2025 Design, Automation & Test in Europe Conference (DATE 2025)

Early Functional Safety and PPA Evaluation of Digital Designs

Michelangelo Bartolomucci*, David Kingston†, Teo Cupaiuolo†, Alessandra Nardi†, Riccardo Cantoro*
* Department of Control and Computer Engineering, Politecnico di Torino, Italy
† Synopsys, Inc.

***Abstract*—The use of semiconductor devices in safety-critical scenarios is increasing in both quantity and complexity. This paper presents a novel approach to support safety requirements from RTL exploration through to implementation, with the aid of a Safety Specification Format (SSF), thereby minimizing costly development iterations and reducing the Time-To-Market. An assessment of the results is given for the CV32E40P open source RISC-V processor.**

***Index Terms*—Digital Design Process, Functional Safety, Safety Critical Domain, Selective Hardening, PPA, SSF**

I. Introduction

The complexity of Very Large Scale Integration (VLSI) circuits is increasing, requiring multiple iterations to meet the Power, Performance, and Area (PPA) targets specified for the design. Achieving these metrics necessitates extensive implementation processes, which, in modern designs, can significantly impact Time to Market (TTM) due to high runtimes.

Additionally, circuit hardening is often necessary to meet Functional Safety (FuSa) standards. According to ISO 26262, FuSa ensures the ”absence of unreasonable risk due to hazards caused by malfunctioning behavior” of electrical/electronic systems [1]. FuSa compliance is measured using several metrics: the Single Point Fault Metric (SPFM), which assesses resilience to single-point faults; the Latent Fault Metric (LFM), which evaluates resistance to latent faults; and the Probabilistic Metric of Hardware Failures (PMHF), which quantifies robustness against random faults, expressed in Failures in Time (FIT), or expected failures per billion hours of operation [2]. ASIL (Automotive Safety Integrity Level) compliance ranges from ASIL-A (least strict) to ASIL-D (most strict).

Implementing Safety Mechanisms (SMs) that exploit redundancy can improve reliability at the expense of PPA overhead. Selective hardening approaches, proposed in prior works [3], with selective hardening approaches proposed in [4, 5], aim to address this issue by targeting specific components for hardening, but they generally rely on multiple iterations or user input, limiting their automation potential. Moreover, these methods are applied to Gate-Level netlists.

Prototyping safety mechanisms early in the design process (e.g., at the RTL stage) can help digital designers optimize hardening strategies, reducing late-stage development effort and, consequently, TTM. Some Electronic Design Automation (EDA) tools have addressed the runtime challenge with post-implementation PPA estimators, including support for FuSa flows [6].

This paper introduces an enhanced safety-aware design flow that enables early exploration of both PPA and safety/reliability metrics. The goal is to rapidly assess the impact of safety mechanisms on PPA and define an optimal strategy for meeting the desired ASIL target. Safety mechanisms are specified in a Safety Specification Format (SSF), and once the configuration is finalized, the flow proceeds to implementation. For transient errors, the flow includes a step to identify critical registers for protection. The proposed methodology is implemented on an open-source RISC-V core, where various safety mechanisms are evaluated against different ASIL targets, comparing the PPA of hardened and unhardened designs. Validation is performed through implementation.

II. Proposed Approach

We propose a multistage automated flow Fig. 1 to help RTL designers assess the impact of hardening on both safety and PPA early in the design process, shifting iteration efforts to the exploration phase. The flow begins with a static RTL safety analyzer to calculate SPFM loss data, which is output in a Safety Specification Format (SSF) file.

The SSF format captures safety-related design details using Tcl commands, enabling integration with safety-aware implementation and verification flows. It specifies design properties (e.g., SPFM loss per cell), intents (e.g., applying safety mechanisms to a module or achieving an SPFM target), and associations (e.g., marking a cell for inclusion in a SM).

In the exploration phase, the SSF is input into an RTL implementation metrics estimator. Using fast synthesis techniques, this tool performs multiple PPA evaluations, providing feedback for RTL designers. After the exploration phase, an implementation flow generates the final netlist. A final safety check, performed using the safety static analyzer in Gate-Level mode, verifies the generated netlist’s SPFM coverage.

The methodology is validated through trend comparison, demonstrating the alignment between estimated metrics and actual implementation results.

III. Case Study

The proposed flow was implemented using Synopsys tools but is adaptable to other EDA environments. The implementation metrics estimator utilized Synopsys *RTL Architect*, while critical circuit parts were analyzed using Synopsys *VC SpyGlass Fault Analysis* for RTL and Gate-Level safety verification to achieve better architectural decision making earlier

