# A 1GHz Fault Tolerant Processor with Dynamic Lockstep and Self-recovering Cache for ADAS SoC Complying with ISO26262 in Automotive Electronics

Jinho Han[1 2], Youngsu Kwon[1], Yong Cheol Peter Cho[1] and, Hoi-Jun Yoo[2]
[1] Processor Research Group, ETRI, Daejeon, Republic of Korea
[2] Department of Electrical Engineering, KAIST, Daejeon, Republic of Korea
soc@etri.re.kr

***Abstract*—We present a processing platform that implements DMR with separate clock and power sources to prevent dependent failures working with a reconfigurable cache that includes BIST with self-recovering function to detect transient faults and error prediction to prevent permanent faults. The fault tolerant processor is analyzed to be complying with the ISO26262 SOTIF for ADAS SoC which is fabricated with 28nm CMOS Technology. The single point faults metric is 99.64% with a safety mechanism.**

***Keywords—fault tolerant processor; ADAS; fault tolerant cache; ISO26262; dynamic lockstep***

## I. INTRODUCTION

Advanced driver-assistance systems (ADAS) such as Forward Collision Warning, Pedestrian Collision Warning, Lane Departure Warning, and Traffic Sign Recognition with Speed Limit Indication recognize objects and calculates the distance and the rational speed by processing images from a camera. ADAS vision processing algorithms are inherently compute intensive, and therefore, require powerful processors [2] Moreover, processors for automobiles should include the fault tolerant feature because of its harsh operation conditions and safety requirements [3].

Semiconductor chips for automotive applications must comply with ISO26262 standard to achieve functional safety [4]. The SOTIF working group in ISO26262 addresses functional safety standard for the intelligent driving system including ADAS and has proposed strict requirements to avoid or mitigate the possibility of the system failure. Previously, ADAS applications executed on DMR (Dual Modular Redundancy)-based CMPs with redundant execution at the other core for error detection and recovery [5]. Also, recent multi-thread based safety processors require complicated threading with complicated cache architectures.

In this paper, we present a processing platform that implements DMR with separate clock and power sources to prevent dependent failures working with a reconfigurable cache that includes BIST with self-recovering function to detect transient faults and error prediction to prevent permanent faults. The processing platform overcomes the low fault coverage of the self-test and the performance overhead by the self-test time in [5] [3].The proposed fault tolerant processor is analyzed to be complying with the ISO26262 SOTIF for ADAS SoC. The processor works in tandem with hardware IPs that includes H.265 video codec and object recognition accelerator.

This work was supported by the ICT R&D program of MSIP/IITP. [2017-0-00261, Intelligent Many-Core Processor and SW based on Low-Power Hypervisor]

## II. THE PROPOSED PROCESSOR ARCHITECTURE

The proposed fault tolerant processor contains three key features: 1) dynamic lockstep (DLS) with separate clock and power sources to reduce dependent failures and have the high performance, 2) the cache with self-recovering function to reduce transient faults, 3) reconfigurable function to reduce permanent faults.

Figure 1 shows a block diagram of the fault tolerant processor. It consists of 2 processor cores, 4 caches, 4 fault managers (FTM) in cache, and 1 external FTM (EFTM). For operating at 1GHz frequency on 28nm node. For the critical path is below 1ns, one processor has 13 pipeline stages with 2-issue superscalar architecture, fetch scheduler fetching 8 instructions maximally, a branch predictor with branch target buffer (BTB) using the GSHARE method with branch history registers, Load and Store Unit with 2 pipeline stages, 32KB I/D cache with 3 pipeline stages, and 32-entry I/D table look-aside buffer (TLB).

The design operates in one of two modes: Dynamic Lockstep (DLS) mode and non-DLS mode. The mode of operation is determined by programming at the software shown as Figure 2. The processors operate in DLS mode when DLS register of the both processors is enabled by a software and, operating in non-DLS mode when DLS register of the both processors is disabled by a software.

