Methodology to Achieve ASIL-D for an IP in SoCs for 360-degree Automotive Display Systems

Jerry (Chaojie) Chen jerry_chen@ovt.com, Niko (Bicheng) Guoniko.guo@ovt.com,

Omnivision Technologies (Shanghai) Co. Ltd

Sesha Sai Kumar C V cvseshu@optima-da.com, Jamil R. Mazzawi jamil@optima-da.com

Optima Desing Automation Ltd.

Abstract

The RETIME IP is a **new** critical component in OmniVision's **image processing** SoCs, responsible for receiving raw image data from camera sensors, processing it, and storing it into SRAM for consumption by downstream modules. Since the host SoC is classified as ASIL-D, the RETIME IP must adhere to ASIL-D requirements in accordance with ASIL decomposition guidelines set forth in ISO 26262-10:2018, Clause 11. While initial Safety-Mechanisms were designed to meet fault coverage targets, subsequent fault injection analysis revealed the need for additional safety features to achieve the final ASIL-D target of 99% Single Point Fault Metric (SPFM). This paper outlines the methodology employed using a Fault Analysis Platform, to analyze, verify, and achieve stringent fault coverage requirements for automotive display systems. Implementing additional safety mechanism including lock-step and data-path parity improves the SPFM to 99%, with an area overhead of 12.8%.

Keywords: ASIL-D, Fault-Injection-Analysis, ISO-26262, Single-Point-Fault-Metric

---

I. Introduction

In automotive 360-degree surround-view systems, the image sensor SoC acquires raw image data from different sources, performs initial processing, and transmits the processed stream to the Application Processor (AP) for further computation and rendering the in-vehicle displays.

The RETIME-block serves as a timing adjustment unit within the data path to ensure synchronization between upstream image sources and downstream display modules.

Any disruption in this transmission pipeline results in loss of real-time visual feedback, particularly during critical maneuvers such as reversing, thereby introducing severe functional safety hazards. Consequently, both the SoC and RETIME are classified as safety-critical and must adhere to ISO-26262 ASIL-D requirements [1].

II. Safety Architecture and Initial Safety-Mechanisms

The RETIME adjusts internal timing of image streams to meet different video receiver requirements. Its primary purpose is to detect input image-stream timing, store it into a buffer, and adjust critical timing parameters including HREF, VALID, and BLANKING signals. The adjusted image stream is then output to external receivers, ensuring downstream modules can perform synchronized read operations to maintain display integrity.

To meet the ISO=26262 functional safety requirements, the initial RETIME safety-architecture incorporates a multi-layered safety strategy designed to detect and mitigate hardware failures that could compromise data integrity or timing. The baseline safety features include:

- **SRAM Boundary Protection:** Implementation of underflow and overflow detection logic to prevent data corruption during asynchronous read/write operations.
- **Timing Integrity Monitoring:** A dedicated timing check unit for raw_data and extra_info signals to ensure synchronization remains within defined safety limits.
- **Memory Reliability:** An integrated memory monitor utilizing Error Correction Code (ECC) to detect and correct single-bit upsets (SBU) while detecting multi-bit upsets (MBU) within SRAM.

The high-level architectural configuration of RETIME, including integration points of Safety-Mechanisms, is illustrated in Figure 1.

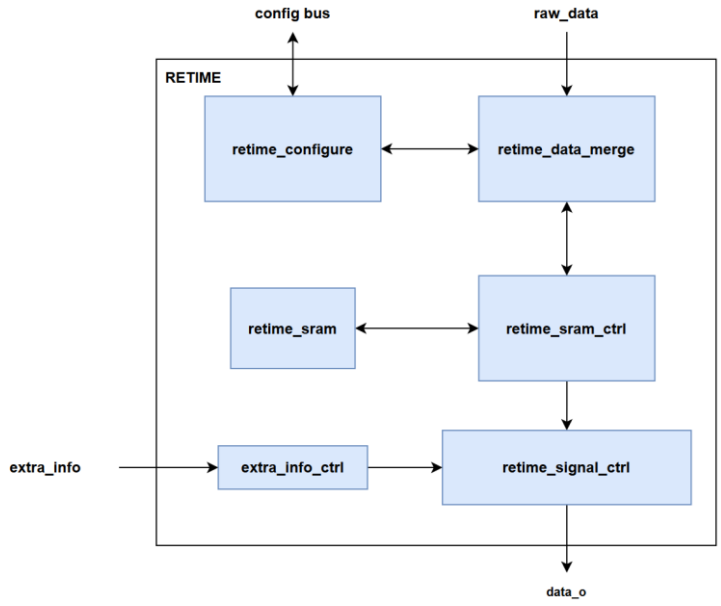


Figure 1: RETIME architecture with integrated Safety-Mechanisms

III. Methodology: Safety Platform Fault Injection Analysis

Evaluating Safety-Mechanisms error detection capability, represented by diagnostic coverage (DC), is essential for ASIL-D compliance. ISO-26262 provides typical DC values for specific Safety-Mechanisms. For example, memory monitors using ECC in SRAMs can achieve 99% DC according to ISO 26262-11: Table 33. However, determining DC values for complex modules with multiple interacting Safety-Mechanisms requires comprehensive fault injection analysis[2].

