Supply Chain Integrity for Electronics Defense
Bryce Winters, Scott Suko, Sam Wanis, Northrop Grumman
Team: Sandia National Labs, Georgia Tech Packaging Center, RFID Global Solution

NORTHROP GRUMMAN

SHIELD
Security and Access

Background

SHIELD Dielet Provides Hardware Root of Trust and Full Authentication Functionality in a Microscopic Integrated Circuit with RF Link

Electronics Counterfeiting a Threat to Military Electronics Integrity

"Over a two year period, from 2009 to 2010, approximately 1,800 cases of suspect counterfeit parts were uncovered"

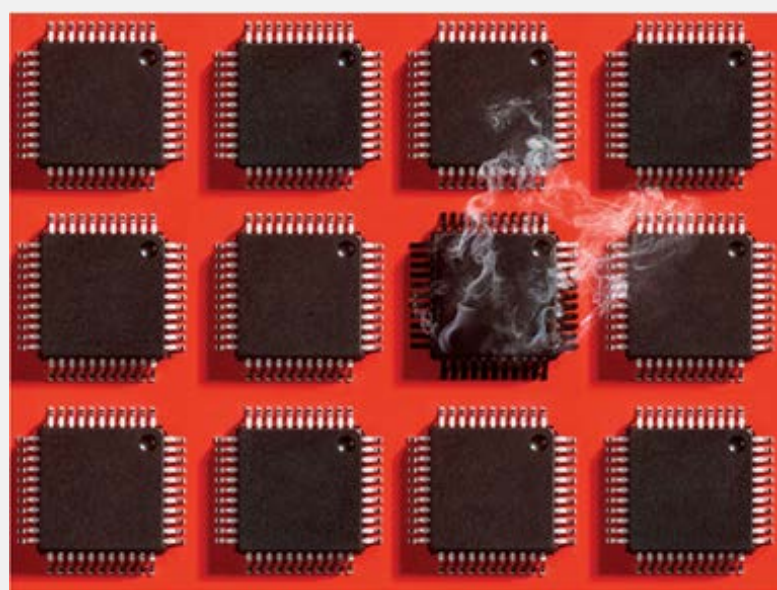*Inquiry Into Counterfeit Electronic Parts in the Department of Defense Supply Chain, May 2012*

Image Source: IEEE Spectrum

SHIELD Defeats Counterfeiting by Building a Complete Electronics Authentication System

Domain expertise assembled for SHIELD team

Global Asset Tracking Management Network

Northrop Grumman Corporation, RFID Global Solution, Georgia Tech, Sandia National Labs, Kilopass, Corwill Technology
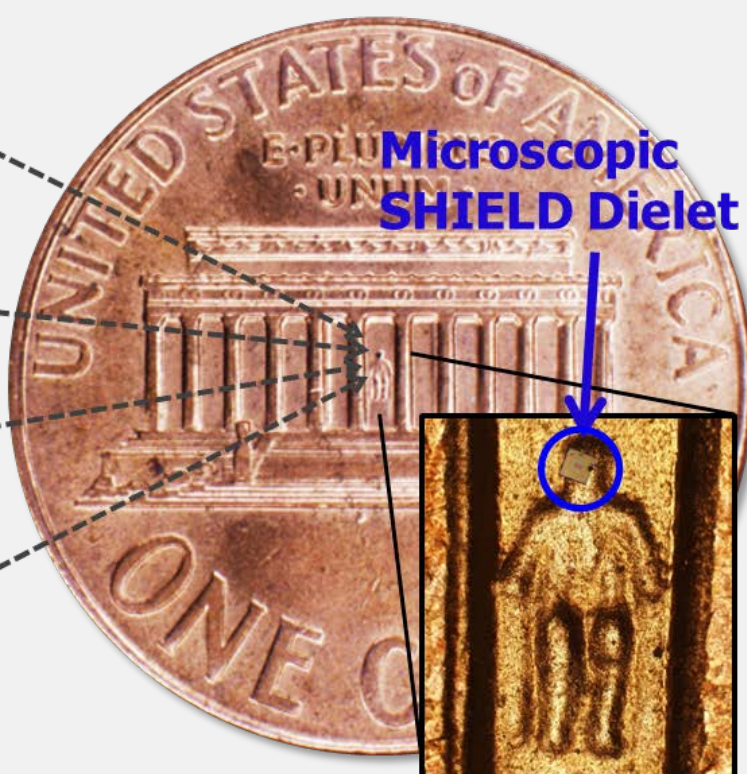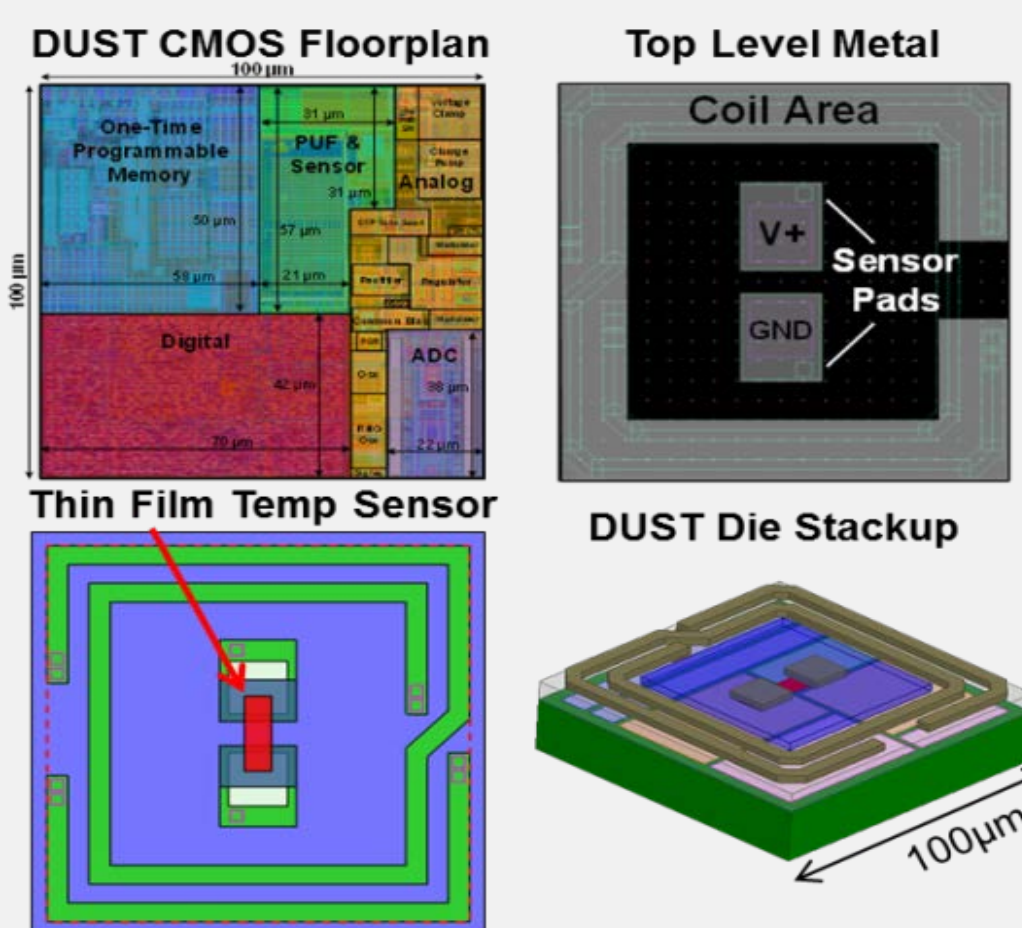

