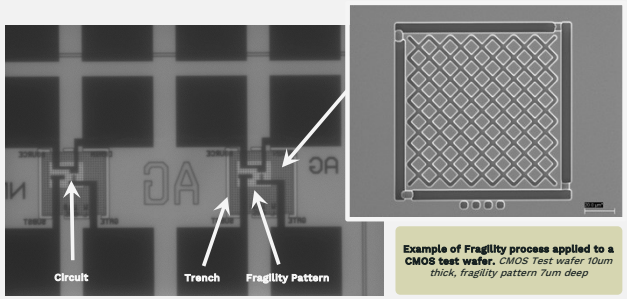
Physical anti-tamper protection and passive sensor technologies

Geremy Freifeld (Draper PI), Murali Chaparala (Draper PI)

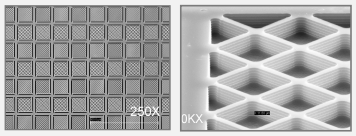
Driving Applications: Supply Chain Hardware Integrity for Electronics Defense (SHIELD)

SHIELD enhanced fragility

Draper is developing **critical hardware assurance features** to combat the threat of counterfeit integrated circuit components entering the global electronics supply chain. To assure against common threat modes such as recycled/repackaged components, test rejects, low-quality clones, and falsely marked parts, our approach, is to **develop technology solutions that simultaneously achieve electrical robustness and physical fragility**. The component with engineered fragility will self-destruct upon attempts to physically open, remove, or transfer it using standard reverse-engineering de-processing techniques. The **manufacturing technology being developed is economically scalable low-cost solution** for broad applicability.



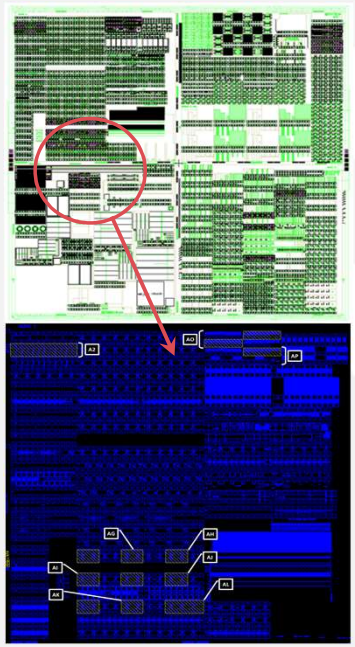
Example of Fragility process applied to a CMOS test wafer. *CMOS Test wafer 10um thick, fragility pattern 7um deep*



Different versions of fragility designs. *Many iterations were manufactured and tested to correlate to the finite element analysis models. Some designs actually increased die strength!*

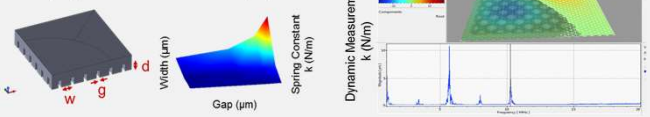
Draper Fragility Enhancement Technology

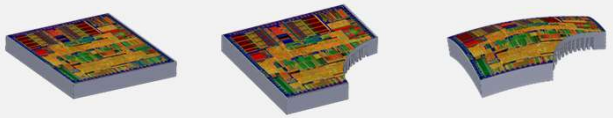
The Draper fragility enhancement technology etches the backside of active CMOS regions of the SHIELD dielets. Fragility enhancement features are engineered to react to physical tampering and ensure either dielet physical fracture, or sufficient mechanical stress changes to alter the electrical functionality; In either case rendering the dielet useless. Using finite element analysis the fragility pattern is designed to reduce the normal uncontrolled variations in chip strength and instead allows highly engineered control/programmability of electromechanical properties that simultaneously achieves electrical robustness and physical fragility. Fragility enhancement designs must retain sufficient mechanical strength to survive the conditions of insertion into the host package, assembly, and normal use. Thus, the design is tailored to fail when it should fail, and survive when it should survive. The patterns etched into the SHIELD dielets result in a 3 micron thickness in some portions of the active CMOS substrate!

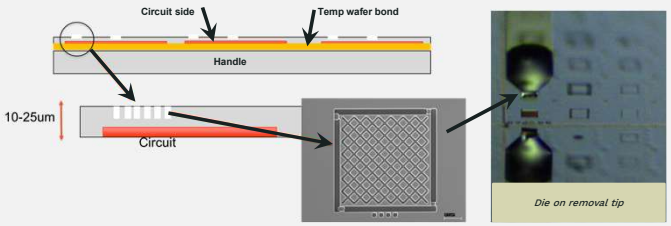


Model of Fragility Design Space

(using results of finite element analysis)







Die on removal tip

Application of Fragility Enhancement Technology

This technology can be used to protect against reverse engineering of embedded IP.

