FITness Assessment
Hardware Algorithm Safety Validation

Andreas Strasser, Philipp Stelzer, Christian Steger

Graz University of Technology
Graz, Austria
Email: {strasser, stelzer, steger}@tugraz.at

Norbert Druml

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

***Abstract*—Error Correction Codes (ECC) are important safety methods for digital data to gain control of Single Event Upsets (SEU) in integrated digital circuits. SEU are responsible for single bit flips inside a digital circuit caused by ionizing radiation. This effect does not affect the physical structure of the components but the correctness of data inside flip flops. Consequently, data gets corrupted and the correct program flow gets disturbed. This effect needs to be considered especially for safety-critical systems. In the new ISO 26262 2nd Edition, the automotive domain suggests controlling SEU effects by algorithms that correct Single Bit Errors and Detect Double Bit Errors (SEC-DED). This raises the question what kind of impact Double Bit Error Correction (DEC) will have on the overall safety level for LiDAR (Light Detection and Ranging) systems. In this publication, we determine the difference between two ECC algorithms from a safety point of view: Hamming's code (SEC-DED) and Bose–Chaudhuri–Hocquenghem-Code (DEC). For this purpose, we developed a novel method for algorithm safety validation and applied it to both algorithms.**

Keywords*–*Safety Validation FPGA, Failure-in-Time Analysis FPGA, Error Correction Codes, ISO 26262 2nd Edition, Algorithm Validation.

I. Introduction

Fully autonomous driving will change our society, as well as individuals's daily routines and will improve overall road safety. To achieve the goal of autonomous driving, novel Advanced Driver-Assistance Systems (ADAS) are necessary. The two best-known ADAS are the Electronic Stability Control and the Anti-Lock Braking System, especially for their positive effect on active safety. Moreover, in the last years, a new generation of ADAS such as the Adaptive Cruise Control (ACC) has been established in middle class cars to avoid collisions. The next big step is introducing a comprehensive system enabling the perception of urban environment, which is one of the main goals of the PRYSTINE project [1].

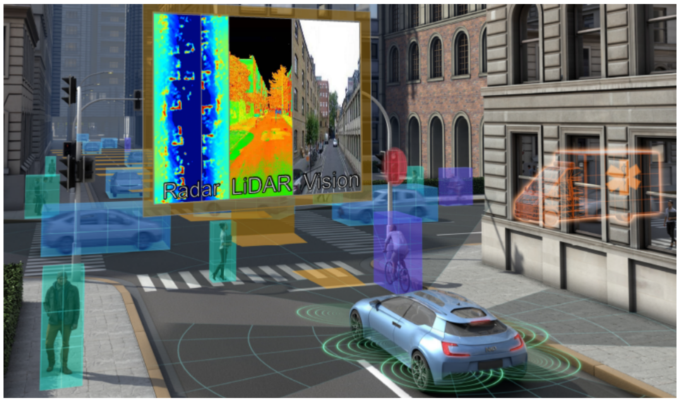

Figure 1. PRYSTINE's concept view of a fail-operational urban surround perception system [1].