For ASIL-D certification, the module's Single-Point Fault Metric (SPFM) must exceed 99%. SPFM calculation is based on failure mode classification according to ISO-26262 fault categories.

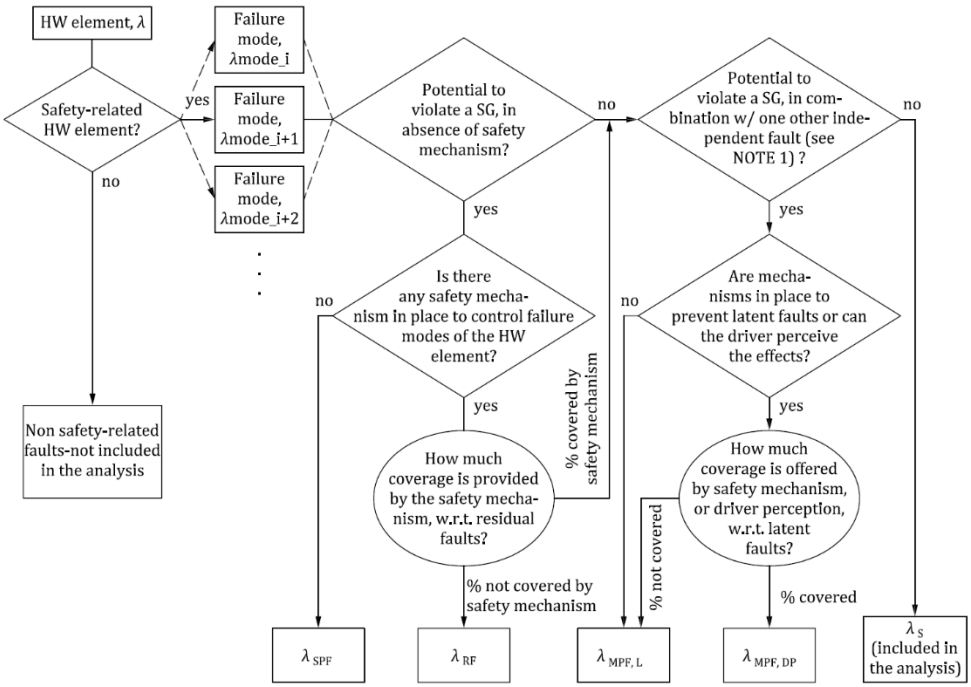


Figure 2: ISO 26262 fault classification flow diagram

We adopted the Optima Safety Platform , OSP, which is certified for use up to ASIL-D per ISO 26262-8:2018, Clause 11, for comprehensive fault injection analysis. In, fault analysis comprises three sequential steps:

1. **Static Analysis:** Classifies faults using Cone of Influence analysis, identifying fault statuses as UI (undetected, unsafe), UV (detected unsafe), SI (safe, irrelevant), and SV (safe, detected).

2. **Constant Analysis:** Determines which faults are masked by constant values in the design.

3. **Hard Error (HE) Fault Simulation:** Injects stuck-at-0/1 errors on cell pins to verify actual fault detection by Safety-Mechanisms and identify residual faults.

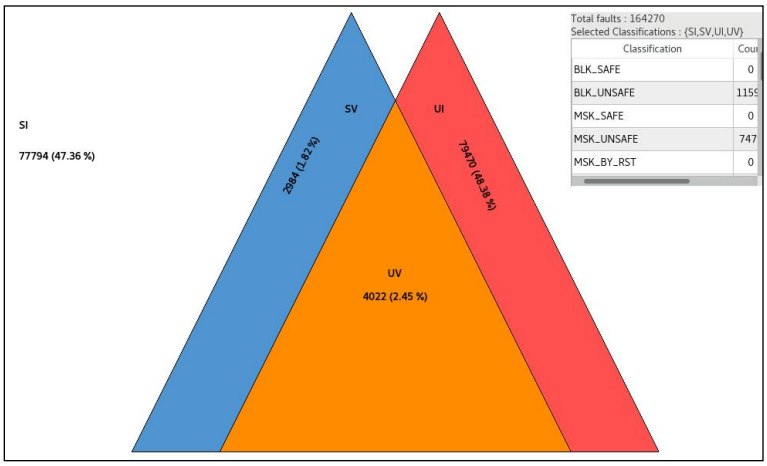


Figure 3: Fault status distribution from static analysis (Design-Version-1)