978-3-9826741-0-0/DATE25/© 2025 EDAA

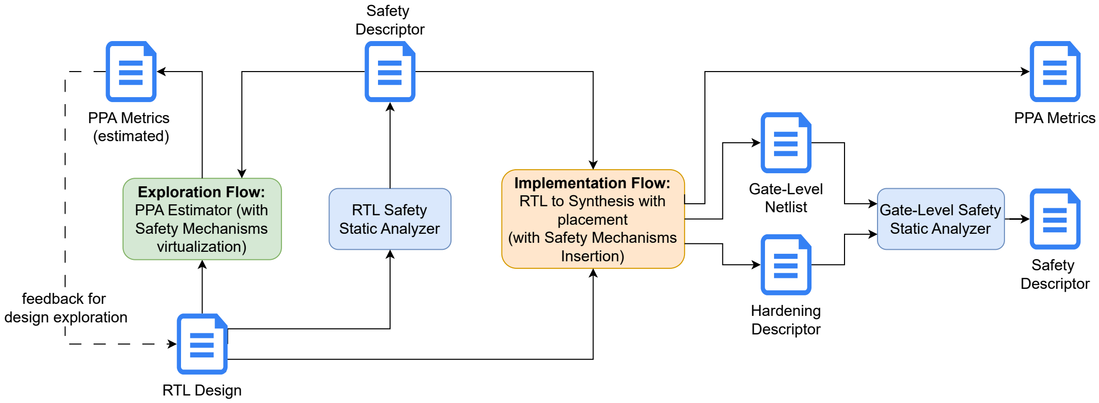
Safety Descriptor
PPA Metrics (estimated)
Exploration Flow: PPA Estimator (with Safety Mechanisms virtualization)
RTL Safety Static Analyzer
Implementation Flow: RTL to Synthesis with placement (with Safety Mechanisms Insertion)
Gate-Level Netlist
Hardening Descriptor
PPA Metrics
Gate-Level Safety Static Analyzer
Safety Descriptor
feedback for design exploration
RTL Design

Fig. 1: Proposed flow for design exploration and implementation

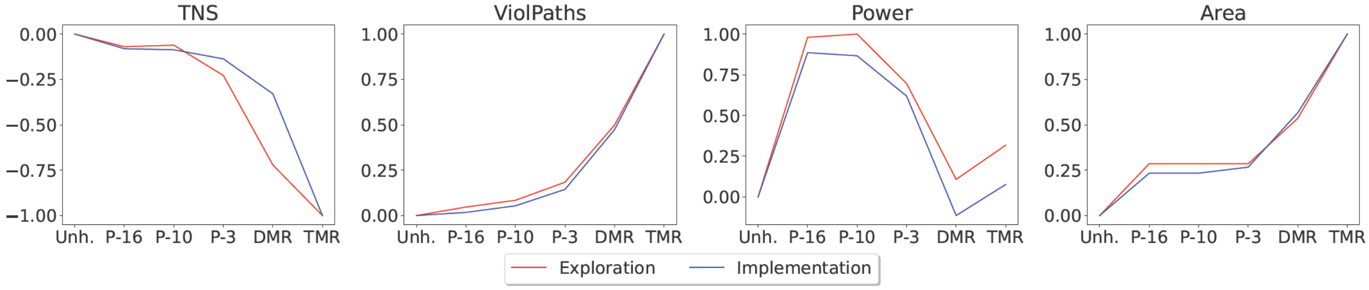

Fig. 2: Exploration versus implementation ASIL-B PPA trends (y-axis normalized metric's values, x-axis hardening type).

in the design cycle. The RTL to synthesis with placement was performed with Synopsys *Fusion Compiler*, using the same synthesis script and library as RTL Architect. The case study was based on the *OpenHW CV32E40P* [7], an open-source RISC-V core, synthesized with a 32nm technology library. ASIL-B compliance was targeted, and various safety mechanisms (SMs), such as TMR, Dual Modular Redundancy (DMR), and XOR-based even-parity encoding/decoding, were tested across different bit slices (e.g., 3, 10, and 16 bits).

We evaluated the impact of different SMs on PPA, considering the extreme case where all selected registers were hardened with the same SM (e.g., TMR or parity). PPA trends were normalized to the range [-1:1], with the unhardened version as the origin. The flow was used to conduct early design explorations, with estimated PPA and safety metrics validated through comparison with implementation results. All experiments were conducted with a 1.00ns target clock period and ASIL-B compliance.

Results, shown in Fig. 2, demonstrate that implementation trends align closely with exploration estimates, validating the flow for architecture and hardening assessments. Any discrepancies were minimal and expected, given that the exploration flow, by design, cannot perform fine-grained optimizations as the final implementation process does.

IV. Conclusions

Synthesis and physical design runtimes are critical factors in determining Time to Market (TTM) for modern digital circuits. Frequent design iterations, driven by verification mismatches or PPA degradation, exacerbate this challenge. This study demonstrates that implementation metrics estimator tools can significantly assist RTL designers by providing accurate PPA predictions for ASIL-hardened designs, reducing exploration time to half of what would be required for full implementation. Future work will focus on developing an adaptive hardening flow that applies appropriate safety mechanisms based on the target module, leveraging these exploration methodologies.

Acknowledgment

This publication is part of the project PNRR-NGEU which has received funding from the MUR – DM 117/2023

References

[1] *ISO 26262-1:2018 - Road Vehicles - Functional Safety*.

[2] A. Nardi et al. “Functional Safety Methodologies for Automotive Applications”. In: *ICCAD 2017*.

[3] I. Polian et al. “Selective Hardening: Toward Cost-Effective Error Tolerance”. In: *IEEE Design & Test of Computers* (2011).

[4] C. Zoellin et al. “Selective Hardening in Early Design Steps”. In: *ETS 2008*.

[5] O. Ruano et al. “A Methodology for Automatic Insertion of Selective TMR in Digital Circuits Affected by SEUs”. In: *IEEE Transactions on Nuclear Science* (2009).

[6] Synopsys. *RTL Architect: Parallel RTL Exploration with Unparalleled Accuracy - White Paper*.

[7] *OpenHW's Group: CV32E40P CPU Core https://github.com/openhwgroup/cv32e40p*.