Image Source: CDW

- Dielet Inserted in Host Chip & Probed for Authentication
- Full Encryption Engine
- Unpowered Passive Sensors
- Inductive Powering and Communication

Microscopic SHIELD Dielet

Microscopic Dielet Inserted into Every Electronics Package

Each Dielet Supports a High Level of Functionality; Developed in 14nm CMOS

DUST CMOS Floorplan
- One-Time Programmable Memory
- PUF & Sensor
- V+
- Digcal
- ADC

Top Level Metal
- Coil Area
- V+
- GND
- Sensor Pads

Thin Film Temp Sensor

DUST Die Stackup

100μm

Wafer Scale Probing of Dielets uses Test Controller, Maximizing Dielet Density on Wafer, Minimizing Test Time and Cost

DIG Test CTL

OTP PRGM & CTRL
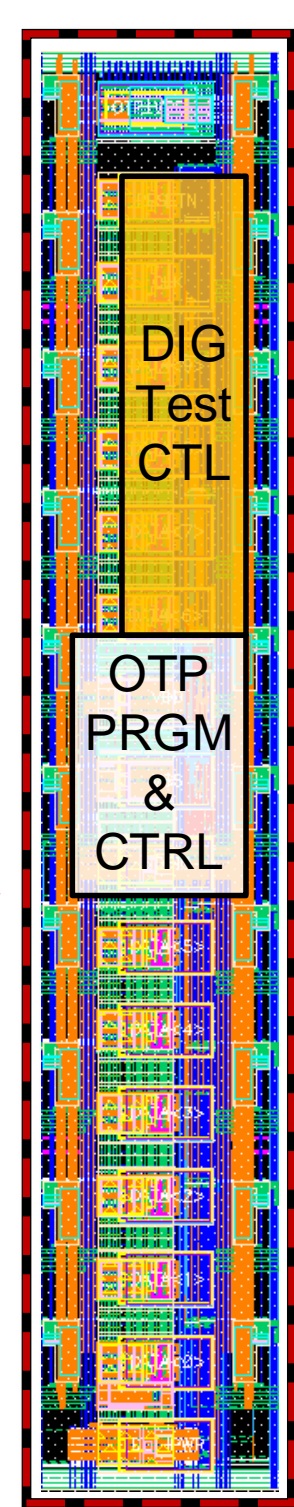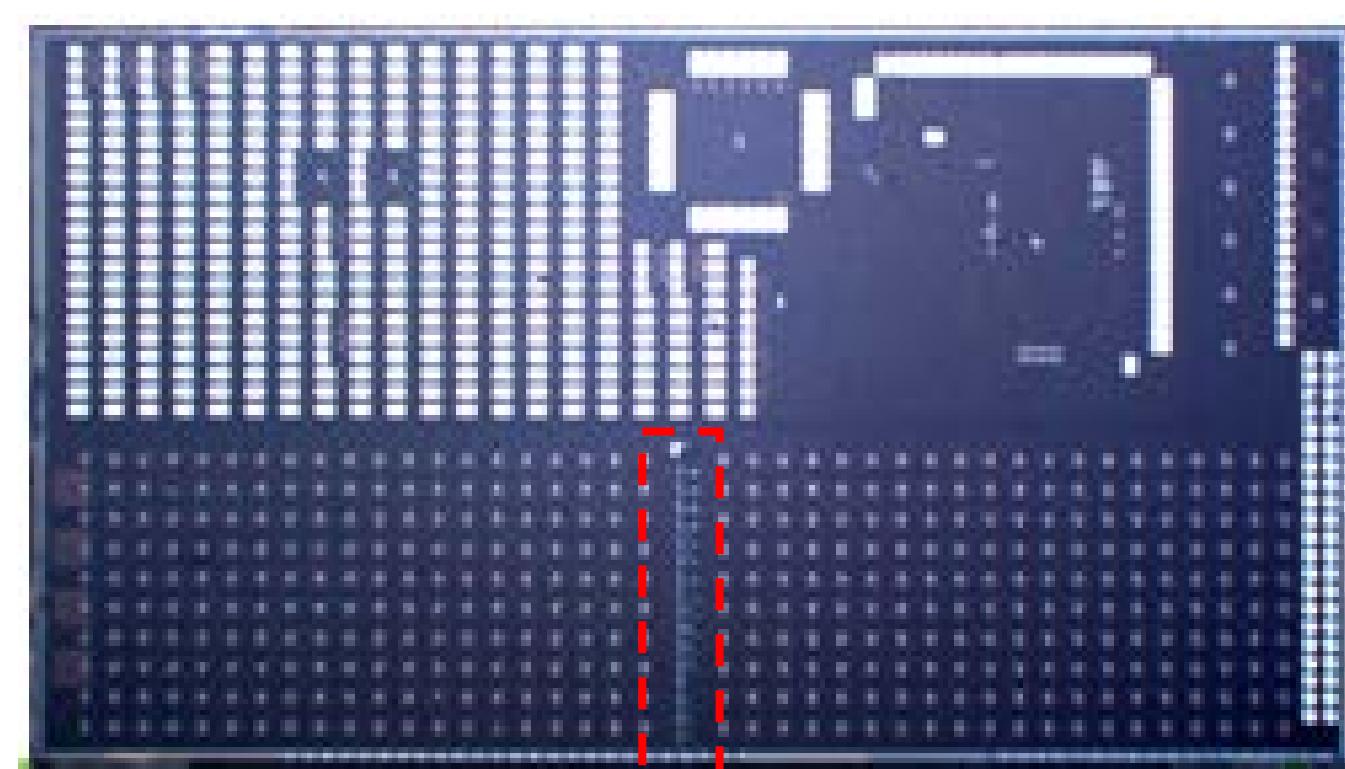
Dielet Array
- Local decoding allows single dielet Power On/Communication
- Simultaneous ATPG scan of entire row (20 dielets) also possible

