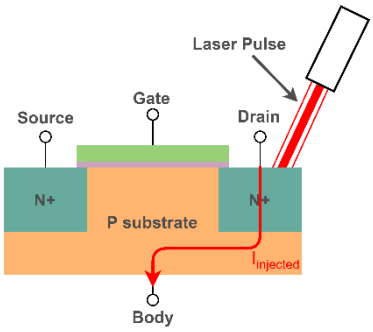
Caspia Technologies

AFIx:

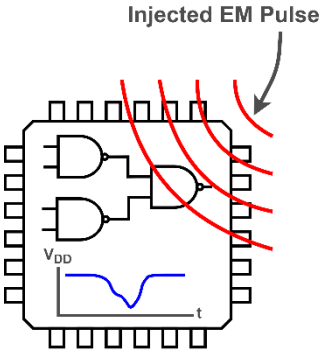
Fault Injection Vulnerability Assessment and Countermeasure

In today's world of complex electronic systems, the security of integrated circuits has become a major concern. Hardware attack methods are becoming less expensive and more easily accessible. Failure to address hardware security vulnerabilities leaves a chip open to threats such as data corruption, denial of service, and the leakage of assets and design secrets. These assets may include cryptographic keys, sensitive user information, passwords, biometrics, configuration bits, and firmware.

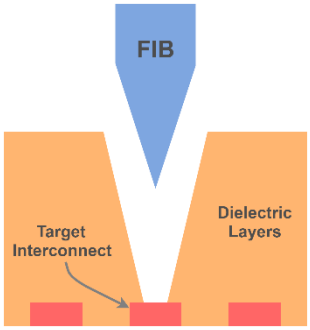
Fault injection is an attack method that is gaining concern as a simple yet powerful form of attack. It involves intentionally injecting faults into a device to cause unexpected behavior, bypassing chip security measures. In other words, successful fault injection attacks usually lead to the corruption of controller or datapath values in the chip. This corrupted data can be propagated throughout the device, and depending on the location and timing of the injected faults, can help extract sensitive information stored inside the chip. Faults can occur in the form of bit flips in registers or memory, transient interconnect voltages, clock disturbances, supply voltage disturbances, or permanent interconnect changes.



Laser Fault Injection (LFI)



Electromagnetic Fault Injection (EMFI)



Focused Ion Beam (FIB)

Fault injection can be carried out through several techniques that are invasive, semi-invasive, or non-invasive. As an example, **laser fault injection (LFI)** uses directed beams of light to alter the functionality of a device during runtime. This injects voltage pulses into the circuit that can flip bits in registers or SRAM. **Electromagnetic fault injection (EMFI)** uses generated magnetic fields to create voltage pulses in metal interconnects. **Focused ion beam (FIB)** milling uses semiconductor editing machinery to alter the structure of a circuit to either cut or add interconnects. Security measures can then be bypassed and points of interest in the circuit can be probed to extract information.

Clock Glitching *Voltage Glitching*

Fault injection attacks can also be used to cause timing violations in a design. **Clock glitching** is an injection technique where the system clock is disturbed, causing setup and hold time violations. A similar technique, **voltage glitching**, temporarily disturbs the chip's voltage supply to increase or decrease propagation delays. Both of these methods ultimately lead to the latching and propagation of incorrect data in the chip. With an understanding of the design functionality, these attacks can be used to force hardware to reveal sensitive information.

Caspia Technologies' solution, **AFIx**, performs fault injection attack assessment at the pre-silicon stage, allowing designers to implement strategic countermeasures to ensure chip security. AFIx can analyze and assess a design to determine specific locations most vulnerable to the fault injection techniques previously discussed. It provides an analysis of the effectiveness of various applicable countermeasures, aiding a designer in choosing the most suitable methods to secure a design. This pointed analysis, done early in the design phase, allows designers to save area overhead and cost by implementing countermeasures only where necessary and with the highest chance of preventing an attack.

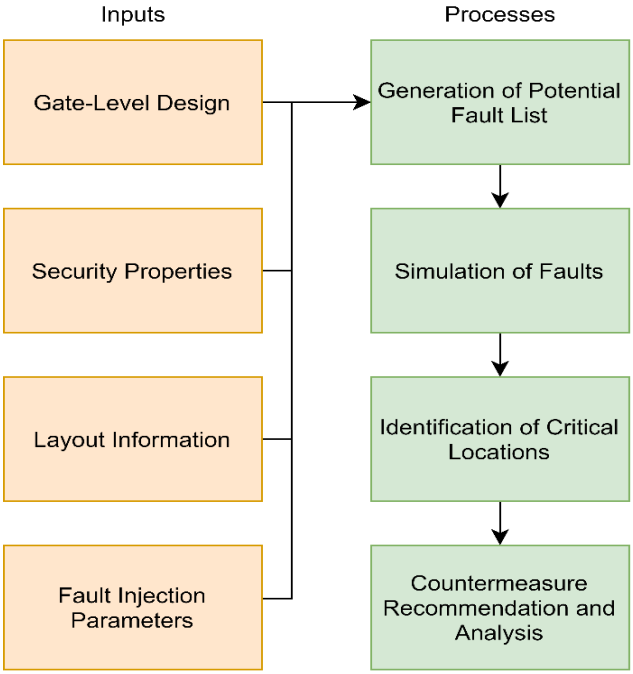


Diagram of the AFIx Workflow and Features

Contributors:

Ramsey Hamed, Hardware Engineer, Caspia Technologies

Beau Bakken, Principal Engineer, Caspia Technologies