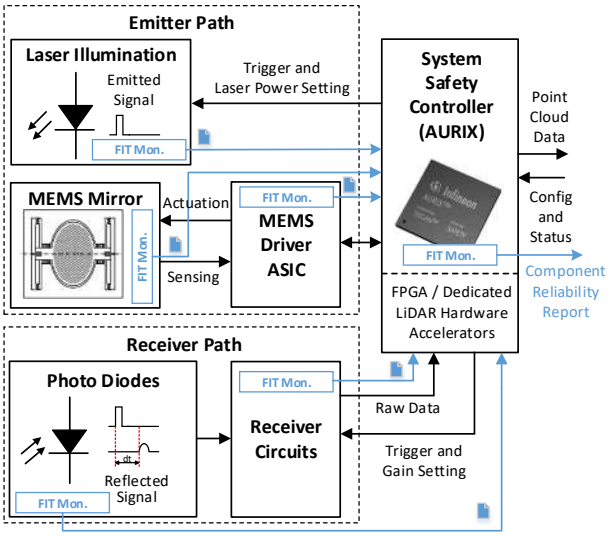

Fig. 3. Live FIT Monitor integration into the safety-critical LiDAR sensor system to enable live safety monitoring [19].

used for our simulation. The lower diagram shows the specific temperature values for each sampling point. In our simulation we have sampled with a frequency of 0.05 Hertz. The related Histogram of our simulation can be seen in Figure 6. Each Histogram Bin represents a 1°C and is distributed on the x-Axis. The amount of samples can be read out on the y-Axis. In our simulation the most samples could be found between 100°C and 110°C. Compared with the temperature profile of Figure 5 this looks plausible.

TABLE I
FIT RESULTS OF OUR SYSTEMC MODEL SIMULATION WITH TEMPERATURE PROFILE INPUT AS SEEN IN FIGURE6.

	FIT_{TS}	FIT_{TTS}	FIT_{LT}	FIT_{RB}	FIT_{Ratio}
FIT in [1]	2.36E-9	2.111E-9	8.5	7.6	1.118

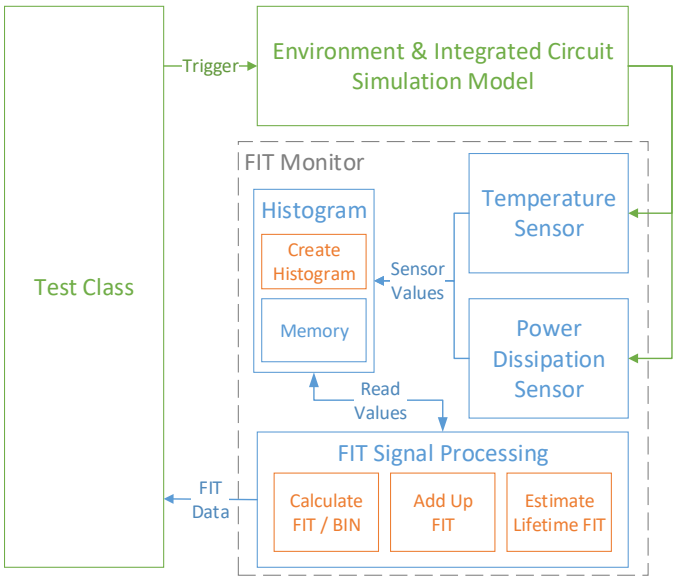

Fig. 4. SystemC model overview of the "RetroFIT" methodology to enable live safety monitoring for safety-critical LiDAR sensor systems.

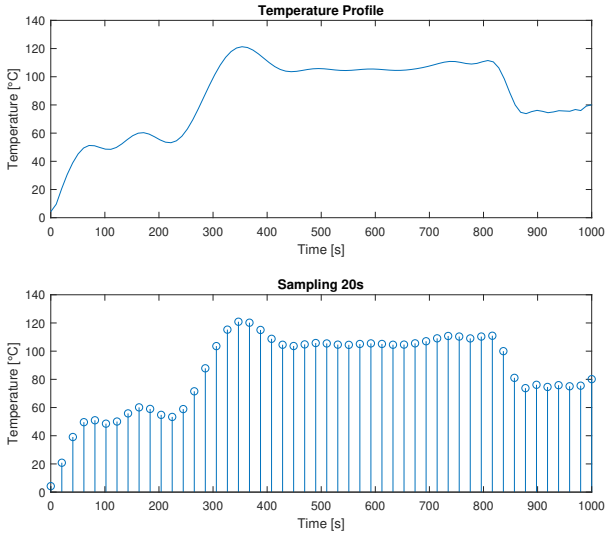

Fig. 5. Measurement results of the "RetroFIT" monitor.

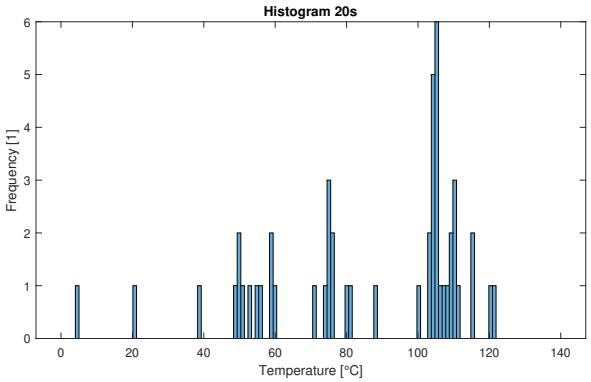

Fig. 6. Histogram results of the "RetroFIT" monitor.