PRYSTINE stands for Programmable Systems for Intelligence in Automobiles and is based on robust Radar and LiDAR sensor fusion to enable safe automated driving in urban and rural environments, as seen in Figure 1. These devices must be reliable, safe and fail-operational to handle safety-critical situations independently [1]. In contrast to Radar, LiDAR has not been implemented in middle class cars yet but there are basic approaches in the automotive industry such as the 1D MEMS Micro-Scanning LiDAR system as seen in Figure 2 [2]. This modern LiDAR system consists of an emitter and receiver path. The emitter path contains the Microelectromechanical systems (MEMS) mirror and the MEMS Driver Application-specific integrated circuit (ASIC). Druml et al. [2] indicate that the MEMS Driver and its precision of sensing, actuation and control directly influence the complete LiDAR system's measurement accuracy. Consequently, the LiDAR system's control-related digital circuits need to be correct and fault-tolerant. Fault-tolerant digital circuits struggle mainly with random hardware faults like Single Event Upsets which are soft errors in semiconductor devices induced by ionizing radiation [3]. These events do not physically harm the semiconductor components but may alter the logical value of a flip flop [4]. These errors have been affecting digital integrated circuits for decades and therefore, Error Correction Codes (ECC) are used for safety-critical systems [5]. ECCs are self-repairing algorithms with the ability to correct certain bit errors and maintain data correction during runtime [6]. The effect of SEU exponentially increases with higher packaging density as less electrons are representing a logic value [4]. As the demand for semiconductor devices rises due to ADAS, packaging density needs to increase even faster to satisfy computation power for real-time video signal processing [7]. Nevertheless, this trend also introduces drawbacks, especially from a safety point of view, as the enhancement of packaging density also increases the sensitivity to SEU [4]. Consequently, the automotive industry needs regulations and standards for safety-related semiconductor devices. For safety-related electrical and electronic devices, the automotive industry considers the functional safety ISO 26262 standard. In nine normative parts, this standard

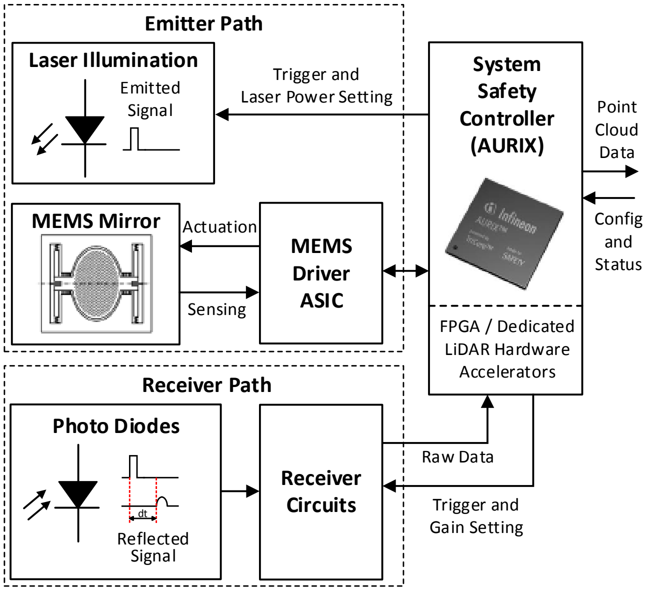

Figure 2. Overview of a LiDAR system for automonomous driving [2].

describes best practices to support engineers and managers in developing fail-safe automotive parts [8]. In the last years, this standard has been extended and the new version will be released end of 2018. The new version is called ISO 26262 2nd Edition and will include a part for semiconductors describing functional safety concepts for semiconductor devices [9]. For soft error mitigation, the standard suggests the use of Single Error Correction and Double Error Detection algorithms to protect digital circuits [9]. For semiconductor devices SEC-DED was already used in 1984 [5]. At that time, semiconductor devices were not that highly integrated and the packaging density was not as high as nowadays. Already in 1984, Chen et al. [5] described that in future semiconductor devices will use more complex ECC algorithms such as Double Error Correction and Triple Error Detection (DEC-TED). Contrary to the prediction of Chen et al. [5], the automotive industry still suggests using SEC-DED ECC algorithms 34 years later. This raises the question whether there are any disadvantages on DEC-TED algorithms or if the SEC-DED still fulfills the requirements for fail-safe automotive systems.

For this purpose, we will elaborate on the following two research questions:

- How can different ECC algorithms be validated from a safety point of view?
- Are Double Error Correction algorithms for LiDAR systems safer than SEC-DED algorithms?