In DLS mode, one processor operates as the leading core while the other operates as a trailing core and the operating frequency of the leading core is bigger than the one of the trailing core and the difference of the operating frequency makes the effect of the temporary redundancy. both processors run the same task by controlling the core id of the both processors to the same core id by EFTM and for the result of the leading core is compared with that of the trailing one to detect faults, the data cache in each processor has stopped and

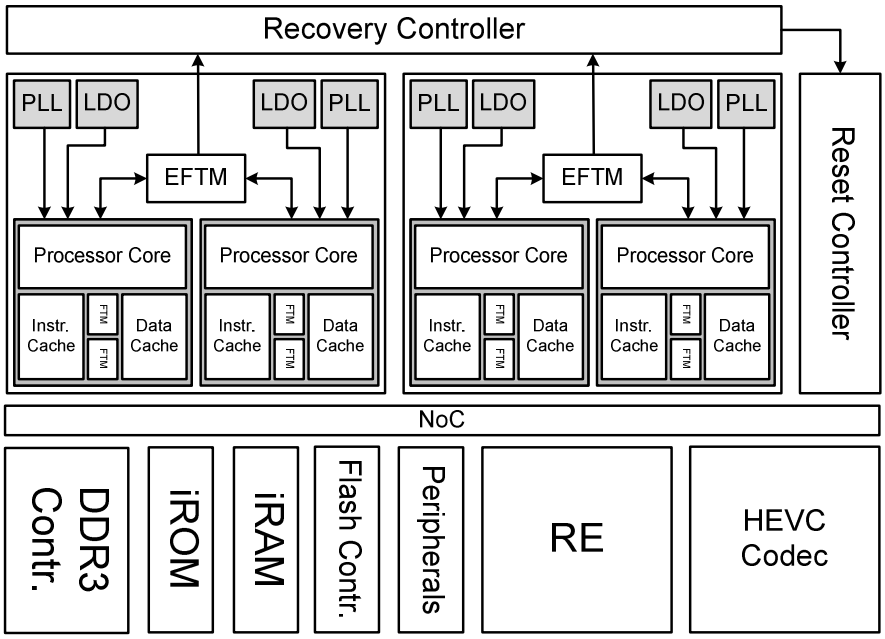



Fig. 1. A fault tolerant processor in ADAS SoC

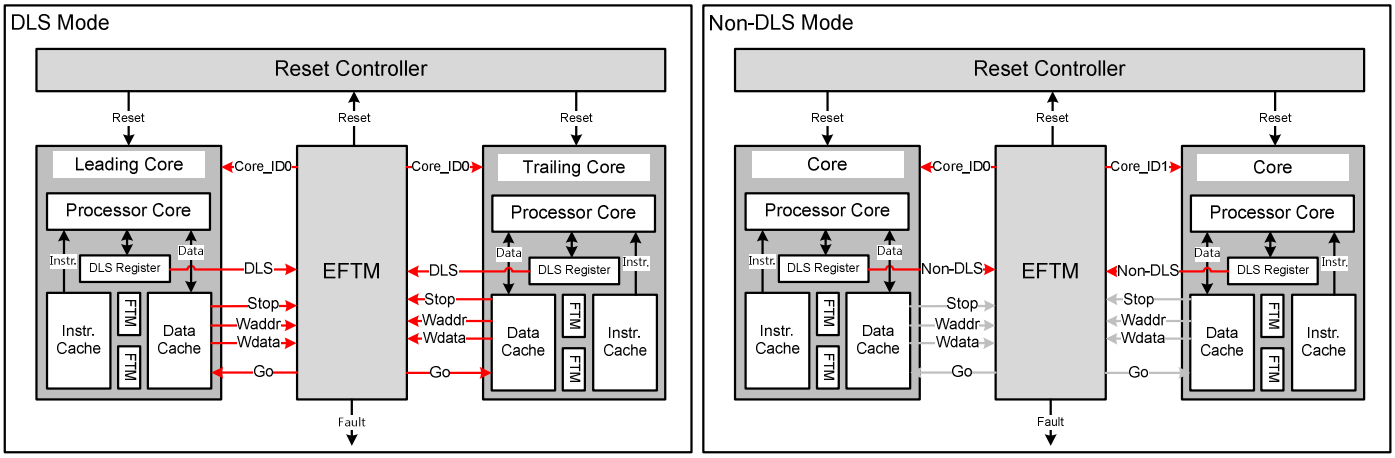



Fig. 2. Dynamic lockstep with separate clock and power sources.

send the write data and address to EFTM when the processor core request the write to the data cache. The frequency of the check point using the cache write is sufficient to identify the fault of the processor.

EFTM compares the cache write of the leading core with the cache write of the trailing core and EFTM starts the data caches of the leading and trailing core if the cache write of the trailing core is resembled from one of the leading core. But, EFTM generates the fault signal if the cache write of the trailing core is not resembled from one of the leading core. The data in SDRAM is not changed by the trailing core because the data is written in the data cache, but the dirty bit of the data cache in the trailing core is not enabled. In the other words, the data is changed by the leading core, and the trailing can use the data which is changed by the leading core.

In non-DLS mode, the two processors operate as a traditional dual-core processor would and thereby increasing throughput by running different tasks on each processor which are not critical for the functional safety of the system. EFTM identifies the DLS register of the both processors is disabled and controls the core id of the each processor to the different core id.

