

# Ensuring Security and Reliability in Space Microprocessors with Hardware-Based Techniques



Alessandro Palumbo  
CentraleSupélec, Inria, CNRS, IRISA  
alessandro.palumbo@inria.fr



**Abstract**—Hardware-based approaches to detect SEUs, SETs, unauthorized program runs, and tampering.

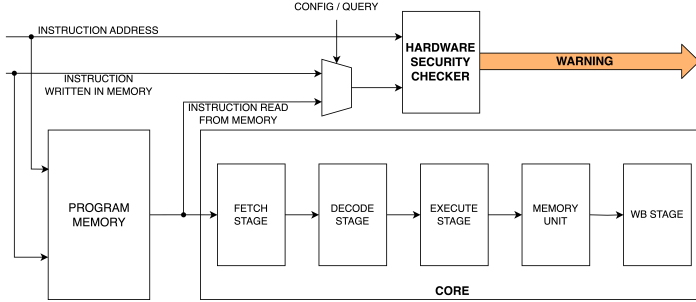


Fig. 1. The Hardware Security Checker implementation

## I. THE HARDWARE SECURITY CHECKER CONFIGURATION

**Configuration:** Recording legitimate instruction-address pairs.

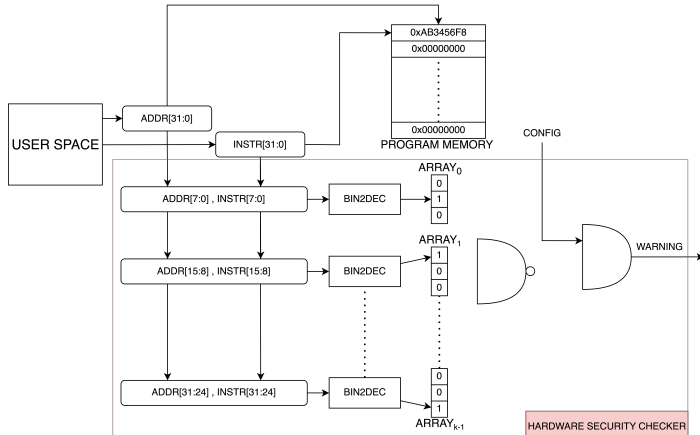


Fig. 2. Configuration phase of the Hardware Security Checker [1]

## II. THE HARDWARE SECURITY CHECKER VERIFICATION

**Verification:** Fetched instructions runtime verification.

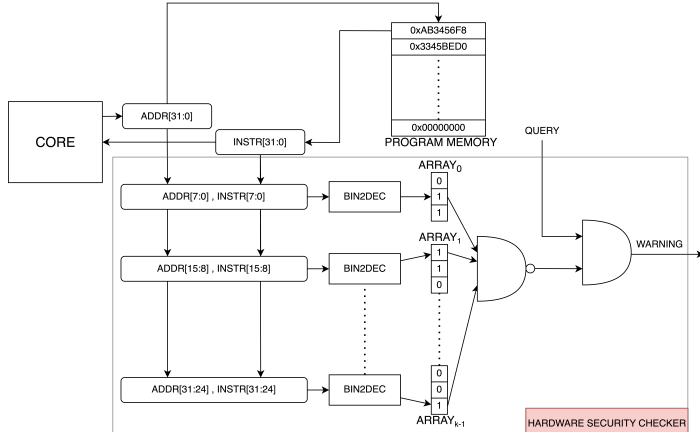


Fig. 3. Verification phase of the Hardware Security Checker [1]

## III. THE HARDWARE SECURITY CHECKER & HAMMING

Enhancing detection capabilities, integrating **Hamming code-based verification**.

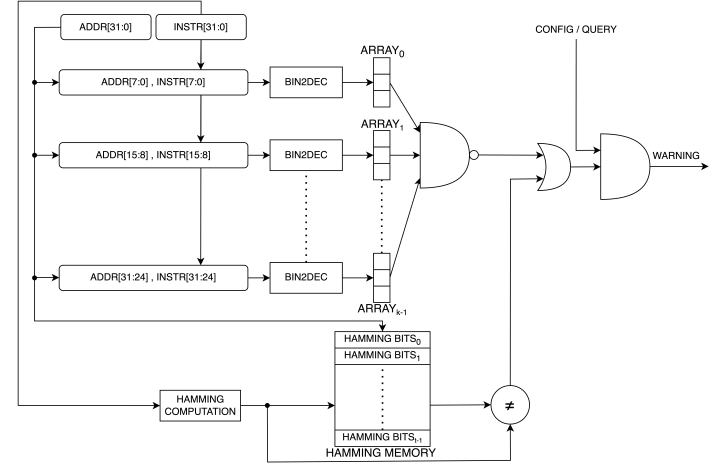


Fig. 4. Improving the Hardware Security Checker [2]

## IV. DETECTING FPGA BITSTREAM TAMPERING WITH ML

Integrating supply chain phases with **ML-based anomaly detection for FPGA security**.

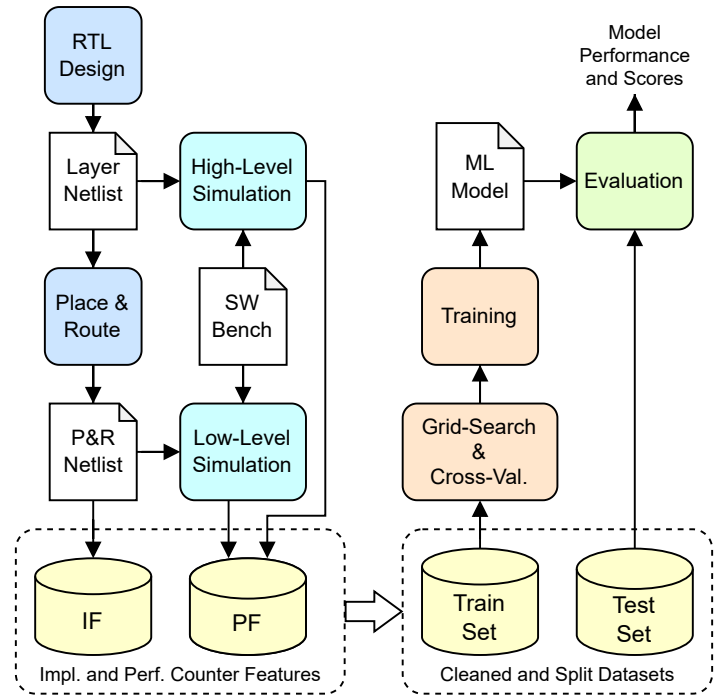


Fig. 5. The workflow for detecting FPGA tampering [3]

TABLE I

BEST ANOMALIES DETECTION RATES AND OVERHEADS

References	Acc.	FP	FN	#LUT	#FF	#BRAM
[1] Fig. 2, 3	100%	0%	0%	75 (0.49%)	31 (0.31%)	8
[2] Fig. 4	100%	0%	0%	82 (0.53%)	31 (0.31%)	8.5
[3] Fig. 5	100%	0%	0%	NA	NA	NA

## REFERENCES

- [1] A. Palumbo et al., "A lightweight security checking module to protect microprocessors against hardware trojan horses," in *DFT*, pp. 1–6, 2021.
- [2] A. Palumbo et al., "Improving the detection of hardware trojan horses in microprocessors via hamming codes," in *DFT*, pp. 1–6, 2023.
- [3] S. Ribes et al., "Machine learning-based classification of hardware trojans in fpgas implementing risc-v cores," in *ICISSP*, pp. 717–724, 2024.