II. Related Work

The need for error correction has always been vital for digital semiconductor devices due to possible alterations of flip flops caused by SEU. Already in 1984, Chen et al. described the application of these codes for semiconductor memory applications [5]. However, the history of ECC already began with punched card read errors in 1950. In this year, Hamming introduced his new approach for an automatic Error Correction Code during run-time to solve read errors [10]. Hamming's code is widely known and used for ECC. The algorithm corrects Single Bit Errors and is able to Detect Double Bit Errors (SEC-DED) by adding an additional parity bit [11]. For correcting more bits, other ECC algorithms are necessary. One of them is the concept of Bose-Chaudhuri-Hocquenghem-Codes (BCH-Codes). BCH-Codes can be used for multiple bit error corrections [12]. These two algorithms are the most important ECC concepts for digital integrated circuits and were already described by Chen et al. in 1984 [5]. Even modern and highly integrated complex systems still make use of Hamming's code and BCH-code [13] [14]. The novel ISO 26262 2nd Edition still refers to Hamming's ECC code to accomplish fail-safe digital circuits.

In the automotive industry, the ISO 26262 standard is used for functional safety. The new version ISO 26262 2nd Edition suggests ECC for diagnosing memory failures and rates the resulting diagnosis coverage as high. Therefore, this measure is often used for safety critical digital components [9] [13] [14]. For ECC, the standard still suggests the use of SEC-DED algorithms such as the Hamming code [9]. This raises the question whether SEC-DED has any advantages over DEC algorithms or vice versa. Still, novel safety critical automotive approaches, such as the fault-tolerant cache system for an automotive vision processor from Han et al. use SEC-DED [14].

The validation of algorithms is an important method for achieving certain requirements such as area, power dissipation or run time. Therefore, there are numerous articles about enhancing efficiency of fault-tolerant mechanisms through algorithm substitution [15] [16] [17]. Rossi et al. analyze the power consumption of fault-tolerant busses by comparing different Hamming code implementations with their novel Dual Rail coding scheme [15]. Also, Nayak et al. emphasize the low power dissipation of their novel Hamming code components [16]. Another example is the work of Shao et al. about power dissipation comparison between the novel adaptive pre-proccesing approach for convolutional codes of Viterbi decoders with conventional decoders [17]. Khezripour et al. provide another example for validating different fault-tolerant multi processor architectures by power dissipation [18]. Unfortunately, power dissipation is just one factor for reliability of safety-critical components and insufficient for safety validation. The most important indicator for safety at hardware level is the component reliability, which is measured in failure in time (FIT) rates [9]. Component reliability is the main indicator for safe hardware components and describes the quantity of failures in a specific time interval, mostly one billion hours [9]. These values can be calculated by specific standards for electronic component reliability such as the IEC TR 62380 [19] or statistically collected by field tests. Oftentimes, these field test have already been conducted by the manufacturers and are compiled in specific datasheets for component reliability [20]. For each component, the datasheets usually contain the specific FIT Rate for a certain temperature. To determine the FIT Rate for other temperatures, the Arrhenius equation as seen in (1) can be used.

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

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 Arrhenius Equation requires the Junction Temperature instead of Temperature values. The Junction Temperature represents the highest operation temperature of the semiconductor and considers the Ambient Temperature, Thermal Resistance of the package as well as the Power Dissipation as seen in (2).

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

where:

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

The validation of ECC algorithms is crucial for designers to pick the optimal ECC. Rossi et al. analyzed SEC-DED and DEC codes on area overhead and cache memory access time but their work did not consider the impact of different ECC algorithms from a safety point of view [21]. For designers of safety-critical digital circuits, it would be helpful to be able to pick the most safe ECC with the advantage of lower FIT Rates. Especially for automotive Tier-1 companies lower FIT Rates imply higher component reliability which is crucial for the economic success or failure of the whole system as profit margins are that small that every defect matters. Therefore, to support designers of safety-critical digital circuits, this paper's contributions to existing research are:

1) Developing a novel method for safety validation of algorithms on Field Programmable Gate Array that is based on the approved ISO 26262 2nd Edition methods.
2) Applying the novel method to quantify the differences between SEC-DED and DEC from a safety point of view.
3) Recommendation of ECC algorithm for safety-critical automotive LiDAR systems, based on the novel method of this paper.

