2022
DESIGN AND VERIFICATION™
DVCON
CONFERENCE AND EXHIBITION
INDIA

What-If analysis of Safety Mechanism's impacts on ETHMAC design under Functional Safety flow

Udaykrishna J*, Sujatha Hiremath^, Kapil Kumar*, Sachin Pathak*, Gaurav Goel*
Siemens EDA*, RV College of Engineering^
Bengaluru

***Abstract*- Functional Safety has been a major concern in the automotive industry to safeguard the functionality of electrical and electronic systems and the life of an end-user (driver/passenger). Depending upon the criticality of the systems, ISO-26262 standard lays out different ASIL levels to be achieved. But as the systems are incorporating more functionalities, SoCs are becoming more complex and so does the task of making these tiny objects functionally safe. This paper walks through a Functional Safety flow and presents the analysis of applying different standard Safety-Mechanisms (SM) on ETHMAC design. The detailed analysis consists of the SM impacts on various parameters such as area, Diagnostic Coverage (DC), flip-flops and ASIL levels. By applying different safety mechanisms on the ETHMAC design, the Register parity SM on Wishbone instance has covered 43.9% DC while Duplication SM has covered 60.46% DC and consumes 67.01% more area. This Analysis can be used for further improvements in Functional Safety process while considering the trade-offs among above mentioned parameters.**

I. INTRODUCTION

Functional Safety is one of the important parts in the overall system development that depends on automatic protection. The response from this automatic system should be correct corresponding to its inputs and it should have predictable responses to failure i.e., it should fail safely. This phase ensures that it safeguards the functionality of the device or a system. ISO 26262 is an international standard focussing on the safety of automotive electrical and electronic systems. ISO 26262 standard introduces a framework of Hazard Analysis and Risk Assessment (HARA) which considers three factors i.e., severity, exposure, and controllability. Based upon the risk assessment the safety standards are classified into different ASIL standards. The functional safety parameters associated to risk assessments are estimated through the Failure Mode Effects and Diagnosis Analysis (FMEDA) and commonly safety standards are measured by using Automotive Safety Integrity Level. ASIL rating is mainly based upon three metrics that are Single Point Fault metric (SPFM), Latent Point Fault Metric (LFM) and Probabilistic Metric for random Hardware Failures (PMHF) that reflect the item's robustness under the failures either by design or by the safety mechanisms.

There are two types of faults: Permanent faults and Transient faults. Permanent faults are the faults which persists for a long duration of time whereas transient faults are present only for a short period of time and revert to normal functionality.

Functional Safety is a process in which a safety mechanism is inserted into the design, keeping its original functionality, to make the design safe under random failures. There are different safety mechanisms such as Register Parity, Duplication, Triplication, and many more. There are few safety mechanisms that are custom made, as per the requirement. The safety mechanisms act as a protection to safeguard the design.

In this paper, as part of the experimental work, an Ethernet IP Core design is used to perform functional safety. The Ethernet IP core is a MAC (Media Access Controller), and it connects to the Ethernet PHY chip on one side and to the WISHBONE SoC bus on the other. The core has been designed to offer as much flexibility as possible to all kinds of applications.

II. Related work

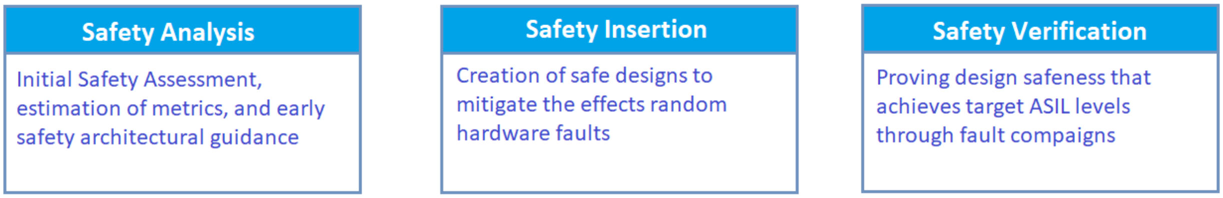
In paper [1], authors carried out the assessment of an automotive safety microprocessor with ISO 26262 hardware requirements which is approached with step-by-step guidelines. Quantitative evaluations such as hardware architecture metrics and probabilistic hardware metrics are obtained to prove the compliance with ISO 26262 hardware development process. Changes in the role of semiconductor industry in automotive supply chain is enhanced [2]. The authors in [3] discussed about the overall flow of the functional safety development of an item and the practices for achieving functional safety for automotive SoCs. The transient fault analysis towards ISO 26262 certification is carried out in [5]. The process to incorporate a collection of safety mechanisms into the design and the validation of the design is done in [4] and with this motivation the analysis on the impacts of SM must be carried out. Many in the semiconductor engineering community are new to the ISO 26262 functional safety standard and the automotive industry. In order to improve the understandability of all elements of the ISO 26262 standards, the paper [6] outlines change in the semiconductor industry's involvement in the automotive supply chain. Discusses the standard's relevancy to both electronic products and the individuals and procedures used in their production. Paper [7] discusses the functional safety concepts that are inhibited in automotive industries and the key elements that are to be taken care while performing the functional safety. Above all, there was a need to understand the impacts of the SM on different levels. With this motivation the analysis on the impacts of SM must be carried out.

