Locked out by Latch-up? An Empirical Study on Laser Fault Injection into Arm Cortex-M Processors

Bodo Selmke, Kilian Zinnecker, Philipp Koppermann, Katja Miller, Johann Heyszl, Georg Sigl, 09/13/2018
Tested Microcontroller

We tested four different non-security microcontrollers for their suitability as LFI test devices:

- ST microelectronics STM32-F0 (ARM Cortex-M0)
- ST microelectronics STM32-F4 (ARM Cortex-M4)
- NXP LPC11E14 (ARM Cortex-M0)
- Infineon XMC1401 (ARM Cortex-M0)
Effect No. 1: Fault Injection
Effect No. 1: Fault Injection

6T-SRAM cell
Effect No. 2: Latch-up

Latch-up locked? | BS | 09/13/2018 | 5

© Fraunhofer
Test Setup

- Wavelength 1064 nm
- Pulse length 800 ps
- Spot size of approx. 4 µm
- Laser scanner with 100 nm positioning precision
- Tested four microcontrollers on their susceptibility to LFI
- Interfacing via SWD / OpenOCD
- Backside fault injection
- Monitoring of the supply voltage
Infineon XMC1401 – ARM Cortex M0
Test for SRAM and Register File faults

Left: Full die scan
Right: Zoom on the register file

Chip hardly affected by Latch-Ups.
Faulting of the Register File and SRAM is feasible without any limitations.
**NXP LPC11E14 – ARM Cortex M0**

**Test for Register File faults**

*Left:* Coarse scan of Register File

*Right:* Detailed scan with **200 nm** resolution

Distinguishable Set- and Rst-Fault sensitive spots, not affected by Latch-Ups.
NXP LPC11E14 – ARM Cortex M0

Test for SRAM faults

Full die scan

Detailed scan with 200 nm resolution

STM32F0 – ARM Cortex M0

Test for SRAM faults

Scan of the SRAM section with various pulse energies

Laser illumination generates only Latch-Ups, hence **no Fault Injection was possible**. Test with increasing pulse energies shows, that there is no transition from FI to LU.
STM32F0 – ARM Cortex M0

Test for faults in the Register File

Detailed scan of a sector in the core area

*Left:* Test for Set-Faults

*Right:* Test for Rst-Faults

Register File highly susceptible for the generation of Latch-Ups.
However, sporadically Fault Injections (Rst only) at the border of the core area were feasible.
STM32F4 – ARM Cortex M4

Test for SRAM and Register File faults

Fault in SRAM is feasible without limitations. However, Fault injection in SRAM region generates mostly Latch-Ups.
## Comparison

<table>
<thead>
<tr>
<th></th>
<th>STM32F0</th>
<th>STM32F4</th>
<th>LPC11E14</th>
<th>XMC1401</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SRAM</strong></td>
<td>LU</td>
<td>FI</td>
<td>LU / FI</td>
<td>FI</td>
</tr>
<tr>
<td><strong>Register File</strong></td>
<td>LU / FI</td>
<td>LU / FI</td>
<td>FI</td>
<td>FI</td>
</tr>
<tr>
<td><strong>Suitability as</strong></td>
<td>low</td>
<td>medium</td>
<td>high</td>
<td>high</td>
</tr>
<tr>
<td><strong>non-security LFI test device</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Effect of LFI into different circuit parts (LU for latch-up, FI for successful fault injection, n/a for no results)
Conclusion

- Latch-Up sensitivity seems to be a major issue on certain devices
- Hence, LFI-based attacks seem not always to be feasible
- Highly different behavior on different devices
- Latch-up sensitive manufacturing process could be used as countermeasure?
Contact Information

Bodo Selmke
Department Hardware Security
Fraunhofer-Institute for
Applied and Integrated Security (AISEC)
Address: Parkring 4
85748 Garching (near Munich)
Germany
Internet: http://www.aisec.fraunhofer.de
Phone: +49 89 3229986-132
Fax: +49 89 3229986-222
E-Mail: bodo.selmke@aisec.fraunhofer.de