

TaMaRa:

An automated triple modular redundancy EDA flow for Yosys

Matt Young

13 August 2024

University of Queensland

Prepared for YosysHQ and Sandia National Laboratories

Table of contents

1. Background
2. TaMaRa methodology
3. Current status & future
4. Conclusion

Background



About me



Matt Young, 21 years old from Brisbane, Australia.

Graduated Bachelor of Computer Science earlier in 2024 from the University of Queensland.

Currently studying Bachelor of Computer Science (Honours) at UQ, which includes a one year research thesis.

Passionate about digital hardware design, embedded systems, high performance/low-level software/hardware. Might take up a PhD in future :)

Fault tolerant computing is important for safety critical sectors (aerospace, defence, medicine, etc.)

Fault tolerant computing is important for safety critical sectors (aerospace, defence, medicine, etc.)

For space-based applications, Single Event Upsets (SEUs) are very common

- Must be mitigated to prevent catastrophic failure
- Caused by ionising radiation

Fault tolerant computing is important for safety critical sectors (aerospace, defence, medicine, etc.)

For space-based applications, Single Event Upsets (SEUs) are very common

- Must be mitigated to prevent catastrophic failure
- Caused by ionising radiation

Even in terrestrial applications, SEUs can still occur

- Must be mitigated for high reliability applications

Fault tolerant computing is important for safety critical sectors (aerospace, defence, medicine, etc.)

For space-based applications, Single Event Upsets (SEUs) are very common

- Must be mitigated to prevent catastrophic failure
- Caused by ionising radiation

Even in terrestrial applications, SEUs can still occur

- Must be mitigated for high reliability applications

ASICs and FPGAs commonly deployed in space (and on Earth)...

Fault tolerant computing is important for safety critical sectors (aerospace, defence, medicine, etc.)

For space-based applications, Single Event Upsets (SEUs) are very common

- Must be mitigated to prevent catastrophic failure
- Caused by ionising radiation

Even in terrestrial applications, SEUs can still occur

- Must be mitigated for high reliability applications

ASICs and FPGAs commonly deployed in space (and on Earth)... but protection from SEUs remains expensive!

Triple Modular Redundancy

TODO describe TMR

Triple Modular Redundancy

TMR can be added manually...

Triple Modular Redundancy

TMR can be added manually...

but this is **time consuming** and **error prone**.

Triple Modular Redundancy

TMR can be added manually...

but this is **time consuming** and **error prone**.

Let's automate it!

TaMaRa methodology

Implement TMR as a pass in an EDA synthesis tool.

- Integrated with the rest of the flow
- Easy to use
- Fully automated

Implement TMR as a pass in an EDA synthesis tool.

- Integrated with the rest of the flow
- Easy to use
- Fully automated

Goal: Pick any design, of any complexity, “press a button” and have it be rad-hardened.

Implement TMR as a pass in an EDA synthesis tool.

- Integrated with the rest of the flow
- Easy to use
- Fully automated

Goal: Pick any design, of any complexity, “press a button” and have it be rad-hardened.

Yosys [1] is the best (and the only) open-source, research grade EDA synthesis tool.

Implement TMR as a pass in an EDA synthesis tool.

- Integrated with the rest of the flow
- Easy to use
- Fully automated

Goal: Pick any design, of any complexity, “press a button” and have it be rad-hardened.

Yosys [1] is the best (and the only) open-source, research grade EDA synthesis tool.

- Proprietary vendor tools (Synopsys, Cadence, Xilinx, etc) immediately discarded
- Can't be extended to add custom passes

Very important prior work done by J. M. Johnson and M. J. Wirthlin [2] at BYU.

Very important prior work done by J. M. Johnson and M. J. Wirthlin [2] at BYU.

TODO algorithm

The TaMaRa algorithm

TODO

Comprehensive verification procedure using formal methods, simulation and fuzzing.

Driven by SymbiYosys tools *eqy* and *mcy*

- In turn driven by theorem provers/SAT solvers

Equivalence checking: Formally verify that the circuit is functionally equivalent before and after the TaMaRa pass.

Equivalence checking: Formally verify that the circuit is functionally equivalent before and after the TaMaRa pass.

- Ensures TaMaRa does not change the underlying behaviour of the circuit.

Equivalence checking: Formally verify that the circuit is functionally equivalent before and after the TaMaRa pass.

- Ensures TaMaRa does not change the underlying behaviour of the circuit.

Mutation: Formally verify that TaMaRa-processed circuits correct SEUs (single bit only)

Equivalence checking: Formally verify that the circuit is functionally equivalent before and after the TaMaRa pass.

- Ensures TaMaRa does not change the underlying behaviour of the circuit.

Mutation: Formally verify that TaMaRa-processed circuits correct SEUs (single bit only)

- Ensures TaMaRa does its job!

TaMaRa must work for *all* input circuits, so we need to test at scale.