III. Methodology

Based on the ASIL level requirement, safety analysis is carried out and safety mechanisms are incorporated into the design. To achieve the required ASIL level, we propose the following 3 step Functional Safety flow as -

1. Safety Analysis
2. Safety Insertion
3. Safety Verification

Figure 1 shows the overall Functional safety workflow:



Safety Analysis

Initial Safety Assessment, estimation of metrics, and early safety architectural guidance

Safety Insertion

Creation of safe designs to mitigate the effects random hardware faults

Safety Verification

Proving design safeness that achieves target ASIL levels through fault compaigns

Figure 1: Functional safety workflow

As shown above, the stages are independent of each other. Each stage can be used individually in parallel manner or can be used sequentially i.e., one after the other.

1. Safety Analysis: This is an initial safety assessment stage where the early analysis/what-if analysis is carried out to see the impacts of safety mechanisms into the specified design portion. The purpose of this stage is to identify how safe the design is currently and provide guidance on additional safety mechanisms to meet a safety requirement.
2. Safety Insertion: In this stage, SM is inserted to provide safety towards the random faults in the design. The inserted Safety mechanisms will detect the fault and provide the safety towards the failure. The intention of this stage is to insert safety mechanisms to create a hardened design. There can be two approaches for inserting the SMs. Applying SM on Instance-level or on Register-level.
3. Safety Verification: In this phase, the effectiveness of SMs in detecting the random hardware faults can be verified. The process of fault injection into the design and fault simulation of safe RTL (SM inserted design), is called as fault campaign. Though there are various approaches for verification, fault campaign is one of the most accepted approaches by industries, an approach that validates systems by injecting faults into safety-critical nodes in the design to check whether the SMs detect them.

The traditional methodology of functional safety process is as shown in Figure 2. This tedious approach will lead to expensive iterations.

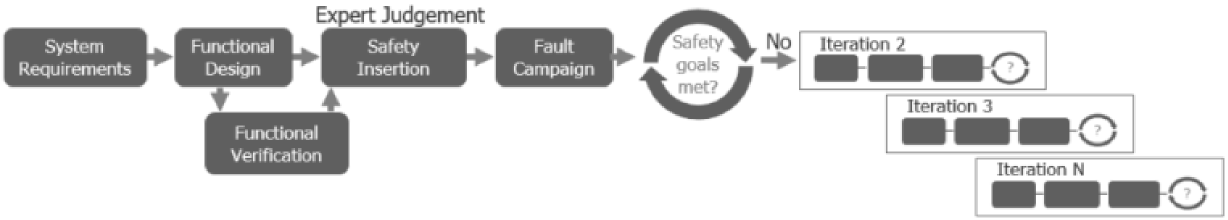


Figure 2: Traditional Functional Safety process

In the traditional approach, the safety insertion process was mainly dependent on expert judgement and multiple iterations of manual safety verification process. This approach was mainly dependent upon the past safety insertion experiences and sometimes lacked relevant data related to the safety impact of particular RTL/IP blocks.

So What-if Analysis provides the information of the design that if a SM is inserted into the design whether the required safety standard is met or not. This approach will left shift the process and the overall cost of the functional safety process will be reduced. ISO 26262 Clause 8 discusses the evaluation of the hardware architectural metrics. The safety metrics and their safeness level can be defined by using the Table 1. Specifically, the metrics is intended to evaluate the effectiveness of the hardware architecture in dealing with random failures.