III. FITNESS ASSESSMENT

To validate different ECC algorithms, it is necessary to quantify the essential values. Based on the functional safety standard ISO 26262 2nd Edition's approved methods, the FIT Rate is the most important factor for safety-critical hardware components. As stated in the Related Work section II, the Derating Factor influences the FIT Rate and is expressed in the Arrhenius equation (1). Combined with the Temperature Junction equation it is obvious that the power dissipation is the most significant quantity that can be influenced by designers of digital circuits (see (3)).

$$DF = e^{\frac{E_a}{k} \cdot (\frac{1}{T_{use}} - \frac{1}{T_{amb} + P_{dis} \cdot \theta_{ja}}))} \tag{3}$$

Consequently, by decreasing Power Dissipation the designer increases component reliability. For Field Programmable Gate Array (FPGA), the power dissipation primarily depends on static and dynamic power consumption. Based on these physical principles, our novel method FITness Assessment for algorithm safety validation on FPGAs is segmented in the following parts, as seen in Figure 3:

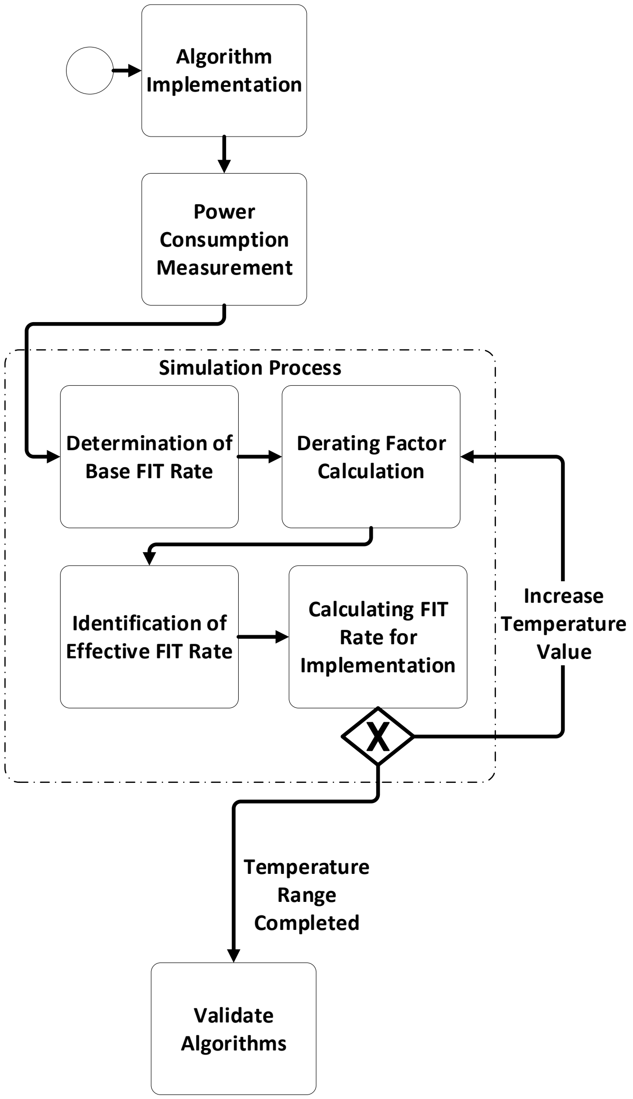
Algorithm Implementation
Power Consumption Measurement
Simulation Process
Determination of Base FIT Rate
Derating Factor Calculation
Identification of Effective FIT Rate
Calculating FIT Rate for Implementation
Increase Temperature Value
X
Temperature Range Completed
Validate Algorithms

Figure 3. Workflow overview of our novel method FITness Assessment for algorithm validation from a safety point of view in Business Process Model and Notation.