Test Controller
- Programs and reads back 400 OTP S/Ns with single touch-down
- Reads raw PUF bits to form a bit mask
- Integrates with Probe functionality to allow full authentication
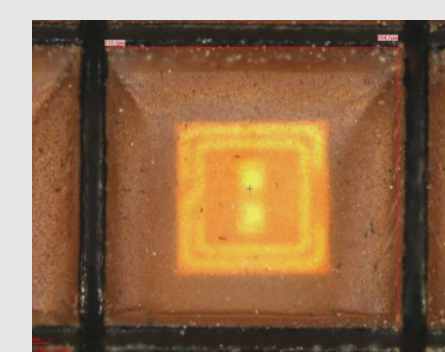- Provides visibility into each dielet's digital core

Approach

Dielet Stretching and Encapsulation Protects Dielets and Allows Handling with Standard Tooling
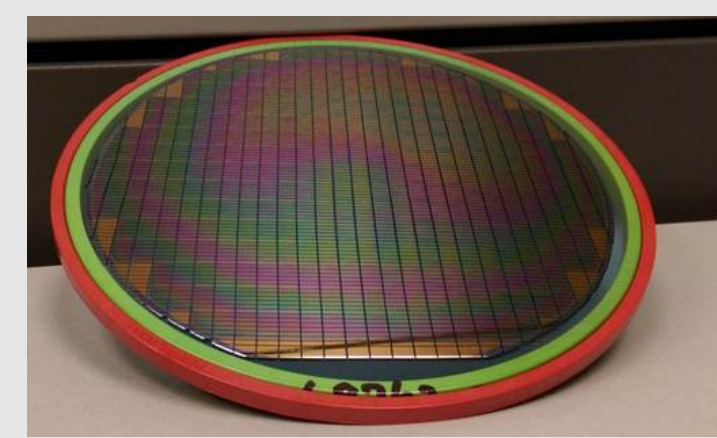
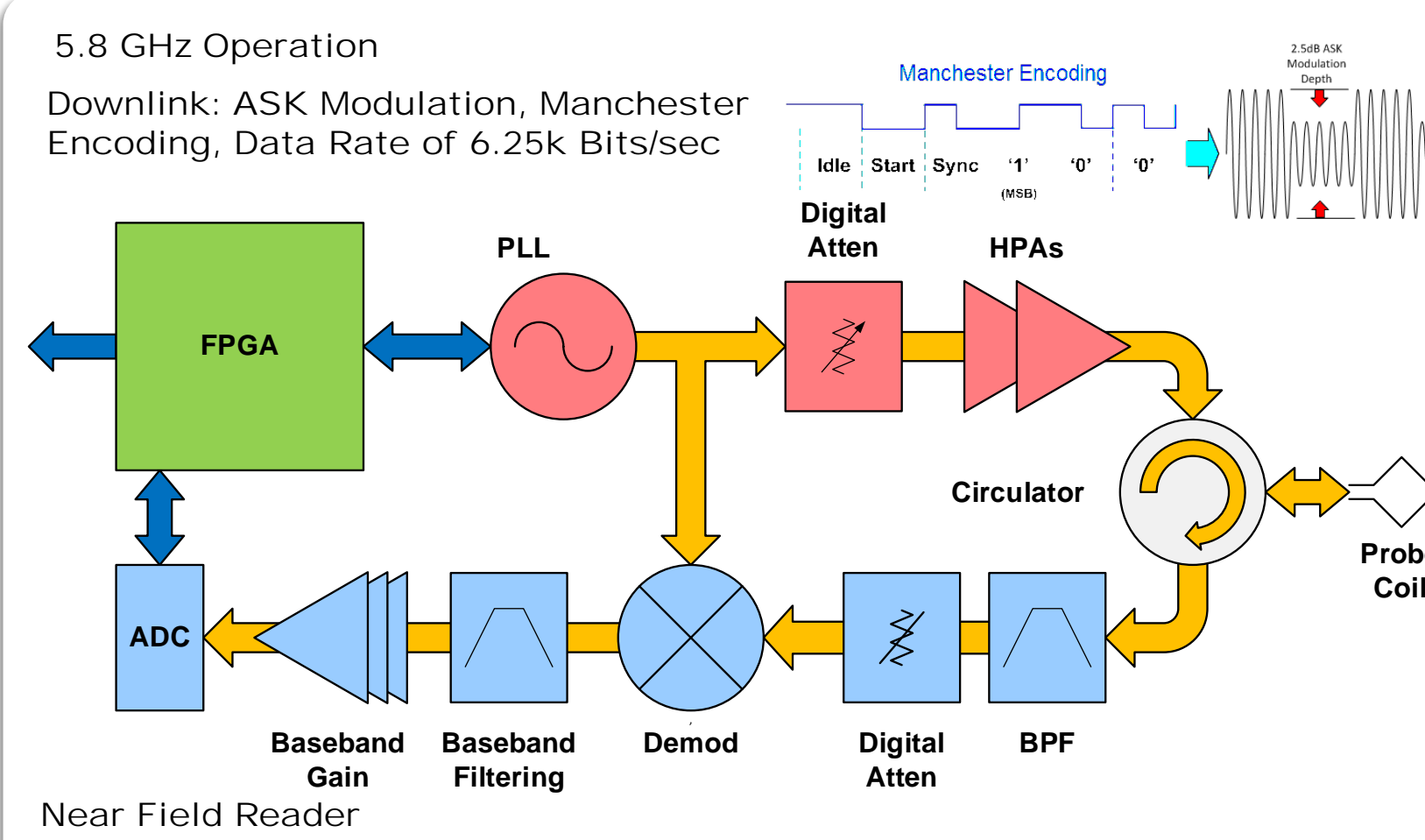Surrogate wafer fabricated in house
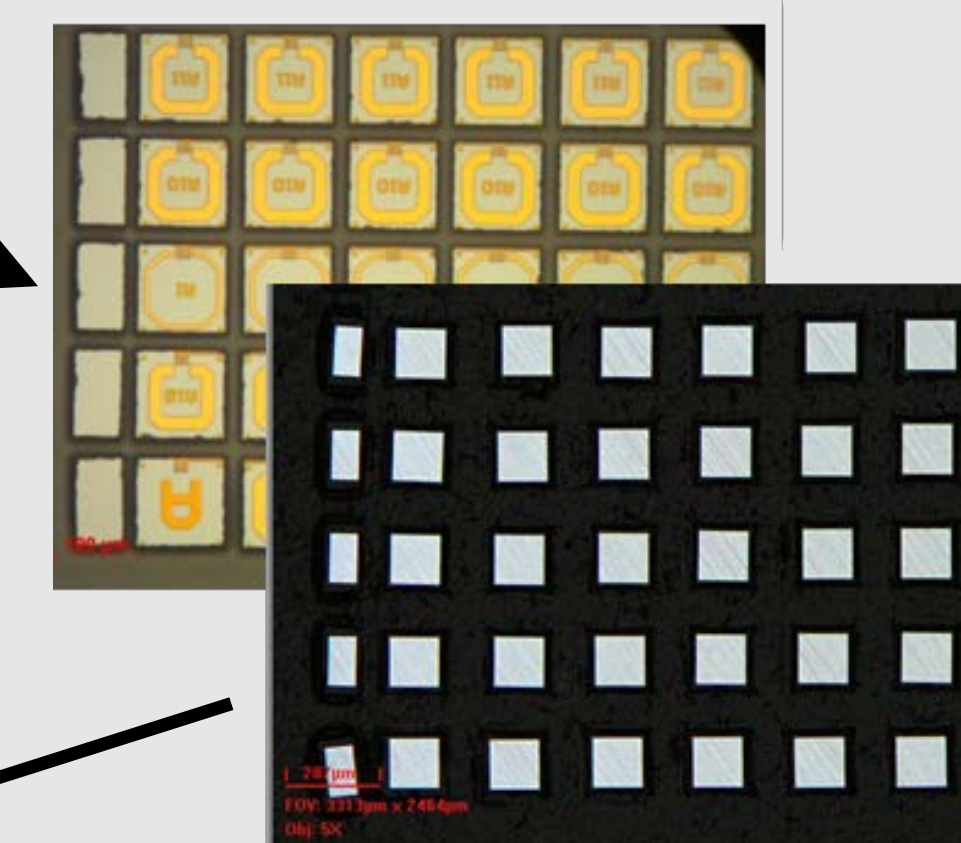
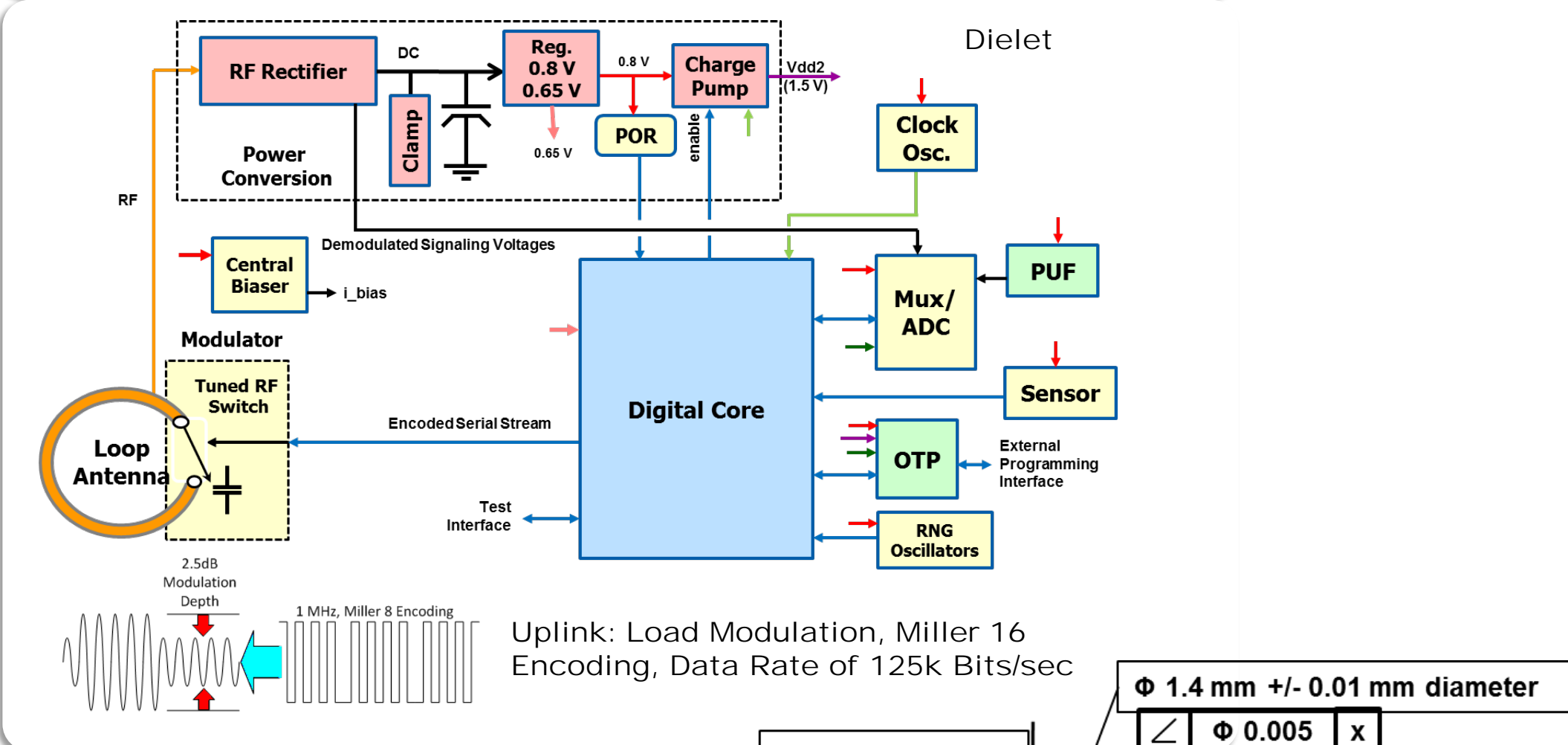Die are singulated and spread on dice tape to increase effective die footprint