IV. Results and Analysis

A. Initial Safety Assessment

Static analysis of the original design (Version 1) revealed that 48.38% of faults lacked safety mechanism coverage. Hard error simulation yielded an initial SPFM of only 68%, significantly below the required 99% for ASIL-D compliance[3].

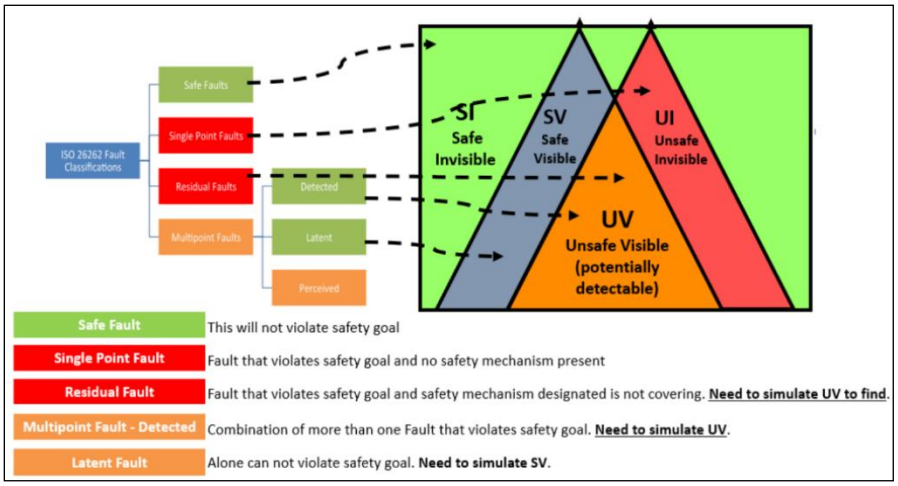


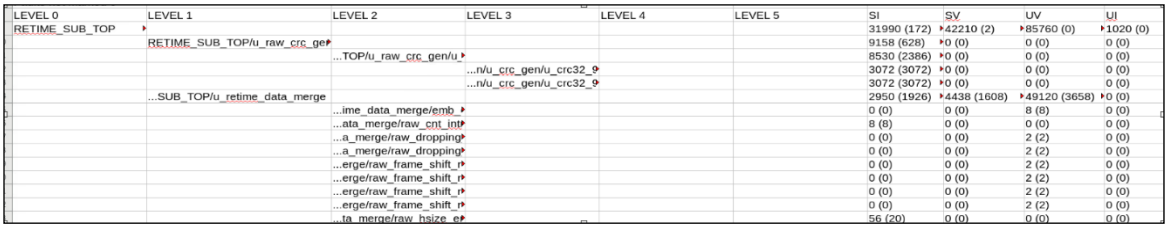
Figure 4: Mapping of fault statuses to ISO 26262 fault classifications

```
Report for instance: RETIME_SUB_TOP
I. Faults considered for SPF analysis(A-B),,161118
     A. Total Faults,164102
     B. Multi-Point Faults Primary(In SM),2984
II. SAFE Faults(C+D+E+I),,109995
     C. User Safe faults,32136
     D. Non Safety Related by SA(SI Faults),77646
     E. Safe marked by CA(by Design&User Const),0
     I. End of Trace SAFE,213
III. DANGEROUS SPF (Single Point Faults),,48698
     F. Single Point Faults(by SA: UI Faults),48698
IV. DANGEROUS UNDETECTED(G+H+J+K+L),,2154
     G. User marked Unsafe,0
     H. Propagated faults,627
     J. End of Trace UNSAFE,507
     K. End OF Trace Time Out,0
     L. CA Unsafe(by Waveform Const),1020
V. DANGEROUS DETECTED(M+N+O+P),,247
     M. Detected Faults,41
     N. Propagated Detected faults,29
     O. Detected Late,31
     P. Detected late and Propagated,146
VI. UNDETERMINED by Engines(Q+R),,24
     Q. Skipped Faults,0
     R. Not Simulated,24
SPFM for RETIME SUB TOP ( 100 * (II+V)/I),,68.0%
```