1) **Algorithm Implementation**
To guarantee similar conditions for different algorithms, it is necessary to implement a generic framework that allows implementing algorithms without major changes.
2) **Power Consumption Measurement**
For each algorithm, a particular measurement is recorded. It is advisable to record the generic framework without any algorithm to be able to determine the algorithms' power consumption by subtraction.
3) **Determinination of Base FIT Rate**
The Base FIT Rate may be calculated by using the IEC TR 62380 [19] standard or analyzed statistically by field tests. Oftentimes, these field test have already been conducted by the manufacturers and are compiled in specific datasheets for component reliability.
4) **Derating Factor Calculation**
The Derating Factor can be calculated with the Arrhenius equation and the related Thermal Junction equation as seen in (1) and (2).

ISBN: 978-1-61208-698-9

5) **Identification of Effective FIT Rate**
The Effective FIT Rate reflects the Base FIT Rate for a specific temperature and can be calculated with:

$$FIT_{ef} = FIT_{base} \cdot DF \tag{4}$$

where:

FIT_{base} is Base FIT Rate from FPGA Reliability Datasheet
DF is Derating Factor as seen in (1)

6) **Calculating FIT Rate of the Implementation**
The Effective FIT Rate as seen in (4) represents the component reliability for the whole FPGA. However, an FPGA is made up of many different logic elements. Consequently, the Effective FIT Rate can be broken down into the amount used by each logical element as seen in (5).

$$FIT_{imp} = \frac{FIT_{ef}}{N_{le}} \tag{5}$$

where:

FIT_{ef} is Effective FIT Rate as seen in (4)
N_{le} is Total Number of Logic Elements of the specific FPGA taken out from Datasheet

7) **Validate Algorithms**
The resulting FIT Rate of the implementation represents the FIT Rate of the specific algorithm and can be used for validation. It is adviseable to measure each algorithm once at room temperature conditions and simulate the rest of the temperature range by starting with the Derating Factor Calculation.

IV. Test Setup

In our research question, we analyze the differences between SEC-DED and DEC. For this purpose, we chose the Hamming code for SEC-DED as this code is recommended in the new ISO 26262 2^{nd} Edition and the BCH-code for DEC, especially because other ECC algorithms are often based on this concept and both algorithms fulfil the following requirements:

- 32 Bit data size
- Combinatorical Logic
- Including Fault Injection Module
- SEC-DED or DEC Functionality

The generic algorithm framework contains a testbench with an automatic up-counter as well as a validator (see Figure 5). Both algorithms can be exchanged in the framework without any major changes. This enables a precise validation from a safety point of view.

In our test setup, we use the MAX1000 - IoT Maker Board by Trenz Electronic. This device is a small maker board for prototyping with sparse additional components. The main controller is the MAX10 10M08SAU169C8G, an FPGA device by Intel. For our research, the main advantages of using this board are:

- Small amount of additional hardware components
- Availability of Reliability Datasheet

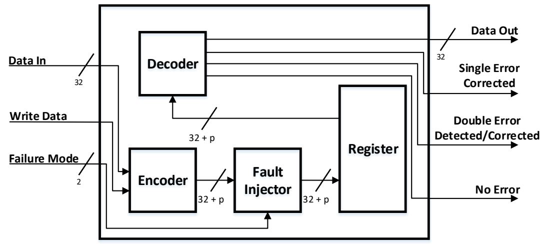

Figure 4. Pin configuration of both algorithms including an overview of functional blocks inside.

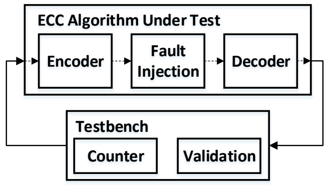

Figure 5. General framework for ECC algorithm validation including testbench and ECC algorithm.