Fully encapsulated die provide enhanced mechanical robustness

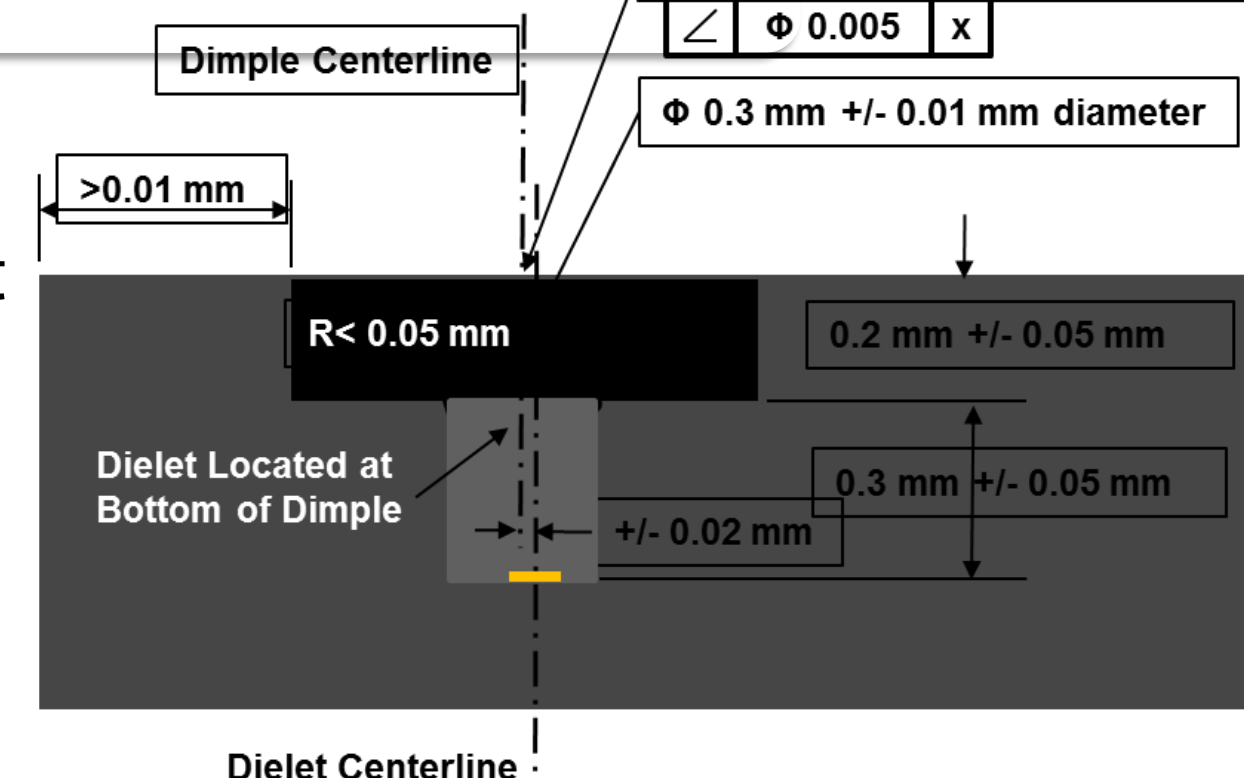Image Source: Georgia Tech Packaging Resource Center

Near Field Reader Architecture Uses Single Coil, Single Frequency System for Simultaneous Power Transfer and Bidirectional Communications

5.8 GHz Operation

Downlink: ASK Modulation, Manchester Encoding, Data Rate of 6.25k Bits/sec

Manchester Encoding

FPGA — PLL — Digital Atten — HPAs

Circulator — Probe Coil

ADC — Baseband Gain — Baseband Filtering — Demod — Digital Atten — BPF

Near Field Reader

Dielet

RF Rectifier — Reg. 0.8V 0.65V — Charge Pump — Clock Osc.