In Table I the FIT results of our SystemC simulation can be seen. The device has an FIT_{RB} value of about 7.6 in 1 Billion operating hours at 100°C. The provided temperature profile, as seen in 5, over-stresses the component and this results in a higher FIT_{LT} of about 8.5. As a result the device has been over-stressed by 11.8%. Consequently, a continuously operated device with this temperature profile would result in a higher FIT Rate than from the designer of the device expected.

VI. SUMMARY

In Section IV, this paper introduces the novel "RetroFIT" sensor to support live safety monitoring of electrical and electronic devices. Nowadays, electronic components such as sensors and micro-controllers fail without any prior indication. Especially for fully automated driving, this circumstance may cause disastrous consequences such as deadly accidents. For future autonomous driving vehicles, our novel method can communicate the actual component reliability.

To give an overview about the application of our novel sensor, we have introduced two common use cases from the customer point of view as well as from the OEM/Supplier point of view. Both cases show that "RetroFIT" has a big impact on the overall road safety as the sensor may for instance trigger component replacement. The values could be obtained

by qualified car repair shops as well as displayed inside the driver's cabin including service deactivation.

In section V, we prove that the sensor concept is feasible and that it is possible to live monitor component reliability for electronic devices.

Fail-operational systems become increasingly essential. Our novel "RetroFIT" sensor enables dynamically changing contracts during run-time. This concept is one of the key enablers of advanced fail-operational systems. Our sensor enables the communication of the actual ASIL level of components and communicates these values to other systems. This will detect ASIL degradation during run-time and trigger safety related functions to increase the overall system safety.

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] R. Faria, L. Brito, K. Baras, and J. Silva, "Smart mobility: A survey," in *2017 International Conference on Internet of Things for the Global Community (IoTGC)*, July 2017, pp. 1–8.

[3] Mmpro. [Online]. Available: https://publicarea.admiralcloud.com/p/a49d3d8ba92f3cdbfa864f

[4] M. Dikmen and C. Burns, "Trust in autonomous vehicles: The case of tesla autopilot and summon," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Oct 2017, pp. 1093–1098.

[5] "Accident investigations." [Online]. Available: https://www.ntsb.gov/investigations/Pages/HWY18FH011.aspx

[6] F. Lambert, Fred, and Electrek, May 2018. [Online]. Available: https://electrek.co/2018/05/09/tesla-model-s-fatal-crash-fire-national/

[7] S. Levin, "Tesla fatal crash: 'autopilot' mode sped up car before driver killed, report finds," Jun 2018. [Online]. Available: https://www.theguardian.com/technology/2018/jun/07/tesla-fatal-crash-silicon-valley-autopilot-mode-report

[8] R. Mariani, "An overview of autonomous vehicles safety," in *2018 IEEE International Reliability Physics Symposium (IRPS)*, March 2018, pp. 6A.1–1–6A.1–6.

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

[10] T. Amorim, D. Ratasich, G. Macher, A. Ruiz, D. Schneider, M. Driussi, and R. Grosu, "Runtime safety assurance for adaptive cyber-physical systems: Conserts m and ontology-based runtime reconfiguration applied to an automotive case study," in *Solutions for Cyber-Physical Systems Ubiquity*. IGI Global, 2018, pp. 137–168.

[11] N. Leveson, *Engineering a safer world: Systems thinking applied to safety*. MIT press, 2011.

[12] H. Shaheen, G. Boschi, G. Harutyunyan, and Y. Zorian, "Advanced ECC solution for automotive SoCs," in *2017 IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS)*, July 2017, pp. 71–73.

[13] D. Sargsyan, "Iso 26262 compliant memory bist architecture," in *2017 Computer Science and Information Technologies (CSIT)*, Sept 2017, pp. 78–82.

[14] P. A. Smith and D. V. Campbell, "A practical implementation of bics for safety-critical applications," in *Proceedings 2000 IEEE International Workshop on Defect Based Testing (Cat. No.PR00637)*, April 2000, pp. 51–56.

[15] M. Beckler and R. D. Blanton, "On-chip diagnosis for early-life and wear-out failures," in *2012 IEEE International Test Conference*, Nov 2012, pp. 1–10.

[16] V. Szekely, M. Rencz, J. M. Karam, M. Lubaszewski, and B. Courtois, "Thermal monitoring of safety-critical integrated systems," in *Proceedings of the Fifth Asian Test Symposium (ATS'96)*, Nov 1996, pp. 282–288.

[17] T. IEC, "62380," *Reliability data handbook–universal model for reliability prediction of electronics components, PCBs and equipment (emerged from UTEC 80-810 or RDF 2000)*, 2004.

[18] "Reliability report," Jul 2018. [Online]. Available: https://www.intel.com/content/www/us/en/programmable/support/quality-and-reliability/reports-tools/reliability-report/rel-report.html

[19] 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.