Table 1: ISO 26262 Quantitative Evaluation metrics

	ASIL B	ASIL C	ASIL D
Single-point fault metric	≥90%	≥97%	≥99%
Latent fault metric	>60%	>80%	>90%
PMHF	<100 FITs	<100 FITs	<10 FITs

The most widely accepted SMs are Dual Core and Triple Modular Redundancy i.e., Duplication and Triplication respectively. Duplication SM can be applied on Registers and Combinational logic. It can also be applied on Instances as well. By doing so the Diagnostic Coverage (the proportion of hardware element failure rate that is detected or controlled by SMs) value of the design increases and continued until the required safeness is achieved. By applying Duplication SM on the design, the area of the design increases by 2X and by applying Triplication, the area increases 3X which is less desirable. One of the major concerns in the semiconductor industry is the area consumption. To reduce the area consumption in functional safety process, there is a need to design a SM so that it provides the required safeness to the design with optimum area consumption. *Our goal would be to reach the optimal safety goal (SPFM goal) while keeping the area less than 2X.*

IV. EXPERIMENTAL WORK

Let’s consider EthMAC design for functional safety process. For the EthMAC design shown in Figure 3, comparison is carried out with duplication SM and custom made SMs to individual Instances.

First, for a given RTL, Safety analysis is carried out to analyse the Base FIT rate and understand the contribution of each module towards failure. With the help of the contribution metrics, it is easy to understand which module or instance contributes the most towards the failure. Accordingly, SM is applied to that module to increase the safeness of the design as well as area concern is also met. In this stage, What-if Analysis is carried out in series of experiments to see the effects of different SMs towards the DC value before inserting them into the design.

For the EthMAC design, safety analysis is carried out and the contribution of each module towards permanent faults and transient faults is obtained as shown in Figure 3. As seen in Figure 3, Wishbone module contributes the most towards the failure.

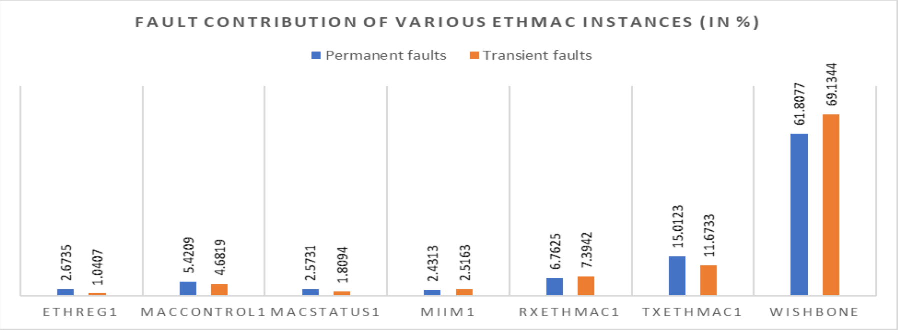


Figure 3: Fault Contribution of EthMAC Instances

It can be seen that Wishbone is contributing the highest towards the failure rate. If we are able to protect the Wishbone effectively, that is going to result into a higher SPFM number. We can start with individual Instance and observe the SPFM values of individual Instance and overall EthMAC design as shown in table 2. It also provides the details of increase in area at Instance level and on overall EthMAC design as well. This approach of computing the SPFM at the analysis stage helped us to understand whether the safety goal is reached or not.

Table 2: Metrics obtained after Safety Analysis on different ETHMAC instances

Instance	Safety Mechanism	SPFM (Instance) in %	Estimated area increase (Instance) in %	SPFM (Overall) in %	Estimated Overall area increase (%)
miim.clkgen, miim.shftrg, miim.outctrl	Duplication	86.0429	89.3558	2.4293	1.7976
eth_regs	Duplication	99	100	14.2816	8.8973
maccontrol.receivecontrol, maccontrol.transmitcontrol	Duplication	97.7141	96.619	19.4418	14.0255
txethmac.txcounters, txethmac.txstatem, txethmac.txcrc, txethmac.random	Duplication	91.7945	87.8643	25.2856	19.5843
rxethmac.rxcounters, rxethmac.rxstatem, rxethmac.rxcrc, rxethmac.random	Duplication	90.0091	67.2716	29.9051	23.5069
wishbone.tx_fifo, wishbone.rx_fifo	Duplication	86.8566	86.7585	88.6952	72.0764
macstatus	Duplication	84.6199	100	90.2011	72.8965

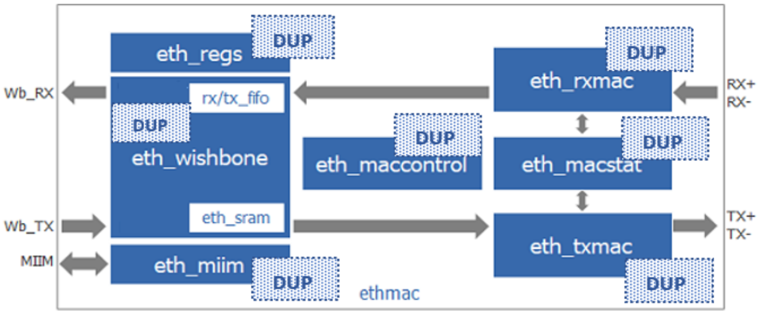


Figure 4: EthMAC module with Duplication SM

The approach of computing the SPFM values in What-if analysis is a pre-fault injection campaign. Pre-fault injection describes that the fault is not injected to obtain the SPFM and still it is available. The SM can be inserted to the registers and the combinational circuit which increases the number of transistors in the design. So, this process must be done carried out carefully to obtain the required DC value to meet the ASIL with optimized area consumption. The further discussion in this paper consists of the comparison of parameters with different SMs are carried out.