Power Conversion — Clamp — POR

Central Biaser — Mux/ADC — PUF

Modulator — Tuned RF Switch — Digital Core — Sensor — OTP — RNG Oscillators

Loop Antenna

Uplink: Load Modulation, Miller 16 Encoding, Data Rate of 125k Bits/sec

Mechanical Insertion of Dielet Into Microelectronics Package

Φ 1.4 mm +/- 0.01 mm diameter
Φ 0.005 x
Φ 0.3 mm +/- 0.01 mm diameter

Dimple Centerline
>0.01 mm
R< 0.05 mm
0.2 mm +/- 0.05 mm
Dielet Located at Bottom of Dimple
0.3 mm +/- 0.05 mm
+/- 0.02 mm

Dielet Centerline

Results and Impact

Temperature Sensor Detects Whether Part Has Experienced Reflow Temperatures

GST-C Sensor
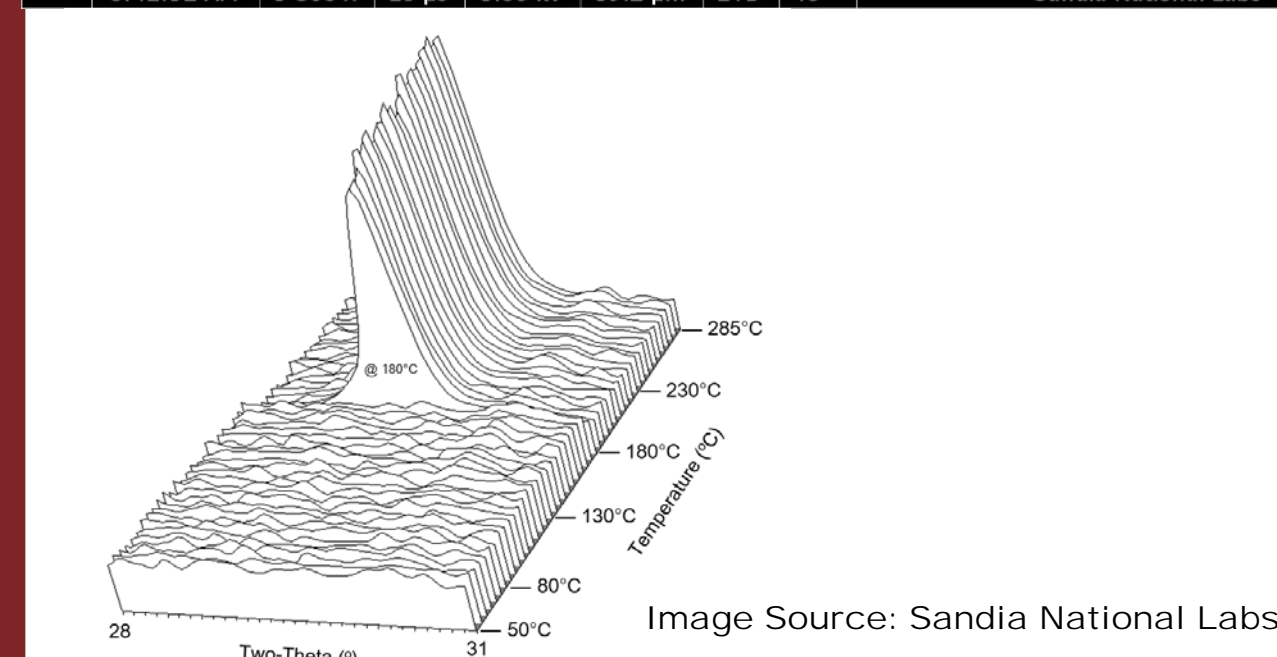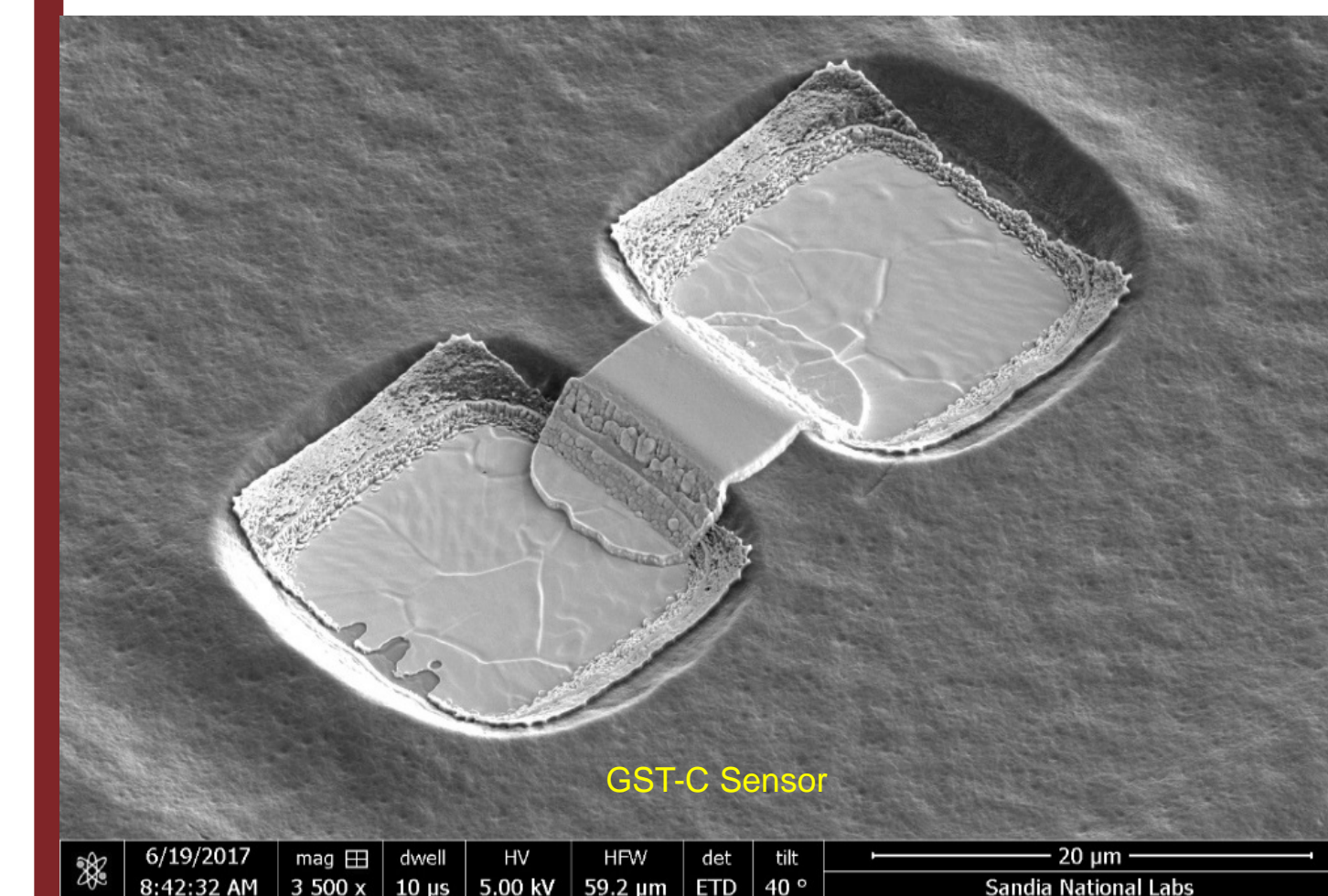
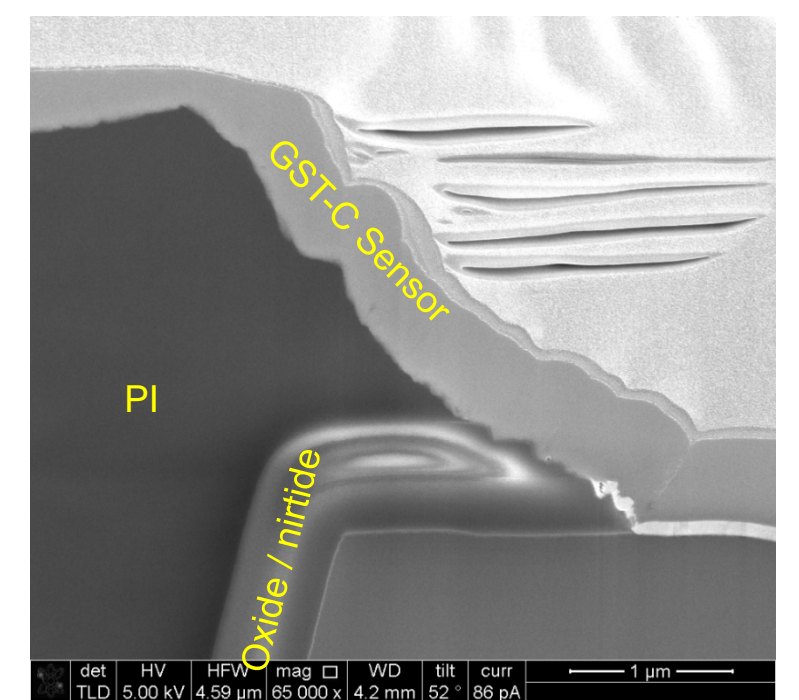Image Source: Sandia National Labs