A cache system is composed of two architectures: 1) the error correction in the memory by using a cache characteristics and error correction code, 2) the reconfiguration by using error predictor as Figure 3. Safety mechanisms in the cache architecture are vital as cache is intrinsically vulnerable to transient faults. In our implementation, the error correction code (ECC) named single error correction and double error detection (SECDED), corrects single errors and detects double errors in data chunks.

FTM monitors double errors and recovers the data using the characteristics of the cache which copies the data of the SDRAM in SRAM of the cache. The data can be recovered by depending on the error state of the valid-bit, tag, dirty-bit, and data memory in the cache when error correction code detect but can't correct errors. If there are no error on valid-bit, tag, dirty-bit memory and the value of dirty-bit of the erroneous data is 0,

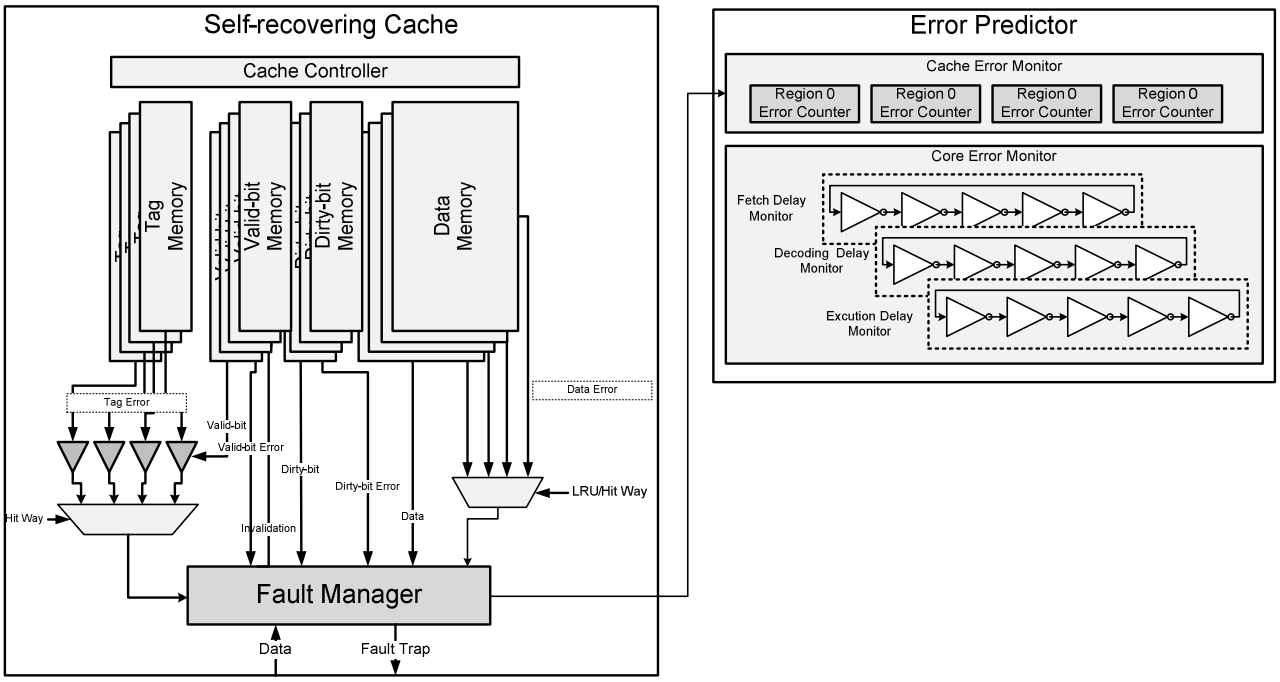
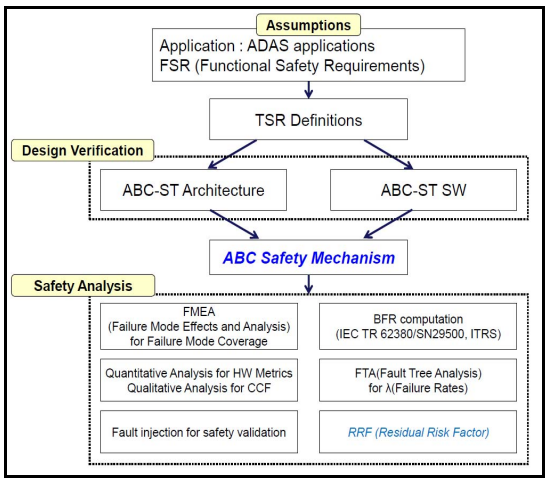
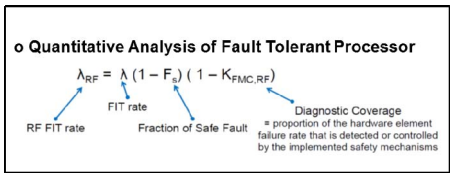



