Politecnico di Torino
1859
Dipartimento di Automatica e Informatica

PhD in Computer and Control Engineering
XXXVI cycle

Supervisor
Massimo Violante

Simulation Techniques for Rapid Software Development and Validation

PhD Candidate: Mohammadreza Amel Solouki

1. Motivation

Special measures should be taken to design embedded systems in case safety-critical applications are executed on these systems.

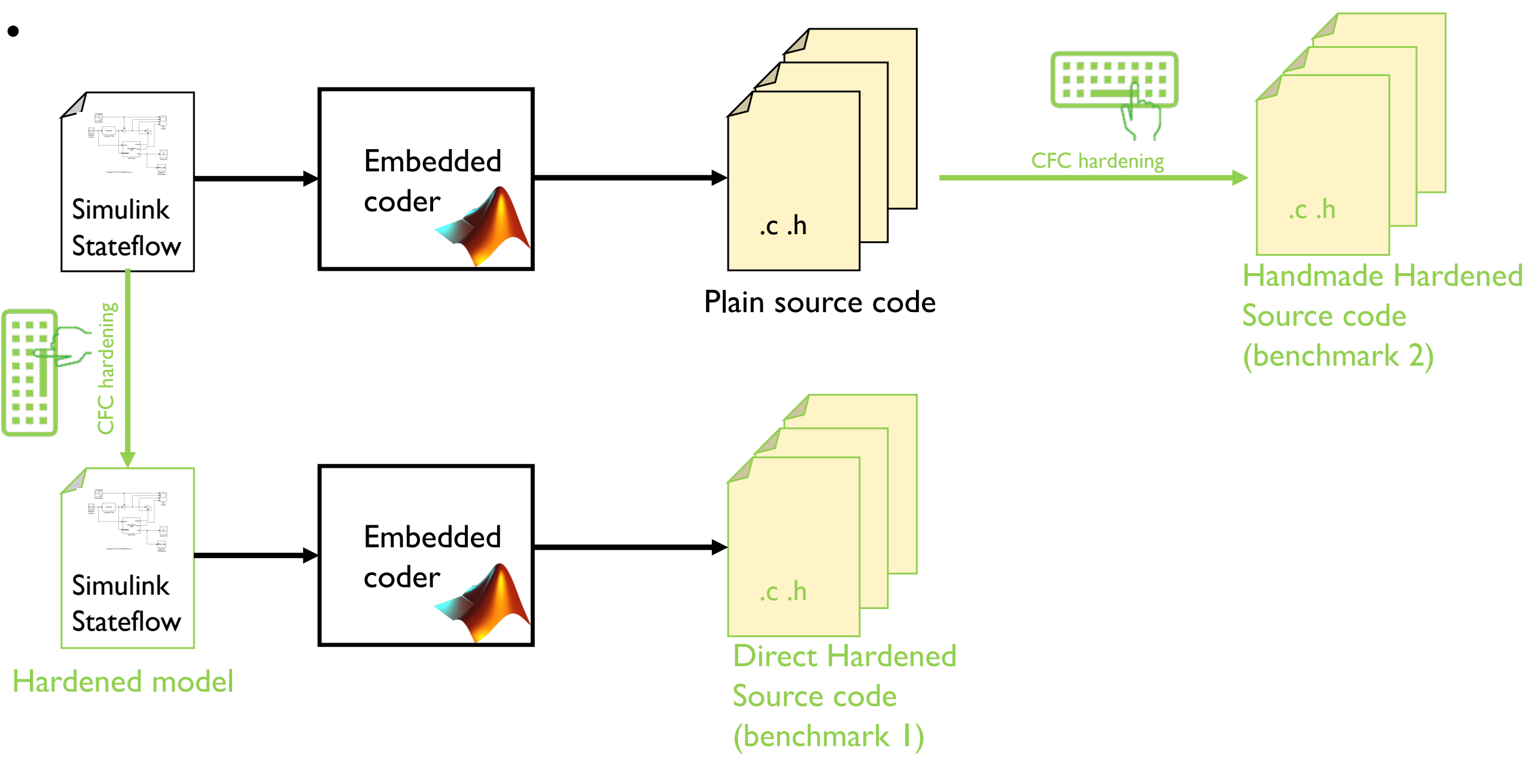
Hardening the system generally means adding redundancy, and this can be implemented by adding extra hardware components or software instructions in the application.

Software redundancy techniques are much more flexible than hardware techniques. They are also much more cost-effective in error detection, especially for high production volumes.

Control Flow Checking (CFC) is considered in our proposal among the various soft error protection techniques available in the literature. In contrast to the common approach, which implements CFC in assembly language, we chose the C programming language to implement CFC.