Like the above approach, now custom SMs are applied to each module and the metrics are obtained accordingly. The custom SM used in this case is the combination of Register Parity (which protects the Registers) and Combinational logic protecting SM i.e., SM1 = Register Parity + Custom SM on Combinational logic. Applying this SM all the metrics shown are calculated.

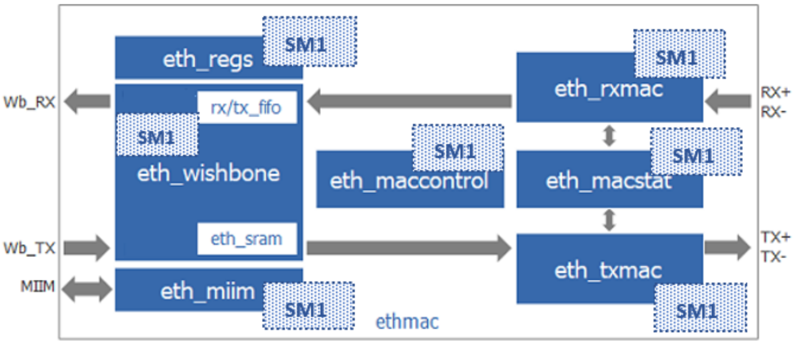


Figure 5: EthMAC module with Custom SM

Table 3 shows the values of SPFM and estimated increase in area of individual Instance and Overall EthMAC design with custom SM. With the help of the table 3, it is clear that the area consumed by the custom SM is less and yet achieving the same safety standard(SPFM value).

Table 3: Metrics obtained after Safety Analysis on different ETHMAC instances with custom SMs

Instance	Safety Mechanism	SPFM (Instance) in %	Estimated area increase (Instance) in %	SPFM (Overall) in %	Estimated Overall area increase (%)
miim.clkgen, miim.shftrg, miim.outctrl	SM1	83.4518	62.5359	2.8532	1.6469
eth_regs	SM1	96.807	78.8856	13.9459	6.371
maccontrol.receivecontrol, maccontrol.transmitcontrol	SM1	98.4149	84.9977	19.1431	8.2746
txethmac.txcounters, txethmac.txstatem, txethmac.txcrc, txethmac.random	SM1	95.4963	79.5994	25.2225	13.2886
rxethmac.rxcounters, rxethmac.rxstatem, rxethmac.rxcrc, rxethmac.random	SM1	92.6778	64.484	29.979	16.5123
wishbone.tx_fifo, wishbone.rx_fifo	SM1	84.6199	61.1119	89.2835	54.4462
macstatus	SM1	98.7465	83.7292	90.1781	55.0583

V. RESULTS

Safety Analysis is carried out on the EthMAC design that is in the pre-fault injection mode and the contribution metrics of each module towards the failure are obtained. Duplication SM is applied on each module and the safety metrics are obtained accordingly. Later custom safety mechanisms are applied to individual module and the respective safety metrics are obtained as well. When these two parameters are compared, it is observed that the Duplication SM consumes more area compared to the custom SMs. It is also seen that for few instances, the custom SMs provide higher SPFM compared to Duplication SM. The overall area increase with Duplication SM was found to be 72.8965% (Table 2) more than the original one whereas with custom SM, the overall increase is 55.0583%. So, there is a reduction of 17.8382% in area consumption using custom SM to achieve the same safeness as the Duplication SM is achieved.

