2021



IC Security Verification of Fault Injection Side-Channel Attack in Semiconductors

WHITE PAPER

OPTIMA DESIGN AUTOMATION
www.optima-da.com

April 2021

Copyright Optima Design Automation ©2021 *Optima Confidential*

IC-Security Verification of Fault-Injection Side-Channel Attack in Semiconductors

INTRODUCTION

Semiconductor security has become a significant concern in chip design, as more security-critical applications have arisen. Examples include the protection of safety critical (e.g. automotive) devices from malicious control takeover, revealing secrets defense related devices, accessing un-encrypted keys and other assets in smart-card chips, mining private data, chip-counterfeiting and even hacking into election machines. According to a recent study by Siemens EDA, and Wilson Research Group [1], 54% of ASIC/IC projects are implementing hardware security features that require verification.

The range of potential security vulnerabilities in a device that must now be countered is broad. Designing security safeguards into a security sensitive semiconductor, and verifying that it is impervious to attack, is a complex and challenging endeavor. Vulnerabilities come in a number of shapes and sizes, and the ingenuity of hackers at identifying and exploiting any weakness continuously evolves.

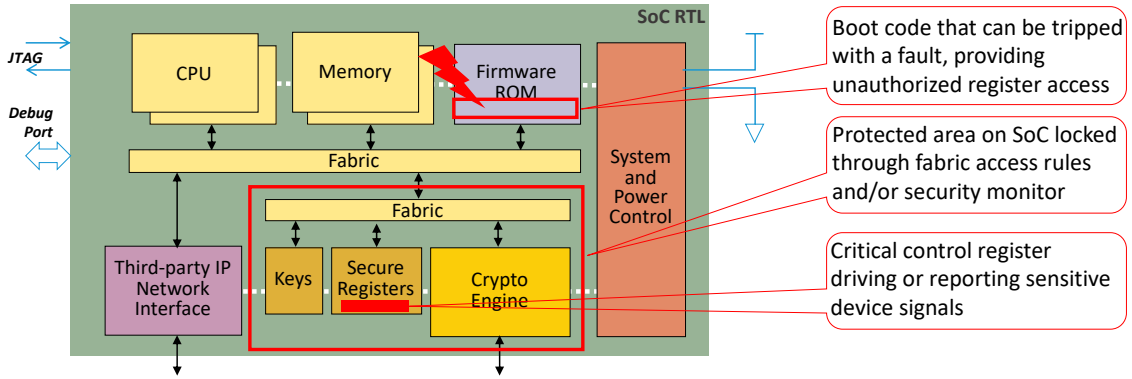


Copyright Optima Design Automation ©2021 *Optima Confidential*

FAULT-INJECTION SIDE-CHANNEL ATTACK

One method of attack that has achieved notoriety is a side-channel attack that uses fault injection to disrupt normal device behavior in such a way that it corrupts the operation of security safe-guards to access key data, control structures, keys or other secure assets. Once this is done, usually at the hackers' labs, the device is compromised and hackers may be able to use the information they discovered to attack similar devices within the applications they are targeting.

In [2], Wiersa and Pareja discuss how effective this fault injection method of attack is in ISO 26262 automotive devices. In this case they looked at the disruption of a UDS communication protocol using a carefully placed fault that stalled an "access-granted" signal. The same method can be used, for example, to disrupt the operation of a system boot process allowing access to critical firmware, or to upset the addressing of critical memory space to acquire private data or secure codes.



Faults may be injected into a device during a "sensitive" period of time (such as the boot process) to trigger the appropriate disruption. They could be introduced using: (1) voltage glitching on the power rails, (2) tempering with clock pins, (3) supplying an electro-magnetic pulse, (4) laser glitching and other methods [3]. If a particular time period for a vulnerable function, such as a UDS communication window, is known then faults may be injected at a variety of moments during this period until an opening is triggered.

These hacks are not performed by a novice hacker, rather by large, organized, well financed engineering teams as the rewards may be great.

Copyright Optima Design Automation ©2021 *Optima Confidential*

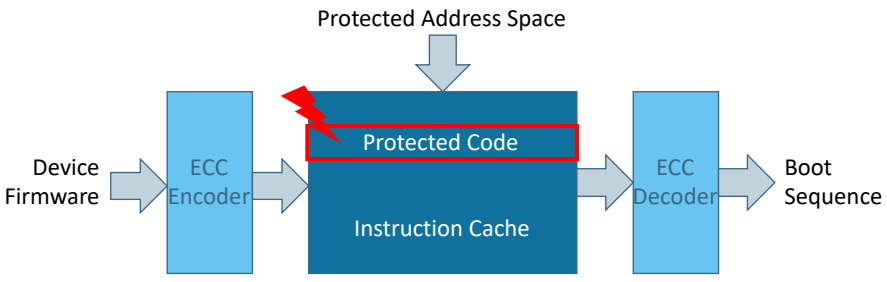
VERIFICATION OF SECURITY PROTECTIONS

Verifying a device to ensure that security vulnerabilities do not exist is a difficult challenge. Unlike most "positive" verification operations, where the existence of some correct functionality is being checked, security verification is a "negative" verification process, where the check is to make sure a specific event sequence cannot occur regardless of other operational detail of the device, including random bit-flips at certain random flip-flops at certain random times. The problem with negative verification in this case is that every possible vulnerability that can be envisaged must be tested. The engineer must predict all these vulnerabilities, which requires an unrealistic imagination of all the possible methods that the device might be hacked.