Figure 5: Hard error simulation results showing initial SPFM of 68%

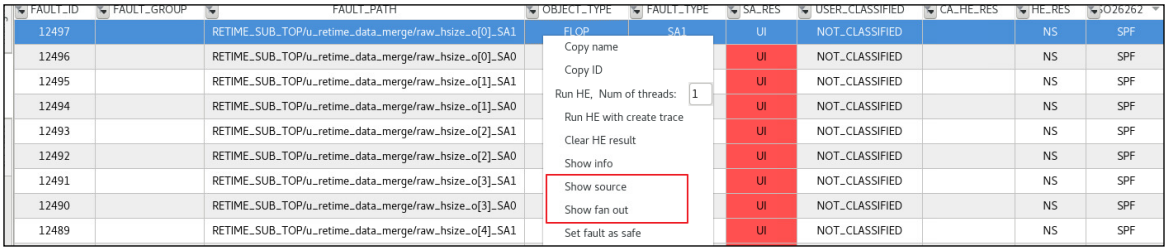
B. Implementation of Additional Safety-Mechanisms

Hierarchical reports identified specific sub-modules lacking coverage, particularly in the data-path and control-logic of the FIFO retime_data_merge.



LEVEL 0	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	SI	SV	UV	UI
RETIME_SUB_TOP						31990 (172)	42210 (2)	85760 (0)	1020 (0)
	RETIME_SUB_TOP/u_raw_crc_ge					9158 (628)	0 (0)	0 (0)	0 (0)
		...TOP/u_raw_crc_gen/u				8530 (2386)	0 (0)	0 (0)	0 (0)
			...n/u_crc_gen/u_crc32_9			3072 (3072)	0 (0)	0 (0)	0 (0)
			...n/u_crc_gen/u_crc32_9			3072 (3072)	0 (0)	0 (0)	0 (0)
	...SUB_TOP/u_retime_data_merge					2950 (1926)	4438 (1608)	49120 (3658)	0 (0)
		...ime_data_merge/emb				0 (0)	0 (0)	8 (8)	0 (0)
		...ata_merge/raw_cnt_int				8 (8)	0 (0)	0 (0)	0 (0)
		...a_merge/raw_dropping				0 (0)	0 (0)	2 (2)	0 (0)
		...a_merge/raw_dropping				0 (0)	0 (0)	2 (2)	0 (0)
		...erge/raw_frame_shift_r				0 (0)	0 (0)	2 (2)	0 (0)
		...erge/raw_frame_shift_r				0 (0)	0 (0)	2 (2)	0 (0)
		...erge/raw_frame_shift_r				0 (0)	0 (0)	2 (2)	0 (0)
		...erge/raw_frame_shift_r				0 (0)	0 (0)	2 (2)	0 (0)
		...ta_merge/raw_hsize_e				56 (20)	0 (0)	0 (0)	0 (0)

Figure 6: hierarchical analysis report identifying uncovered modules



FAULT_ID	FAULT_GROUP	FAULT_PATH	OBJECT_TYPE	FAULT_TYPE	SA_RES	USER_CLASSIFIED	CA_HE_RES	HE_RES	SO26262
12497		RETIME_SUB_TOP/u_retime_data_merge/raw_hsize_o[0]_SA1	FLOP	SA1	UI	NOT_CLASSIFIED		NS	SPF
12496		RETIME_SUB_TOP/u_retime_data_merge/raw_hsize_o[0]_SA0			UI	NOT_CLASSIFIED		NS	SPF
12495		RETIME_SUB_TOP/u_retime_data_merge/raw_hsize_o[1]_SA1			UI	NOT_CLASSIFIED		NS	SPF
12494		RETIME_SUB_TOP/u_retime_data_merge/raw_hsize_o[1]_SA0			UI	NOT_CLASSIFIED		NS	SPF
12493		RETIME_SUB_TOP/u_retime_data_merge/raw_hsize_o[2]_SA1			UI	NOT_CLASSIFIED		NS	SPF
12492		RETIME_SUB_TOP/u_retime_data_merge/raw_hsize_o[2]_SA0			UI	NOT_CLASSIFIED		NS	SPF
12491		RETIME_SUB_TOP/u_retime_data_merge/raw_hsize_o[3]_SA1			UI	NOT_CLASSIFIED		NS	SPF
12490		RETIME_SUB_TOP/u_retime_data_merge/raw_hsize_o[3]_SA0			UI	NOT_CLASSIFIED		NS	SPF
12489		RETIME_SUB_TOP/u_retime_data_merge/raw_hsize_o[4]_SA1			UI	NOT_CLASSIFIED		NS	SPF

Copy name
Copy ID
Run HE, Num of threads: 1
Run HE with create trace
Clear HE result
Show info
Show source
Show fan out
Set fault as safe

Figure 7: Fanout-analysis identifying code coverage gaps

Based on this analysis, we implemented new targeted Safety-Mechanisms:

1) Data-Path Protection: One-bit parity generation for every pixel of input data, propagated throughout the data path[1].