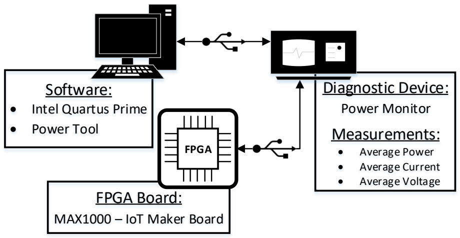

Figure 6. Overview of the entire measurement setup including software and hardware components.

This board also contains an FTDI chip that draws about 50 mA on average, which we will subtract out for our analysis. The power consumption measurement is performed by the Mobile Device Power Monitor of Monsoon Solutions. The big advantage of this power monitor is the direct measurement of USB devices. The entire measurement setup is shown in Figure 4 and 6 and contains the following software and hardware parts:

- Quartus Prime 18.0 (Intel)
- Power Tool 5.0.0.23 (Monsoon Solutions)
- Mobile Device Power Monitor (Monsoon Solutions)
- MAX1000 - IoT Maker Board (Trenz Electronic)

V. Results

This section summarizes our results of the comparison of SEC-DED and DEC ECC algorithm. The validation was performed with our novel FITness Assessment method for algorithm validation from a safety point of view as described in Section III.

The first algorithm we implemented was the Hamming code, which is a SEC-DED ECC algorithm. The implementation reserves 45 logic elements of the used FPGA and the whole board has an average power dissipation of 571.78 mW. With the second BCH-code DEC ECC algorithm, the board consumes an average of 599.05 mW and assignes 65 logic elements. The first result shows a difference between both algorithms in logic elements as well as in power dissipation resulting in a varying FIT Rate. The next step is the simulation

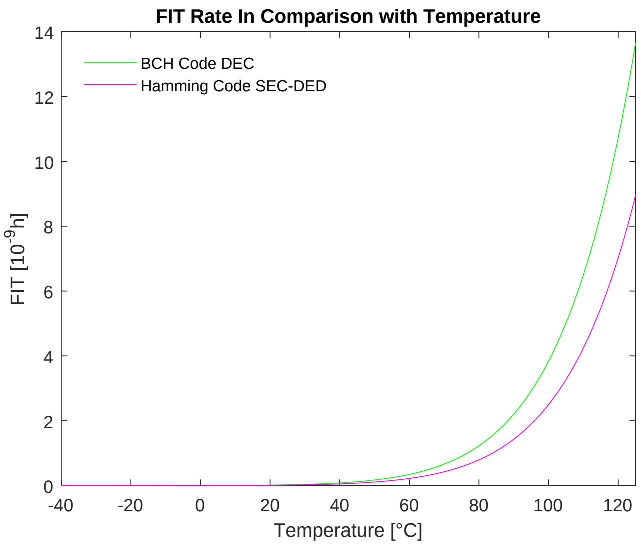

Figure 7. Simulation results of the resulted FIT Rates between -40°C and 125°C for both ECC implementations.

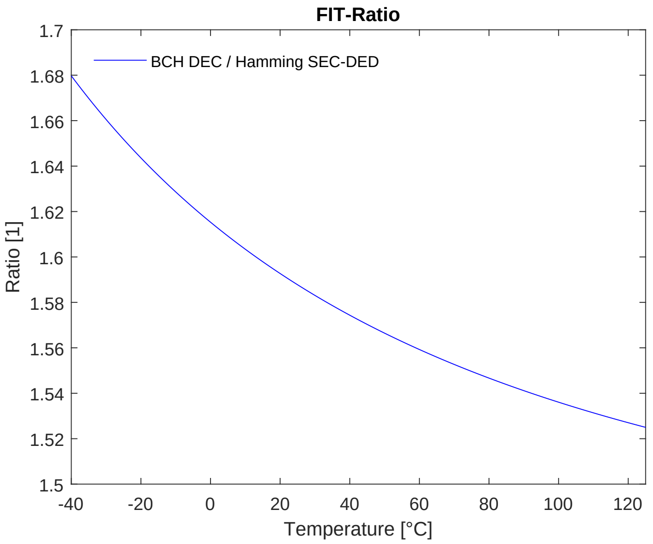

Figure 8. Overview of the FIT Rate overhead between SEC-DED and DEC ECC algorithm.

process over the whole temperature range. We selected a temperature range between -40°C and 125°C and the values of Table I were used for the simulation process. In our simulation we neglected the alteration of power dissipation through temperature because it would affect both ECC implementations evenly.