Fig. 3. A fault tolerant cache with self-recovering, and error predictor.




| Failures / parts | Permanent | | Transient |
|---|---|---|---|
| | Single Point Faults Metric (SPFM) | Latent Faults Metric (LFM) | Single Point Faults Metric (SPFM) |
| Core | 85.25% | 97.31% | 98.99% |
| Memory | 95.00% | 89.52% | 92.33% |
| Peripheral | 90.00% | 83.88% | 90.10% |
| PADs | 90.00% | 90.00% | 96.99% |
| SM | 93.83% | 87.88% | 90.19% |

Fig. 4. SEooC flow and quantitative analysis of ISO26262.

the error is recovered by reading the data from SDRAM the error case which is composed the error state of valid-bit, tag, dirty-bit, and data memory and can be recovered and invalidated is descripted in [6].

Error predictor has cache error monitor and core error monitor as shown in Figure 3. In cache error monitor, the silent fault is counted when the error is corrected by ECC and the data of the cache is recovered by the fault manager by a region, which is divided by 8KB. The each region of the cache is powered off based on the fault frequency, or when the silent fault count of the region is bigger than the number of the pre-defined silent faults. The processors are switched in DLS mode when one of delay monitors for the pipeline stages has bigger delay than the period considering the guard band in core error monitor. Not only the transient fault but also the permanent fault can be prevented by the error predictor.

## III. Implementation Results and Fault Analysis

The functional safety of the processor in ADAS SoC is analyzed to Safety element out of context (SEooC) method of ISO26262 as shown Figure. 4. With the implementation process for the Semiconductor with ISO26262 Compliance, the semiconductor has the fault-tolerant design, which is the wearout prevention for permanent faults, the multicore lockstep and part-wise checker for transient faults, dependent failures, and the designs for the transient, permanent, and dependent failures are analyzed and verified by FMEA, FTA, qualitative analysis, and fault injection.

The proposed fault tolerant design has self-recovering BIST and DLS for transient faults and error monitor for permanent faults. The dependent failures of two or more circuits are resulting from a single specific event or root cause. So, the

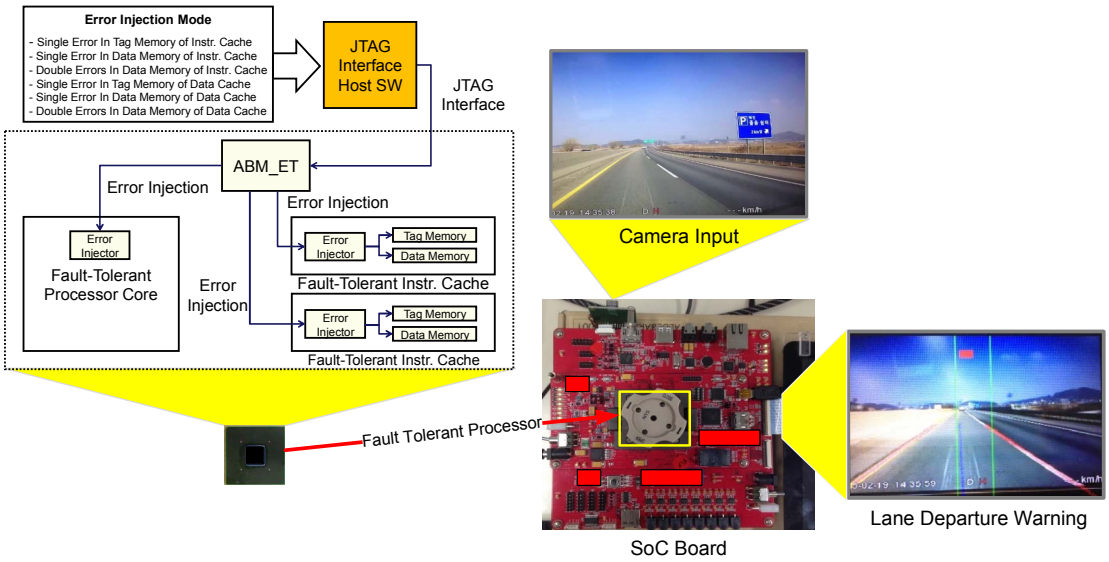
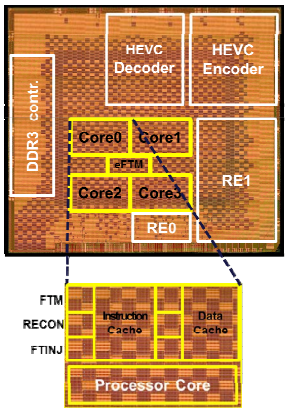