TaMaRa must work for *all* input circuits, so we need to test at scale.

Idea:

1. Use Verismith [3] to generate random Verilog RTL.
2. Run TaMaRa synthesis end-to-end.
3. Use formal equivalence checking to verify the random circuits behave the same before/after TMR.

TaMaRa must work for *all* input circuits, so we need to test at scale.

Idea:

1. Use Verismith [3] to generate random Verilog RTL.
2. Run TaMaRa synthesis end-to-end.
3. Use formal equivalence checking to verify the random circuits behave the same before/after TMR.

Problem: Mutation

TaMaRa must work for *all* input circuits, so we need to test at scale.

Idea:

1. Use Verismith [3] to generate random Verilog RTL.
2. Run TaMaRa synthesis end-to-end.
3. Use formal equivalence checking to verify the random circuits behave the same before/after TMR.

Problem: Mutation

- We need valid testbenches for these random circuits, how would we generate that?
- Under active research in academia (may not be possible at the moment)

We want to simulate an SEU environment.

- UQ doesn't have the capability to expose FPGAs to real radiation
- Physical verification is challenging (how do you measure it?)

We want to simulate an SEU environment.

- UQ doesn't have the capability to expose FPGAs to real radiation
- Physical verification is challenging (how do you measure it?)

Use one of Verilator, Icarus Verilog or Yosys' own cxxrtl to simulate a full design.

- Each simulator has different trade-offs
- Currently considering picorv32 or Hazard3 as the DUT

We want to simulate an SEU environment.

- UQ doesn't have the capability to expose FPGAs to real radiation
- Physical verification is challenging (how do you measure it?)

Use one of Verilator, Icarus Verilog or Yosys' own cxxrtl to simulate a full design.

- Each simulator has different trade-offs
- Currently considering picorv32 or Hazard3 as the DUT

Concept:

- Iterate over the netlist, randomly consider flipping a bit every cycle
- Write a self-checking testbench and ensure that the DUT responds correctly

Technical implementation

Currently implemented in C++20, using CMake.

Technical implementation

Currently implemented in C++20, using CMake.

Load into Yosys: `plugin -i libtamara.so`

Technical implementation

Currently implemented in C++20, using CMake.

Load into Yosys: `plugin -i libtamara.so`

TMR is implemented as two separate commands: `tmr` and `tmr_finalise`

Technical implementation

Currently implemented in C++20, using CMake.

Load into Yosys: `plugin -i libtamara.so`

TMR is implemented as two separate commands: `tmr` and `tmr_finalise`

Run `tmr` after synthesis, but before techmapping.

Technical implementation

Currently implemented in C++20, using CMake.

Load into Yosys: `plugin -i libtamara.so`

TMR is implemented as two separate commands: `tmr` and `tmr_finalise`

Run `tmr` after synthesis, but before techmapping.

Run `tmr_finalise` just before techmapping (ensuring no more optimisation passes will run).

Current status & future

TODO

Mostly focused around literature reviews, scoping out the problem, formulating requirements, etc.

Skeleton plugin does exist.

This will be implemented for my Honours thesis over the next 1 year.

- Honours is kind of like mini masters, it's an Australia-specific thing.
- Supervised by Assoc. Prof. John Williams (former PetaLogix, Xilinx)

This will be implemented for my Honours thesis over the next 1 year.

- Honours is kind of like mini masters, it's an Australia-specific thing.
- Supervised by Assoc. Prof. John Williams (former PetaLogix, Xilinx)

Programming hopefully finished *around* January 2025.

This will be implemented for my Honours thesis over the next 1 year.

- Honours is kind of like mini masters, it's an Australia-specific thing.
- Supervised by Assoc. Prof. John Williams (former PetaLogix, Xilinx)

Programming hopefully finished *around* January 2025.

Ideally, TaMaRa will be released open-source under the MPL 2.0.

- Pending university IP shenanigans...

Conclusion

TODO

- D. Shah, E. Hung, C. Wolf, S. Bazanski, D. Gisselquist, and M. Milanovic,
- [1] “Yosys+nextpnr: an Open Source Framework from Verilog to Bitstream for Commercial FPGAs,” *CoRR*, 2019, [Online]. Available: <http://arxiv.org/abs/1903.10407>
- J. M. Johnson and M. J. Wirthlin, “Voter insertion algorithms for FPGA designs using triple modular redundancy,” in *Proceedings of the 18th annual ACM/SIGDA international symposium on Field programmable gate arrays*, in FPGA '10. ACM, Feb. 2010. doi: 10.1145/1723112.1723154.
- [2]
- Y. Herklotz and J. Wickerson, “Finding and Understanding Bugs in FPGA Synthesis Tools,” in *ACM/SIGDA Int. Symp. on Field-Programmable Gate Arrays*, in FPGA '20. Seaside, CA, USA: ACM, 2020. doi: 10.1145/3373087.3375310.
- [3]

Thank you!

Any questions?