Introducing Scalable New Core IP for Mission Critical Use

Murali Vijayaraghavan
Principal Engineer, Formal Methodology Group
Mission-critical SoC Markets

Automotive
- ISO 26262
- 34B

Avionics
- DO-254
- DO-178
- 2.6B

Industrial
- IEC 61511
- IEC 61513
- 19B

Medical
- IEC 62304
- 4B

Robotics
- IEC 62061
- ISO 13849
- 7.2B
Requirements for Automotive safety certification

• Functional Correctness:
  – No design bugs or systematic failures

• Functional Safety (ISO 26262):
  – Low and graceful failures due to random transient errors
    • Automotive Safety Integrity Levels (ASIL) define random failure rates

• Security (ISO / SAE 21434):
  – No risks of cyber-attacks on vehicles
New mission-critical design methodology

Legacy methodology

- **CPU**: Build for high volume markets
- **Retrofit**: Add safety mechanisms to existing cores
- **Certify**: Get functional safety certification

Build from ground up, beyond PPA

- **Security**: 100% adherence to functional spec
- **Functional safety enabled designs**

**SiFive Apex**
## Achieving Functional Correctness

<table>
<thead>
<tr>
<th></th>
<th>Traditional Verification</th>
<th>Model Checking</th>
<th>Proof-assistant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Effort</td>
<td>High</td>
<td>Medium to High</td>
<td>Medium</td>
</tr>
<tr>
<td>Time to achieve functional correctness goals</td>
<td>Slow</td>
<td>Slow</td>
<td>Fast</td>
</tr>
<tr>
<td>100% Guarantee</td>
<td>x</td>
<td>x</td>
<td>✓</td>
</tr>
</tbody>
</table>
Kami – A new methodology for formal verification

Kami RISC-V Formal Spec

Mechanically checked

Proof certificate (semi-automatic)

Kami RISC-V core Implementation

Compiler

https://github.com/sifive/Kami

https://github.com/sifive/RiscvSpecFormal

Verilog for RISC-V core
Single Formal Spec to rule them all

Kami RISC-V Formal Spec

- Kami RISC-V core Implementation (embedded)
- Kami RISC-V core Implementation with address translation
- Kami RISC-V core Implementation with PMP support

Rigorously tested and validated
Formal Verification of Generators

Kami RISC-V Formal Spec

Kami RISC-V In-order core generator

Kami RISC-V In-order 3-stage embedded core

Kami RISC-V Dual issue In-order 8-stage application core

Kami RISC-V OOO core generator

Kami RISC-V 3-wide OOO application core

Kami RISC-V 4-wide OOO application core
Achieving Functional Correctness

<table>
<thead>
<tr>
<th>Human Effort</th>
<th>Traditional Verification</th>
<th>Model Checking</th>
<th>Proof-assistant</th>
<th>Kami</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to achieve functional correctness goals</td>
<td>High</td>
<td>Medium to High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>100% Guarantee</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Proves Generators</td>
<td>✗</td>
<td>✗</td>
<td>Enables</td>
<td>✗</td>
</tr>
</tbody>
</table>
Introducing Functional Safety Partner Resiltech
ResilTech s.r.l.

- Design of Safe System
- Verification & Validation & Safety
- Security Assessment

SW Safety • Research & Development
SoC Diagnostic Software •
Certification •
Training •

ISO TC22/SC32/WG6
ISO26262
ISO21448 (SOTIF)

Automotive
Industrial

Railway
ResilTech will enable SiFive in achieving successfully deployment of their RISC-V solutions in mission-critical application thanks to

- Key people with +20 years experience in safety assessment
- High technical expertise of CPUs, safety software, and complex SoC architectures
- Safety analysis supported by state of the art and custom tools and methodologies
- Directly supporting SiFive customers (SoC or system levels) to achieve Safety Compliance
Summary

New blueprint for mission-critical markets built from the ground up

• Brand new design methodology for mission-critical workload optimized cores
  – Fully formally verified core generators based on open-source Kami technology

• Introducing SiFive Apex products in 2020 with lead partners and customers