2. Proposed Methodology

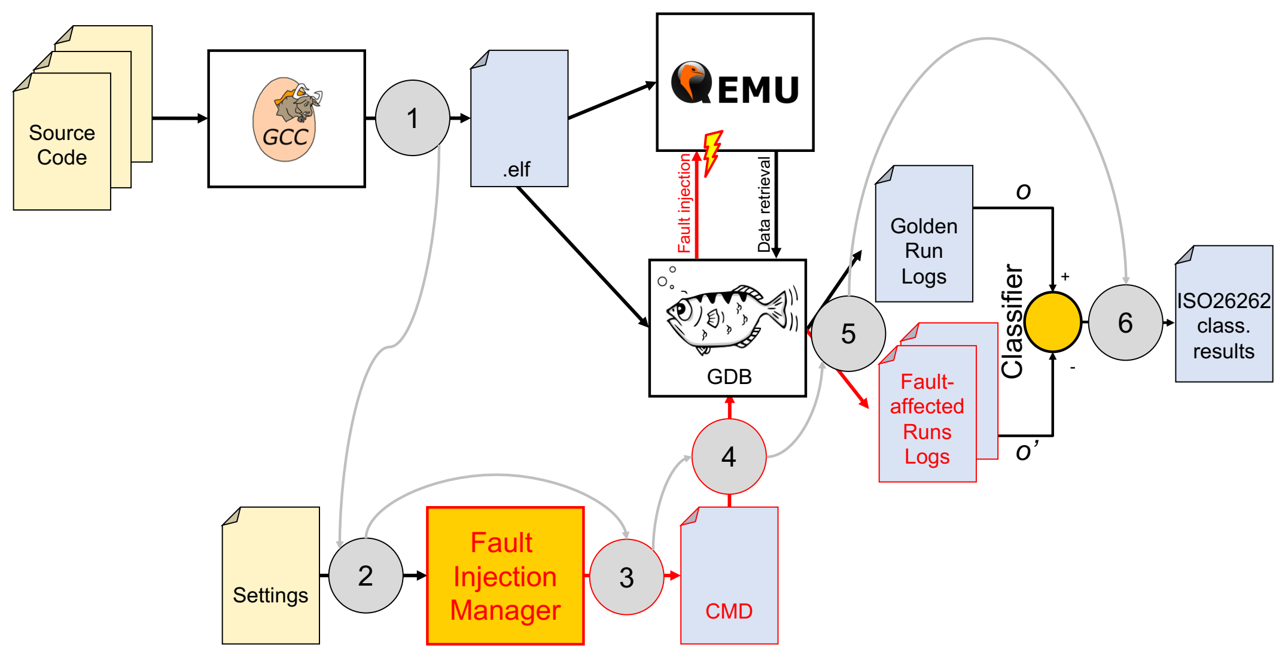
We implemented two benchmark applications by Model-Based Software Design using Simulink Coder. Two established CFC techniques, YACCA and RACFED, have been employed to harden them.



Different ways to harden the application [1]

3. Results

To perform the fault injection campaigns, we used a fault injection tool [1] injecting permanent faults. These affect only one bit of the target register. Furthermore, the experimental results are classified in compliance with ISO 26262.[2,3,4]



The architecture of the used fault injection system [1]

Algorithm (Mask)	Detected			Undetected	
	Safe	Detected	Latent	Residual	False Positive
YACCA (0x3F00)	0.00%	69.20%	16.60%	14.20%	0.00%
YACCA (0x3FFC)	0.00%	62.40%	11.00%	26.60%	0.00%
YACCA(0x3FC0)	4.00%	6.80%	88.30%	4.90%	0.00%
RACFED(0x3F00)	0.00%	60.30%	8.30%	31.40%	0.00%
RACFED(0x3FC0)	0.00%	52.90%	8.60%	38.50%	0.00%
RACFED(0x3FFC)	0.00%	57.20%	6.10%	36.70%	0.00%
RACFED(0x3FC0)	5.20%	5.305	94.50%	0.00%	0.00%

ISO26262 compliant results on Diagnostic coverage on the two benchmarks. [3]
The first benchmark in yellow, the second in white.

4. Conclusion

Our research has focused on assessing the diagnostic coverage of the detection mechanisms designed to recognize random hardware failures affecting digital components and implemented by the embedded software. The test bench was developed to comply with parts 5 and 11 of the ISO 26262 automotive functional safety standard..

5. References

1. J.Sini et al."A Novel ISO 26262-Compliant Test Bench to Assess the Diagnostic Coverage of Software Hardening Techniques against Digital Components Random Hardware Failures", MDPI Electronics 2022, 11(6), 901;
2. **M.Amel Solouki** et al. "Implementation of Control-Flow Checking - A New Perspective Adopting a Model-Based Software Design Approach." Electronics 2022, 11, 3074.
3. **M.Amel Solouki** et al., "High-level Programming in Control Flow Checking for Automotive Embedded Applications Compliant with ISO 26262." Submitted IEEE Access, Under Review
4. **M.Amel Solouki** et al., "Effectiveness of Control Flow Checking Algorithms Using a Model-Based Software Design Approach: An Empirical Study." In 29th IEEE International Conference on Electronics Circuits and Systems October 2022.