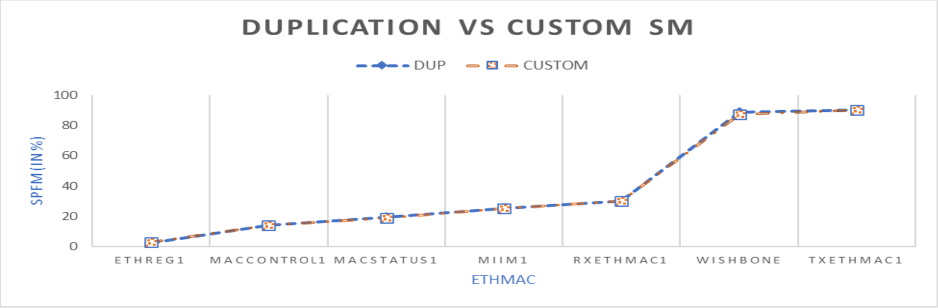


Figure 6: Comparison of Duplication SM and Custom SM in reaching SPFM

As we can see in Figure 6 that both Duplication SM and Custom SM are approaching towards the same SPFM value i.e., achieving the same safety standard. Figure 7 shows the comparison of increase in area with Duplication and Custom SM on EthMAC design. This clearly shows that with the help of custom SM, the overall increase in area consumption for functional safety process can be reduced.

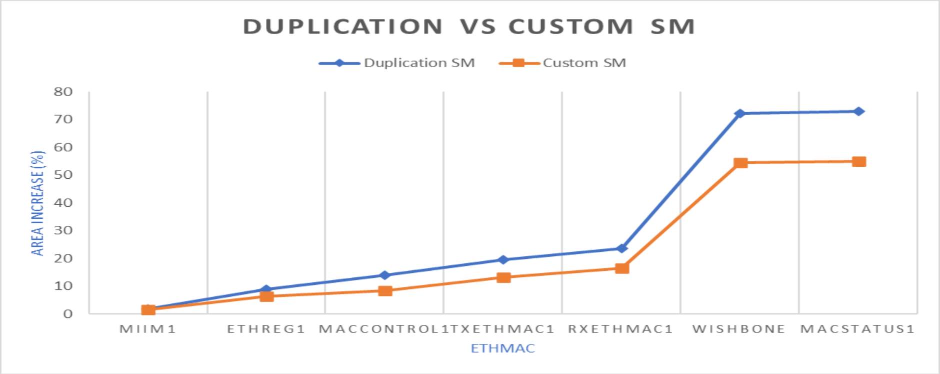


Figure 7: Comparison of area increase with Duplication SM and Custom SM

V. Conclusion

In this paper, we have presented a safety workflow methodology in a 3-step process. We have explored with Duplication SM and with Custom SM on EthMAC design. As a result, at EthMAC we were able to achieve the total DC value (or) SPFM value of 90% without violating the 2X area target. What-if analysis provides the SPFM metrics before even injecting the faults into the design i.e., we are performing pre-fault injection safety analysis to identify the safeness of the design. This pre-fault injection approach will reduce lot of resources used and time consumption as well. This analysis also helps in deciding the proper SM that must be inserted to achieve the required standard. Also, this work explains that by using Custom SM the overall area consumption for functional safety process can be reduced by achieving the required safety standard. There is scope to extend this work with different experimentations on custom SMs that requires less area to achieve required ASIL standard.

References

[1] Y. -C. Chang, L. -R. Huang, H. -C. Liu, C. -J. Yang and C. -T. Chiu, "Assessing automotive functional safety microprocessor with ISO 26262 hardware requirements," Technical Papers of 2014 International Symposium on VLSI Design, Automation and Test, 2014, pp. 1-4, doi: 10.1109/VLSI-DAT.2014.6834876.

[2] S. Chonnad, R. Iacob and V. Litovtchenko, "A Quantitative Approach to SoC Functional Safety Analysis," 2018 31st IEEE International System-on-Chip Conference (SOCC), 2018, pp. 197-202, doi: 10.1109/SOCC.2018.8618540.

[3] W. Chen and J. Bhadra, "Practices and Challenges for Achieving Functional Safety of Modern Automotive SoCs," in IEEE Design & Test, vol. 36, no. 4, pp. 31-47, Aug. 2019, doi: 10.1109/MDAT.2019.2908643.

[4] Avidan Efody, “Whose fault is it? Advanced techniques for optimizing ISO 26262 fault analysis”, Design and Verification Conference and Exhibition, USA, 2019.

[5] Ping Yeung, Jin Hou, Vinayak Desai, Jacob Wiltgen, “Are You Safe Yet? Safety Mechanism Insertion and Validation”, Design and Verification Conference and Exhibition, USA, 2019.

[6] Ross, Hans-Leo. "Why Functional Safety in Road Vehicles?." Functional Safety for Road Vehicles. Springer, Cham, 2016. 7-39.

[7] Hopkins, Andrew. "The functional safety imperative in automotive design." ARM, Tech. Rep., 09 (2016).

[8] Ethernet MAC 10/100 mbps. url: https://opencores.org/projects/ethmac.

[9] Feabhas - A quick guide to ISO 26262

[10] Jake Wiltgen, The importance of effective Safety Analysis. url: blogs.sw.siemens.com