Calibrated temperature sensor readout vs the dielet temperature profile
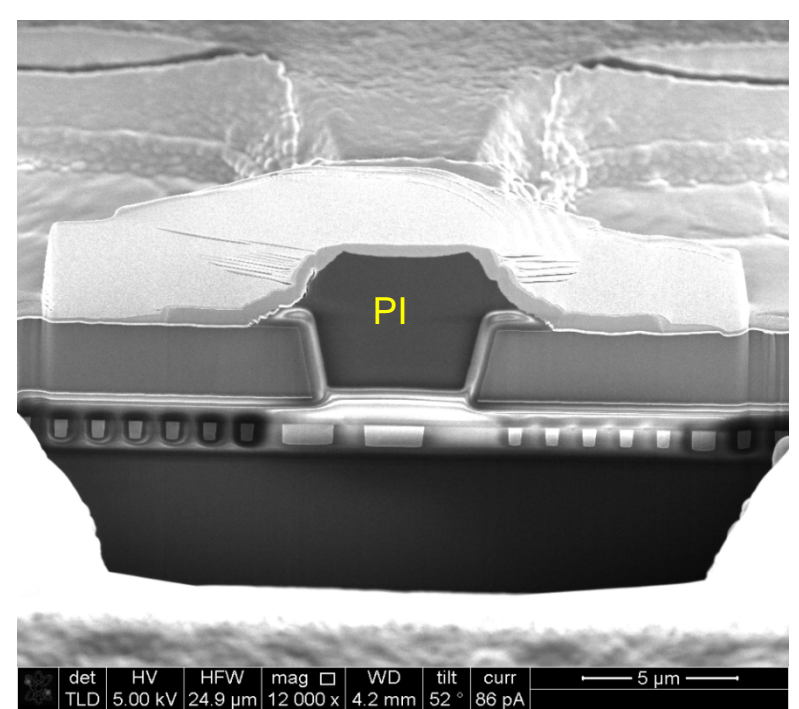Ratio of the calibration frequency to the sensor frequency across PVT corners
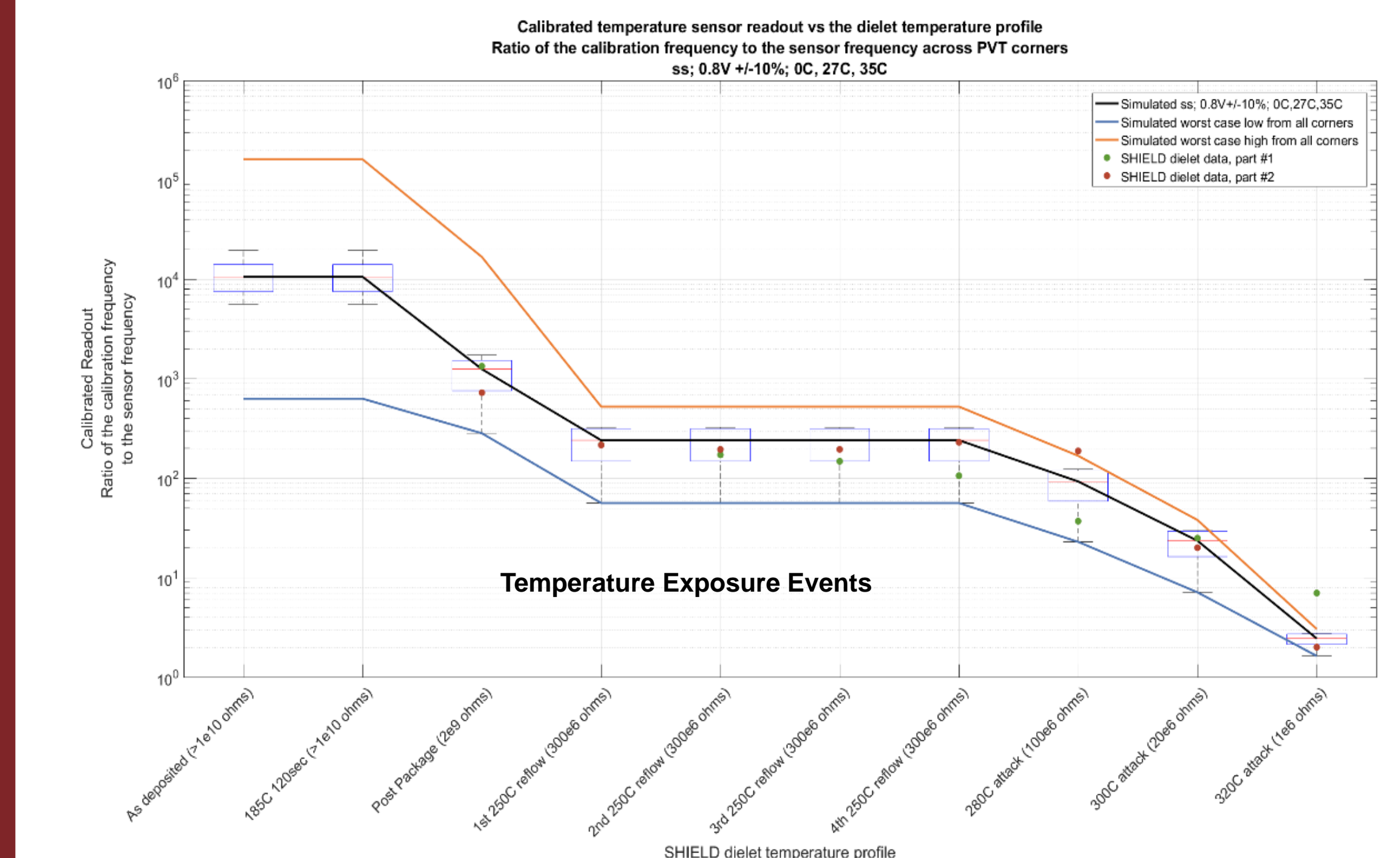
Under the T&AM proposed program, managed by Army AvMC Protective Technologies, the SHIELD Range Extension and Enhanced Temperature Sensor will result in:

- A microscopic dielet with a Near Field RF link with a > 3mm range implemented in Global Foundries 12 nm CMOS
- Challenge Response Protocol for Authentication and Dual key AES Encryption using Physically Unclonable Function and One-Time Programmable keys
- Enhanced Temperature History Sensor for Wider Range of Tamper Detection
- Reader using passive (reflectivity modulation) RFID technique

SHIELD Dielet

Host Device

Reader
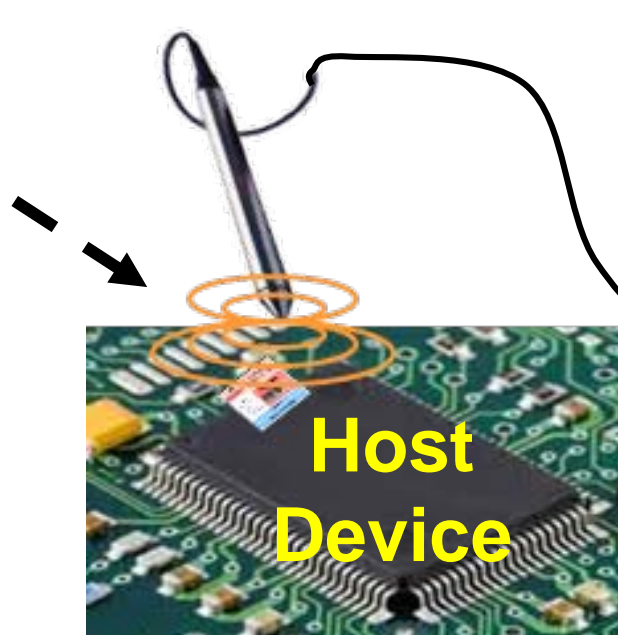
Authentication Database

Impact: Provides an automated, dependable counterfeit avoidance method