To verify the protection against fault injection hacking, possibly a better verification approach is to perform fault-injection simulation in a manner similar to the hacker's own methods. Fault-simulation can be performed on every key signal and signal combination and protection added where such a fault or fault-combination can cause harm. For safety critical devices, particularly those for automotive, this is analogous to the ISO 26262 process that must be undertaken to protect the device from incorrect operation due to **soft-errors**, or "bit flips" caused by environmental effects.

To perform this task, fault simulation may be used to verify the design while injecting faults in all possible signals. This is a very time-consuming task so to perform it in a reasonable amount of time, high-performance fault simulation technology is required. Assuming this may be executed quickly enough, then critical fault locations may be protected using a "security mechanism," analogous to a safety mechanism in safety critical designs. This security mechanism would correct the flipped bit, or detect an attack in progress and take the right protective measures. Fault simulation may be used to test that the security mechanism works under all conditions.

For the fault simulation to be efficient, some pre-simulation static analysis is required that would identify the entire fault list that should be examined. This analysis function will test the design and examine logic cones that drive specific critical fault instances to ensure that key faults are included in the fault list, while redundant faults are omitted.



Fault simulation verifies injected fault corrected by Error Correction Code (ECC) decoder

Copyright Optima Design Automation ©2021 Optima Confidential

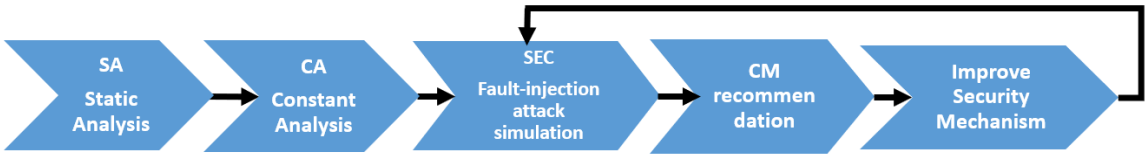
INTRODUCING OPTIMA-SEC™

Optima Design Automation has specialized in this fault simulation and static analysis technology, see [4]. Having already proven this approach for ISO 26262 functional safety verification. Together with Optima's team expertise in Security verification since 2012, see [5], Optima is launching its dedicated security analysis tool, Optima-SEC. Using Optima-SEC, security verification can be accomplished within a reasonable schedule, a task not possible using current tools.

Optima-SEC is a dedicated tool for security verification. It is built on top of Optima's FIE (Fault Injection Engine) technology featuring an engine with orders of magnitude faster fault-simulations, combined with specialized smart-algorithms that perform multiple bit-flips in a random fashion imitating hacker attack. Combining these two technologies allows the simulation of millions of potential attacks to assess the design vulnerabilities and produce database driven recommendations to improve it.

Using Optima-SEC, verification engineers not only verify their security measures, but can also discover vulnerabilities in those mechanisms. Recommendations from Optima-SEC CM technology are used to improve them in a silicon cost-effective manner.

The security verification process goes through five steps of: Static Analysis, Constant Analysis, Fault-injection attack simulation, Examining CM recommendations, implementing them and repeating as needed.



Using Optima's Coverage Maximizer technology, users can identify "hot-points" in the design where a significant number of faults can cause operational issues. Leveraging Artificial Intelligence (AI) approaches, rules are applied to these hot points that, if violated, will indicate a potential vulnerability. These techniques allow a high degree of automation to be applied in the detection and repair of complex vulnerabilities.

SUMMARY:

Security is becoming a necessary aspect of semiconductor development, requiring complex, specialized verification hard to achieve with today's tooling. Optima has applied their next-generation fault simulation technology to this issue, targeting common, notorious security vulnerabilities with a highly automated approach that provides a rapid and high-quality solution.

Copyright Optima Design Automation ©2021 *Optima Confidential*

REFERENCES

[1] Foster, Harry, Part 7: The 2020 Wilson Research Group Functional Verification Study, December 2020

[2] Wiersma, N., and Pareja, R. Safety != security: On the resilience of ASIL-D certified microcontrollers against fault injection attacks. In 2017 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2017, Taipei, Tai- wan, September 25, 2017 (2017), IEEE Computer Society, pp. 9–16.

[3] Bhunia, Swarup and Tehranipoor, Mark, Hardware Security, A Hands-on Learning Approach. 2019, p 209-210

[4] www.Optima-DA.com

[5] Hanna, Ziyad and Mazzawi, Jamil, Formal Analysis of Security Data Paths in RTL Design, 2012 at Haifa Verification Conference (Link https://www.research.ibm.com/haifa/conferences/hvc2012/papers/HVC2012_jamil_mazzawi.pdf)

Copyright Optima Design Automation ©2021 ***Optima Confidential***