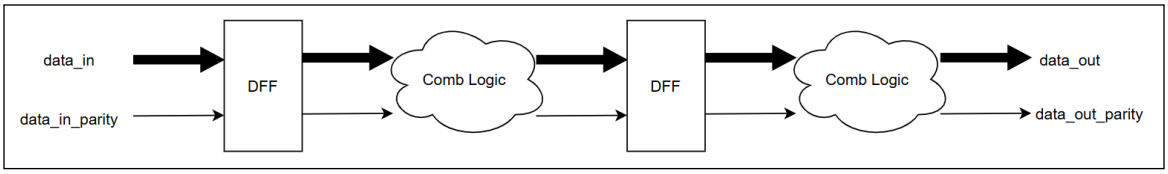


Figure 8: Data path parity protection mechanism

2) Control Logic Protection: Using lock-step for control logic elements. With one-cycle delayed input with error reporting on inconsistency.

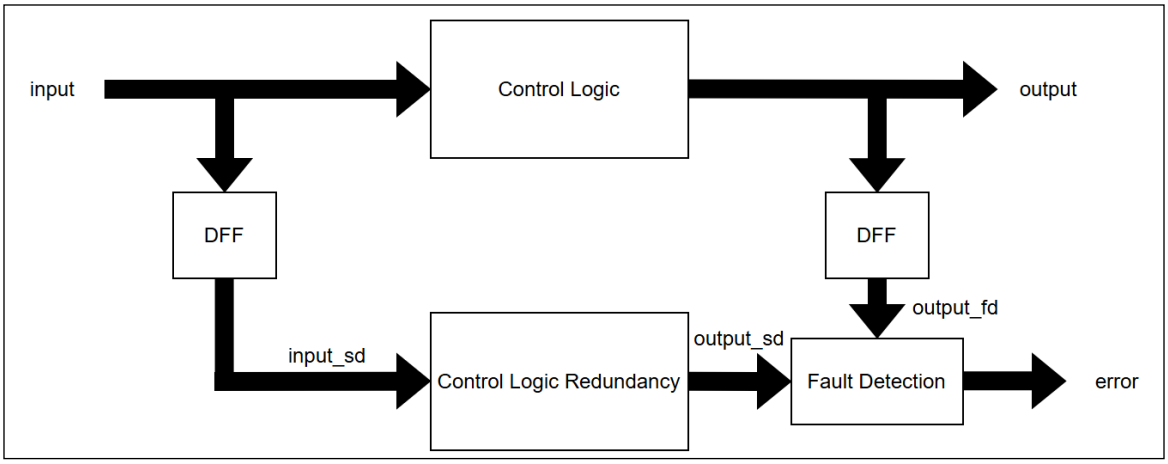


Figure 9: Lock-step redundancy mechanism for control logic protection

C. Verification and Final Results

After implementing additional Safety-Mechanisms, new full-fault-analysis showed the following results:

```
Report for instance: RETIME_SUB_TOP
I. Faults considered for SPF analysis(A-B),,107750
     A. Total Faults,164102
     B. Multi-Point Faults Primary(In SM),56352
II. SAFE Faults(C+D+E+I),,57755
     C. User Safe faults,32136
     D. Non Safety Related by SA(SI Faults),24278
     E. Safe marked by CA(by Design&User Const),0
     I. End of Trace SAFE,1341
III. DANGEROUS SPF (Single Point Faults),,144
     F. Single Point Faults(by SA: UI Faults),144
IV. DANGEROUS UNDETECTED(G+H+J+K+L),,19671
     G. User marked Unsafe,0
     H. Propagated faults,12524
     J. End of Trace UNSAFE,1819
     K. End OF Trace Time Out,7
     L. CA Unsafe(by Waveform Const),5321
V. DANGEROUS DETECTED(M+N+O+P),,30156
     M. Detected Faults,1271
     N. Propagated Detected faults,2539
     O. Detected Late,4828
     P. Detected late and Propagated,21518
VI. UNDETERMINED by Engines(Q+R),,24
     Q. Skipped Faults,0
     R. Not Simulated,24
SPFM for RETIME_SUB_TOP ( 100 * (II+V)/I),,81.0%
```

Figure 10: Fault analysis results after implementation of additional Safety-Mechanisms

These results showed undetected faults due to insufficient detection time windows after violation. Re-running fault-simulation with extended simulation windows (set_stop_sim_time_after_initial_decision = 260,000,000 ps) and additional waveforms significantly improved detected faults.