Fig. 5. Fault injection experiment.




| Technology | 28nm 1P12M Logic CMOS |
|---|---|
| Chip Size | 7341 x 7541 ㎛² |
| Gate Count | 18M gates |
| SRAM | 1,077KB |
| Supply Voltage | 1.05V - 1.15V |
| Clock Frequency | 50MHz - 1.0GHz |
| Fault Tolerant Processor | |
| Size | 1505.8 x 1246.4㎛² |
| Gate Count | 216K gates |
| SRAM | 110KB (64KB data, 40KB ECC, 4KB tag) |
| Supply Voltage | 1.05V - 1.15V |
| Clock Frequency | 600MHz -1.0 GHz |
| Power Consumption | 48 - 216mW |
| Power Efficiency | 0.08 - 0.18mW/MHz |

Fig. 6. Die photo and summary.

TABLE I. THE FAULT TOLERANCE PERFORMANCE COMPARISON.

| Parameter | No FT | FT Cache | DCC[5] | Takahashi [3] | This Work |
|---|---|---|---|---|---|
| Fault Detection Coverage | N/A | Medium | High | Medium | Medium ~ High |
| ECC | X | SECDED | N/A | N/A | SECDED |
| Fault Detection | X | ECC | DMR | Self-BIST | DLS with Separate Cock and Power, Self-recovering Cache |
| Fault Detection Time | X | 1 cycle | 137 cycles | <2ms | 1 cycle |
| Fault Prediction | X | X | Thread Control | Droop Monitor Adaptive Clock Control | Error Predictor Reset/Cache Size Control |
| Fault Injection | X | X | X | X | O |
| Fault Traps | 100 % | 83 % | N/A | 10-7 RHF/Hour | 28 % |
| Single Point Fault | X | N/A | N/A | N/A | 99.64 % |
| Latent Fault | X | N/A | N/A | N/A | 93.23 % |

dependent failures is prevented because the root cause of power sources and the single specific event of the clock sources does not exist by using the separated clock and power. With FMEA, transient faults are analyzed by fault injection at ADAS in automotive electronic system as shown Figure. 5. Permanent faults and dependent failures are analyzed by quantitative analysis with safety mechanism of DLS and self-recovering cache.

## IV. CONCLUSION

We implemented ADAS SoC with the proposed fault tolerant processor. The fault tolerant processor is fabricated with 28nm CMOS Technology, having the footprint with the specification as Figure 6. The fault tolerant processor has two dual-core with DLS and the instruction cache and the data cache with a self-recovering function. The each cache can store 32KB of data with 20KB of ECC. A self-recovering cache and DLS achieves 80% reduced error traps as TABLE I when compared with the previous works. As a result, the single point faults metric about the permanent faults is 99.64% with a safety mechanism, and the latent faults metric about the permanent faults is 93.23% with a safety mechanism.

## REFERENCES

[1] K. J. Lee, et al., "A 502GOPS and 0.984mW Dual-Mode ADAS SoC with RNN-FIS Engine for Intention Prediction in Automotive Black-Box System," ISSCC Dig. Tech. Papers, pp.256-257, 2016.

[2] J. Tanabe, et al., "A 1.9TOPS and 564GOPS/W Heterogeneous Multicore SoC with Color-Based Object Classification Accelerator for Image-Recognition Applications," ISSCC Dig. Tech. Papers, pp.328-329, 2015.

[3] C. Takahashi, et al., "A 16nm FinFET Heterogeneous Nona-Core SoC Complying with ISO26262 ASIL-B: Achieving 10-7 Random Hardware Failures per Hour Reliability," ISSCC Dig. Tech. Papers, pp.80-81, 2016.

[4] Road vehicles – Functional Safety, ISO26262, 2012.

[5] C. Lafrieda, et al., "Utilizing Dynamically Coupled Cores to Form a Resilient Chip Multiprocessor," IEEE Intl. Conf. on Dependable Systems and Networks Tech., pp. 317-326, 2007.

[6] J. H. Han, et al., "A Fault Tolerant Cache System of Automotive Vision Processor Complying with ISO26262,", IEEE Trans. Circuits Syst. II Exp. Briefs, vol. 63, Issue. 12, pp. 1146-1150, Dec. 2016.