SECURE-iC
THE SECURITY SCIENCE COMPANY

PRODUCT SHEET

Securyzr™ > Securyzr™ Security IP > Securyzr™ Digital Sensor > SCZ_IP_DS_200

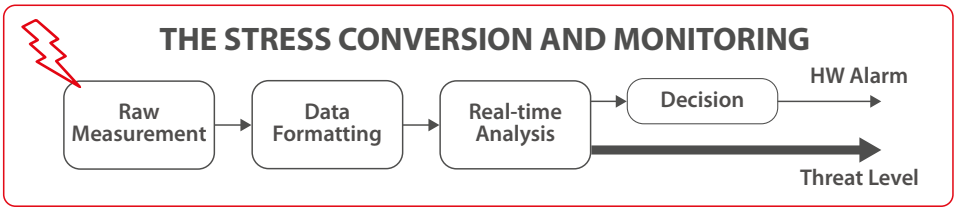
DIGITAL SENSOR

In cryptography, an attack can be performed by injecting one or several faults into a device thus disrupting the functional behavior of the device. Techniques commonly used to inject faults consist in introducing variations in the source voltage, clock frequency, temperature, or irradiating with a laser beam etc.

Unlike analog sensors which are dedicated to the detection of a specific perturbation attack, the Digital Sensor is designed to detect various threats belonging to the family of Fault Injection Attacks (FIA):

- Input clock frequency (clock glitches, overclocking)
- Input voltage (power glitches, underfeeding)
- Temperature (heating)
- Radiations (laser spot, light spot, electromagnetic)

Digital Sensor converts all monitored stresses into a timing stress which is then measured. When a threat is detected, it provides the system with a measurement of the threat's level and it raises the hardware alarm.



Features

- Detects global and local fault injections such as laser, EMFI, clock or temperature
- Difficult to identify by an attacker (melted within the rest of design)
- Real-time hardware alarm
- Embeds health-test to validate the integrity of the IP during the boot and on-demand
- Proven technology with stochastic model for reliability and security estimation
- Tested in the Security Science Factory Lab, using global stress (e.g., clock glitch) and local stress (e.g., electromagnetic injection)
- Security certification ready (incl. Common Criteria)
- Fully digital and designed with the standard cells library
- Transferable to any design kit
- Lightweight
- Customizable sensitivity
- Compatible with clock gating feature
- Several sensors can be regrouped around a unique bus interface
- No calibration after design
- Support DVFS
- Easy to integrate into the system
- AMBA (APB, AHB, AXI) interface

Applications

- IoT
- Set-top Box
- Mobile
- Automotive
- Defense
- Etc.

Deliverables

- Technical specifications,
- Self-checking RTL Testbench based on reference scenario for simulation
- Front-end RTL and constraints files .sdc
- Remote support for integration
- Integration guidance for back-end

V1.2

CONTACT US

EMEA
sales-EMEA@secure-ic.com

AMERICAS
sales-US@secure-ic.com

APAC
sales-APAC@secure-ic.com

JAPAN
sales-JAPAN@secure-ic.com

CHINA
sales-CHINA@secure-ic.com

SECURE-IC
THE SECURITY SCIENCE COMPANY

HEADQUARTERS
Digital Park B - ZAC Atalante Via Silva
801 avenue des Champs Blancs
35510 Cesson-Sévigné - France
+33 (0)2 99 12 18 72 - contact@secure-ic.com