This setting ensures that the fault detection time interval is limited to 0.26ms, which meets the requirement for fault-tolerant time interval.

```
Report for instance: RETIME_SUB_TOP
I. Faults considered for SPF analysis(A-B),,107750
     A. Total Faults,164102
     B. Multi-Point Faults Primary(In SM),56352
II. SAFE Faults(C+D+E+I),,64882
     C. User Safe faults,34722
     D. Non Safety Related by SA(SI Faults),24278
     E. Safe marked by CA(by Design&User Const),0
     I. End of Trace SAFE,5882
III. DANGEROUS SPF (Single Point Faults),,131
     F. Single Point Faults(by SA: UI Faults),131
IV. DANGEROUS UNDETECTED(G+H+J+K+L),,767
     G. User marked Unsafe,0
     H. Propagated faults,427
     J. End of Trace UNSAFE,191
     K. End OF Trace Time Out,5
     L. CA Unsafe(by Waveform Const),144
V. DANGEROUS DETECTED(M+N+O+P),,41933
     M. Detected Faults,1241
     N. Propagated Detected faults,11562
     O. Detected Late,4828
     P. Detected late and Propagated,24302
VI. UNDETERMINED by Engines(Q+R),,24
     Q. Skipped Faults,0
     R. Not Simulated,24
SPFM for RETIME_SUB_TOP ( 100 * (II+V)/I),,99.0%
```

Figure 11: Final fault-analysis with comprehensive coverage

The combined analysis achieved the critical 99% SPFM target, meeting ASIL-D certification requirements.

D. Area Overhead for additional Safety Mechanism

After the OSP simulation, we analyzed the area overhead introduced by additional safety mechanisms.

These additional safety mechanisms result in 12.85% area overhead relative to the total area, and a 45% overhead with respect to the logic area excluding SRAMs.
For data path parity, 1 bit parity will be added for every 12 bit data. This part of logic can only introduce about 8.3% area overhead.

For the control logics protected by lock-step, their areas without lock-step are much smaller than that of the data path in RETIME module. According to the lock-step mechanism, at least two DFFs are added for each bit of the control signal, which leads to significant area overhead for these logics.

For ASIL-D compliant chips, additional area overhead is unavoidable. For chips with lower ASIL requirements, however, area-intensive safety mechanisms such as lock-step are unnecessary. In these projects, safety mechanisms can be deployed incrementally, with OSP verification applied at each stage to balance SPFM requirements and area overhead.

V. Conclusion

This paper demonstrated a systematic methodology for achieving ASIL-D compliance for safety-critical IP blocks in automotive SoCs. Through comprehensive fault-analysis using the Safety Platform, we identified coverage gaps in the initial RETIME design and implemented targeted Safety-Mechanisms addressing both data path and control logic vulnerabilities. The combination of parity protection for data paths and lock-step redundancy for control logic successfully elevated SPFM from 68% to 99%, meeting stringent ASIL-D requirements. This methodology, leveraging certified fault injection tools and ISO-26262 compliance frameworks, provides a replicable approach for functional-safety verification in automotive display systems and similar safety-critical applications.

References

[1] OmniVision™ Product Manuals, OmniVision Technologies, Inc.

[2] Optima Safety Platform™ User Guide, Version 2.0, Optima Safety Platform Documentation.

[3] ISO 26262:2018, "Road Vehicles – Functional Safety Part 10: Guideline on ISO 26262," International Organization for Standardization, Geneva, Switzerland.

[4] ISO 26262:2018, "Road Vehicles – Functional Safety Part 11: Guidelines on application of ISO 26262 to semiconductors," International Organization for Standardization, Geneva, Switzerland.

For more information about Optima's products, solutions and services,

please contact us at: sales@optima-da.com

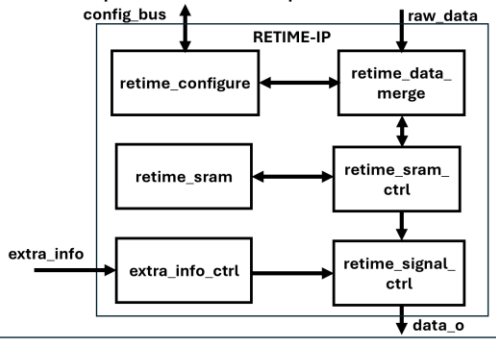
Following is a 6 slides summary of the paper:

Motivation

- ❑ The Image Sensor SoC is critical in 360^{O} surround view system in automotive
  - ➢ Acquires raw image data, processes it and transmits to Application Processor(AP)
  - ➢ Processed information is rendered on to the in-vehicle displays
- ❑ Any disruption in pipeline can results in loss of real-time feedback to the driver
  - ➢ Safety Hazard in critical manoeuvres like reversing
- ❑ RETIME-IP serves as timing adjustment in this pipeline data-path
  - ➢ It ensures synchronization between upstream image source to downstream display modules
- ❑ RETIME-IP is therefore classified as safety critical component to be protected by Safety Mechanisms, with ASIL-D requirements
  - ➢ Timing disorder in the output image can propagate as frame corruption
  - ➢ Potential violation of safety goal

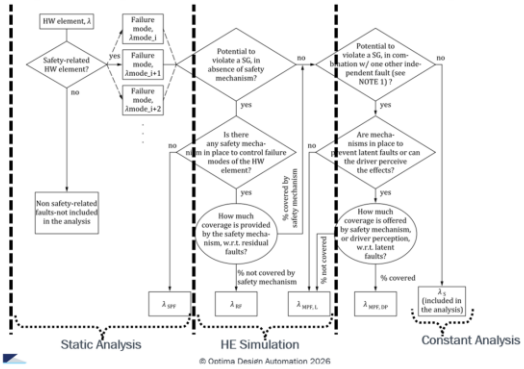
Achieving ASIL-D for RETIME-IP

- ❑ As per Functional Safety requirements of ISO26262 RETIME-IP initially had the following safety mechanisms incorporated
  - ➢ SRAM boundary Protection
  - ➢ Timing integrity monitoring
  - ➢ ECC (Error Correction Code) for memory reliability
- ❑ These initial Safety Mechanisms (SMs) are evaluated
  - ➢ Faut injected FuSa verification as per ISO26262-11:4.8.1
  - ➢ DC (Diagnostic Coverage) Obtained
- ❑ SPFM with initial SMs is computed
  - ➢ Result is only 68%, while ASIL-D requirement is 99%
- ❑ Methodology used to improve initial SM's and introduce additional ones to increase the SPFM and meet the 99% requirement
- ❑ ISO26262 Certified tool to be used for Fault Injection Analysis
  - ➢ Evaluated Tool Confidence level for up to ASIL-D as per ISO26262-8:11



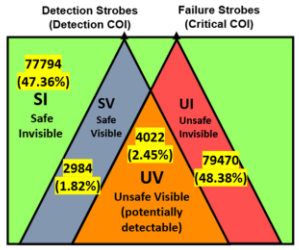
Methodology to achieve ASIL-D

- ❑**Static Analysis:** Classifies faults using Cone of Influence analysis, identifying fault statuses as UI (undetected, unsafe), UV (detected unsafe), SI (safe, irrelevant), and SV (safe, detected).
- ❑**Constant Analysis:** Determines which faults are masked by constant values in the design.
- ❑**Hard Error (HE) Fault Simulation:** Injects stuck-at-0/1 errors on cell pins to verify actual fault detection by Safety-Mechanisms and identify residual faults.

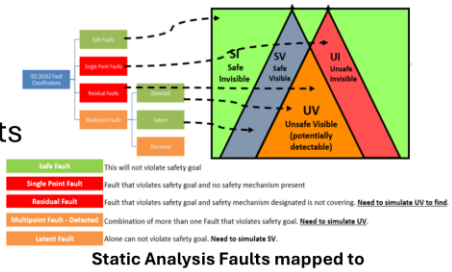


Static Analysis and Fault Mapping

- ❑ Static Analysis classifies faults into
  - ➢ SI: SAFE INVISIBLE
  - ➢ SV: SAFE VISIBLE
  - ➢ UV: UNSAFE VISIBLE
  - ➢ UI: UNSAFE INVISIBLE
- ❑ Mapping of faults with respect to ISO26262 as shown
- ❑ UI Faults which are not detectable mapped to SPF
  - ➢ SPF(Single Point Faults) which don't have Safety Mechanism
- ❑ Identified areas which contributed to UI faults
  - ➢ FIFOs of Data merge areas
- ❑ Implemented additional safety mechanisms
- ❑ Marked faults blocked by Constant Analysis as SAFE



Static Analysis shows Lot of UI faults (48.38%)