Figure 7 points out that both algorithms vary in their FIT Rate and rise exponentially with increasing temperature. The FIT Rate may be neglected for temperatures up to 40 °C. The Hamming code with SEC-DED shows a better FIT Rate indicating more reliability of the hardware components which results in a higher safety level. The reason for this difference is the greater number of logic elements used for the DEC ECC algorithm and the resulting increase of power dissipation. The higher power dissipation results in a higher Thermal Junction temperature as seen in (2) which leads to a higher FIT Rate.

TABLE I. RESULTS OF THE RESERVED LOGIC ELEMENTS AND AVERAGE TOTAL POWER DISSIPATION OF BOTH ECC IMPLEMENTATIONS.

	Hamming Code	BCH-Code
Used Logic Elements	45	65
Total Average Power Dissipation	571.78 mW	599.05 mW

Both algorithms were implemented without any safety measures. This means that any damage to the Logic Element of the FPGA leads to failure of the whole ECC algorithm and the safe memory block. The ECC algorithm is the measure against SEU related altered flip flops inside the memory block which decreases the specific FIT Rate of the memory block. The results of Figure 7 do not represent the FIT Rates of the memory block but the FIT Rate of the pure ECC implementation. It is important to understand that the ability of more bit error correction is not considered for the algorithm validation because it only positively influences the FIT Rate of the memory block.

Moreover, it is important to understand that the absolute values of the FIT Rate always correlate to a specific FPGA. Consequently, it is advantageous to look at the ratio between the algorithms because this gives a better overview of the overhead. The SEC-DED/DEC ECC FIT Ratio is depicted in Figure 8. The FIT Ratio overhead of the DEC ECC algorithm is slighly decreasing with increasing temperature, which is negligible in practice.

We recommend using the Hamming code algorithm for SEC-DED error correction for 32 bit memory size registers in automotive LiDAR systems. The SEC-DED algorithm used in our experiment resulted in a FIT Rate that was at least 52% lower than the DEC ECC algorithm.

VI. Conclusion

In this paper we analyzed SEC-DED and DEC ECC algorithms from a safety perspective. In Section III, we introduced the FITness Assessment, a novel method for algorithm validation from a safety point of view. This method is based on approved methods of the novel automotive functional safety standard ISO 26262 2nd Edition. The result clearly shows that different algorithms lead to different FIT Rates. FITness Assessment allowed the measurement of each algorithm's specific FIT Rate, facilitating the selection of the most reliable ECC algorithm. Our case shows a DEC ECC algorithm that has a higher FIT Rate than the SEC-DED ECC algorithm. The FIT Rate reflects component reliability which is an important hardware indicator for safety.

The paper's findings demonstrate that algorithm validation from a safety point of view is possible and that different ECC algorithms also result in different FIT Rates. These differences should not be neglected from a safety as well as from a business point of view. The FIT Rate also statistically indicates the amount of defective components, which is an economically important indicator as lower FIT rates also result in less defect components. Our results also give an explanation why the automotive industry still suggests using SEC-DED ECC algorithms instead of DEC ECC algorithms as SEC-DED offers a lower FIT Rate than DEC. In our case, the difference in FIT Rate was at least 52% and consequently, we suggest using SEC-DED for LiDAR systems.

The automotive industry is disrupted by autonomous driving which is why fault-tolerance, safety and reliability will become increasingly important in the next years. Our novel method FITness Assessment enables the validation of different algorithms to be able to select the most reliable one, which helps improve the overall safety level of the automotive vehicle by increasing component reliability.