1. Design fragility structures under the critical circuitry.
2. Fabricate the fragility structures after the circuit is fabricated at standard CMOS foundry.

The fragility structures can be designed to shatter the critical circuitry up on being subjected to physical FA processes or to alter the circuit performance.

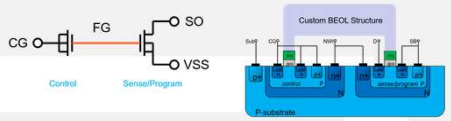
SHIELD Sensor | Objective and Concept

Main Objective: Passively detect and record environmental shifts in temperature & radiation for use in an advanced supply chain hardware authentication technology.

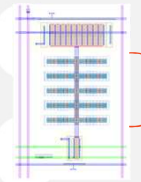
The sensor is based on a I/O 2T lateral single-poly floating-gate cell, schematically shown in Figure 1 with a cross-sectional diagram shown in Figure 2. Quantum tunneling is used to initially program charge onto the floating-gate. As the sensor is exposed to energy, such as temperature elevation and radiation exposure, it will undergo mobile charge compensation, which will deplete the amount of charge stored proportional to the exposure.

Charge loss sensitivity is tailored using custom back-end-of-line (BEOL) structures in device layout. A predictable correlation between charge loss and energy exposure is determined by the proportionality of the floating-gate surface area exposed to the interlayer isolation dielectric in the ASIC process.

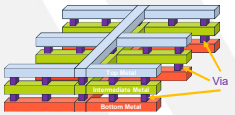
The device hits an asymptotic limit to charge loss below a specific energy threshold, which prevents the sensor from discharging in typical ambient environments.



Layout (Top-Down)



BEOL Cross Section

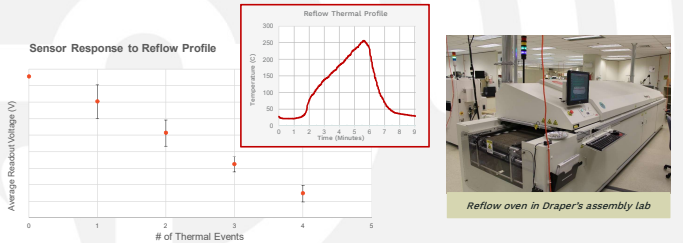


Sensor Concept of Operation

1. Sensor system is manufactured.
2. Initial program & calibration is performed at a trusted site and access to reprogramming is removed.
3. Device is packaged and pre-screened.
4. Device is sent to distributors for eventual assembly and deployment.

Thermal Test Approach & Results

The figure at right shows the corresponding voltage, as a function of charge on the floating gate, that remains after a varying number of reflow profile exposures (referred to as thermal events). Each thermal event corresponds to approximately 90 seconds over 200º C.



Reflow oven in Draper's assembly lab

Radiation Test Approach & Results

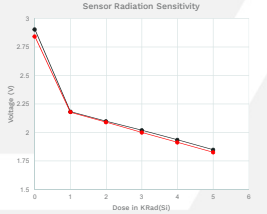
X-ray source parameters

- Energy = 50KV
- Filament current = 80uA
- Distance = 3cm
- No collimator
- Time/distance exposure corresponds to a dose of ~1KRad(Si)

A 700Rad(Si) exposure would cause a similar voltage shift as a high-temp thermal event. Depending on the material, the package & lid will provide varying levels of shielding. I.e. 10mils of Kovar would provide 100% shielding for this testing.

Typical imaging exposure levels using micro computed tomography (μCT) are in the 20Krad range. Appreciable operational degradation would also require exposure levels in excess of 10KRad. Any attempt at either reverse-engineering or accelerated premature failure of host die using x-ray exposure, would certainly be detected by sensor.

Mini-x-ray test fixture in Draper's Radiation Effects Lab



Application of Floating Gate Sensor Technology

This technology can be used to detect warranty nulling exposure of electronics to high temperature or to radiation. The floating gate technology can be adapted to detect exposure to various chemistries, light, etc.

DRAPER®

This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA). The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

THE ELECTRONICS RESURGENCE INITIATIVE