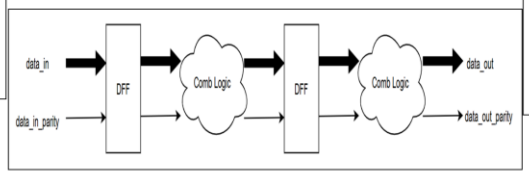


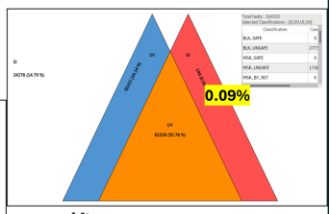
Static Analysis Faults mapped to ISO26262

SPFM increase with new SM: HE sim

Before:
Static Analysis shows Lot of UI faults (48.38%) not covered by existing SMs

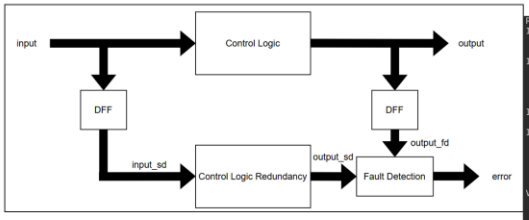
1-bit Parity for every 12-bit. Area Overhead **8.3%↑**





After:
Static Analysis shows negligible UI faults (0.09%) not covered by existing SMs.

```
Report for instance: RETIME_SUB_TOP
I. Faults considered for SPF analysis(A-B),,161118
     A. Total Faults,164102
     B. Multi-Point Faults Primary(In SM),2984
II. SAFE Faults(C+D+E+I),,109995
     C. User Safe faults,32136
     D. Non Safety Related by SA(SI Faults),77646
     E. Safe marked by CA(by Design&User Const),0
     I. End of Trace SAFE,213
III. DANGEROUS SPF (Single Point Faults),,48698
     F. Single Point Faults(by SA: UI Faults),48698
IV. DANGEROUS UNDETECTED(G+H+J+K+L),,2154
     G. User marked Unsafe,0
     H. Propagated faults,627
     J. End of Trace UNSAFE,507
     K. End OF Trace Time Out,0
     L. CA Unsafe(by Waveform Const),1020
V. DANGEROUS DETECTED(M+N+O+P),,247
     M. Detected Faults,41
     N. Propagated Detected faults,29
     O. Detected Late,31
     P. Detected late and Propagated,146
VI. UNDETERMINED by Engines(Q+R),,24
     Q. Skipped Faults,0
     R. Not Simulated,24
SPFM for RETIME_SUB_TOP ( 100 * (II+V)/I),,68.0%
```



Additional Safety Mechanism: Lockstep for the control path.
Area Overhead: **12.85% ↑ of** total area **45% ↑** if mem is not considered

```
Report for instance: RETIME_SUB_TOP
I. Faults considered for SPF analysis(A-B),,107750
     A. Total Faults,164102
     B. Multi-Point Faults Primary(In SM),56352
II. SAFE Faults(C+D+E+I),,64882
     C. User Safe faults,34722
     D. Non Safety Related by SA(SI Faults),24278
     E. Safe marked by CA(by Design&User Const),0
     I. End of Trace SAFE,5882
III. DANGEROUS SPF (Single Point Faults),,131
     F. Single Point Faults(by SA: UI Faults),131
IV. DANGEROUS UNDETECTED(G+H+J+K+L),,767
     G. User marked Unsafe,0
     H. Propagated faults,427
     J. End of Trace UNSAFE,191
     K. End OF Trace Time Out,5
     L. CA Unsafe(by Waveform Const),144
V. DANGEROUS DETECTED(M+N+O+P),,41933
     M. Detected Faults,1241
     N. Propagated Detected faults,11562
     O. Detected Late,4828
     P. Detected late and Propagated,24302
VI. UNDETERMINED by Engines(Q+R),,24
     Q. Skipped Faults,0
     R. Not Simulated,24
SPFM for RETIME_SUB_TOP ( 100 * (II+V)/I),,99.0%
```

Before: SPFM with existing SMs: 68%

After: SPFM with New SMs: 99%

Summary

- ❑ RETIME-IP is critical safety component in the SoC
  - ➢ Need to be ASIL-D compliant
  - ➢ ASIL-D was achieved using the methodology described in the full presentation.
- ❑ Key insights
  - ➢ Faults need to be analyzed in a systematic way rather than fault simulation alone
  - ➢ Important to choose ISO26262 compliant advance fault analysis tools
  - ➢ Decision on the additional safety mechanisms based on the fault classification assessment
  - ➢ Using static analysis to identify safe fault and faults not covered by any-SM proven to be beneficial to reduce the time needed for fault-simulation and debug
  - ➢ Capturing realistic scenarios like lock-step delays to have more faults covered