VII. 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] 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.

[3] B. D. Sierawski, J. A. Pellish, R. A. Reed, R. D. Schrimpf, K. M. Warren, R. A. Weller, M. H. Mendenhall, J. D. Black, A. D. Tipton, M. A. Xapsos, R. C. Baumann, X. Deng, M. J. Campola, M. R. Friendlich, H. S. Kim, A. M. Phan, and C. M. Seidleck, “Impact of low-energy proton induced upsets on test methods and rate predictions,” IEEE Transactions on Nuclear Science, vol. 56, no. 6, Dec 2009, pp. 3085–3092.

[4] R. Islam, “A highly reliable SEU hardened latch and high performance SEU hardened flip-flop,” in Thirteenth International Symposium on Quality Electronic Design (ISQED), March 2012, pp. 347–352.

[5] C. L. Chen and M. Y. Hsiao, “Error-Correcting Codes for Semiconductor Memory Applications: A State-of-the-Art Review,” IBM Journal of Research and Development, vol. 28, no. 2, March 1984, pp. 124–134.

[6] J. Singh and J. Singh, “A Comparative Study of Error Detection and Correction Coding Techniques,” in 2012 Second International Conference on Advanced Computing Communication Technologies, Jan 2012, pp. 187–189.

[7] 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.

[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] R. W. Hamming, “Error detecting and error correcting codes,” The Bell System Technical Journal, vol. 29, no. 2, April 1950, pp. 147–160.

[11] H. Liu, D. Kim, Y. Li, and A. Z. Jia, “On the separating redundancy of extended hamming codes,” in 2015 IEEE International Symposium on Information Theory (ISIT), June 2015, pp. 2406–2410.

[12] Z. Xie, N. Li, and L. Li, “Design and Study on a New BCH Coding and Interleaving Techniques Based on ARM Chip,” in 2008 4th IEEE International Conference on Circuits and Systems for Communications, May 2008, pp. 315–318.

[13] S. Sooraj, M. Manasy, and R. Bhakthavatchalu, “Fault tolerant FSM on FPGA using SEC-DED code algorithm,” in 2017 International Conference on Technological Advancements in Power and Energy (TAP Energy), Dec 2017, pp. 1–6.

[14] J. Han, Y. Kwon, K. Byun, and H. Yoo, “A fault tolerant cache system of automotive vision processor complying with ISO26262,” in 2016 IEEE International Symposium on Circuits and Systems (ISCAS), May 2016, pp. 2912–2912.

[15] D. Rossi, A. K. Nieuwland, S. V. E. S. van Dijk, R. P. Kleihorst, and C. Metra, “Power Consumption of Fault Tolerant Busses,” IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 16, no. 5, May 2008, pp. 542–553.

[16] V. S. P. Nayak, C. Madhulika, and U. Pravali, “Design of low power hamming code encoding, decoding and correcting circuits using reversible logic,” in 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT), May 2017, pp. 778–781.

[17] W. Shao and L. Brackenbury, “Pre-processing of convolutional codes for reducing decoding power consumption,” in 2008 IEEE International Conference on Acoustics, Speech and Signal Processing, March 2008, pp. 2957–2960.

[18] H. Khezripour and S. Pourmozaffari, “Fault Tolerance and Power Consumption Analysis on Chip-Multi Processors Architectures,” in 2012 Seventh International Conference on Availability, Reliability and Security, Aug 2012, pp. 301–306.

[19] T. IEC, “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.

[20] “Reliability Report,” Jul 2018, [retrieved: 01, 2019]. [Online]. Available: https://www.intel.com/content/www/us/en/programmable/support/quality-and-reliability/reports-tools/reliability-report/rel-report.html

[21] D. Rossi, N. Timoncini, M. Spica, and C. Metra, “Error correcting code analysis for cache memory high reliability and performance,” in 2011 Design, Automation Test in Europe, March 2011, pp. 1–6.