Tech Insights

Hardware Anti-Tampering and Data Integrity Protection

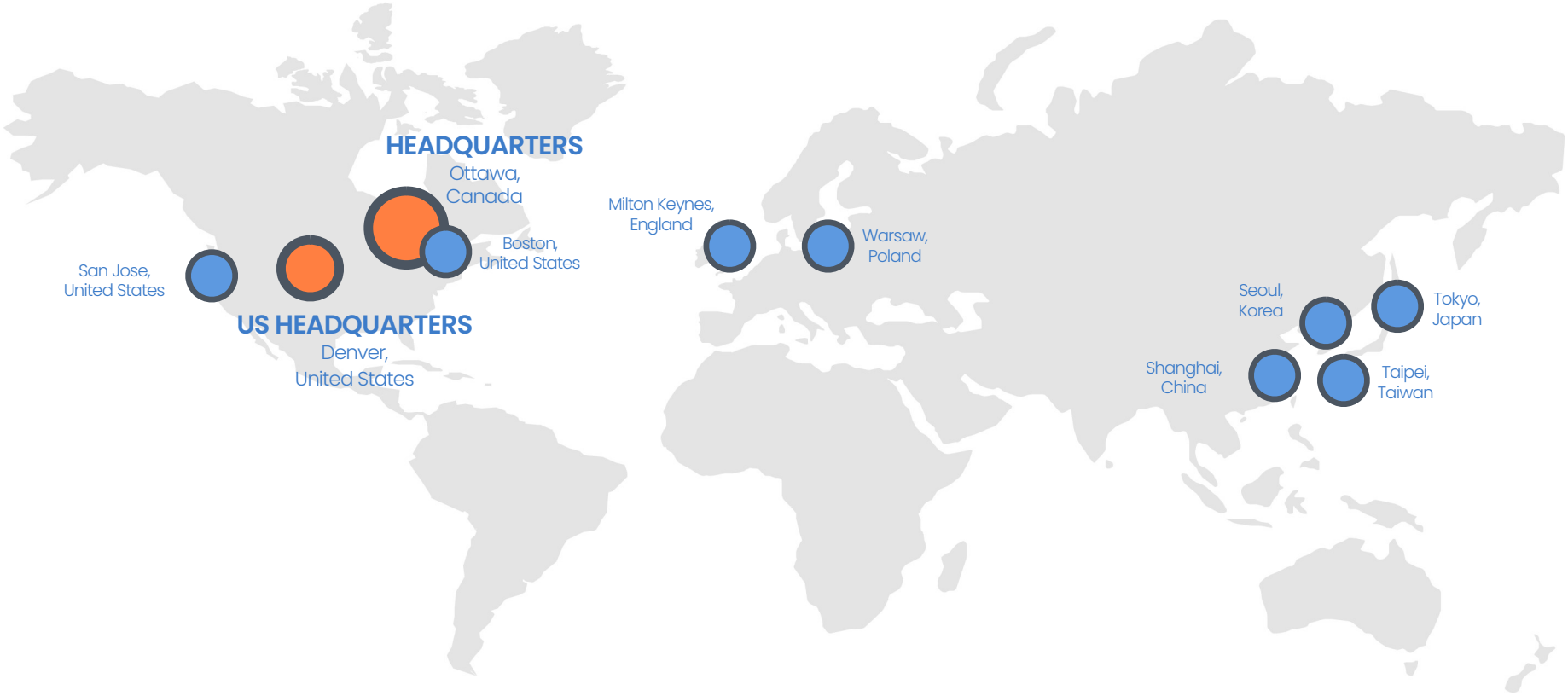
March 2025

Carlos Lopez
clopez@techinsights.com

MPI-SP / RUB

www.techinsights.com

Global Presence



Who is TechInsights?

- TechInsights is the authoritative information platform for the semiconductor industry

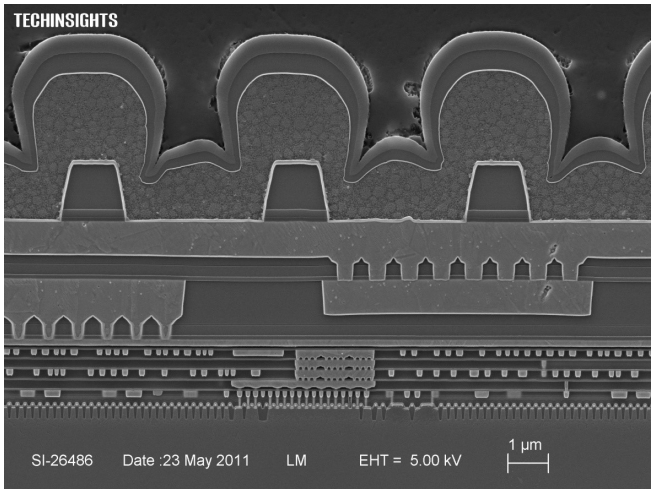
- 30+ years of experience
- Headquartered in Ottawa, Canada with over 400 employees and offices around the world

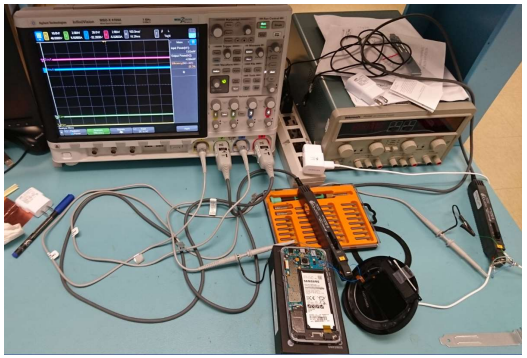
- 1.5m+ reports
- 100k+ chips torn down
- 95k+ platform users
- 650+ companies served

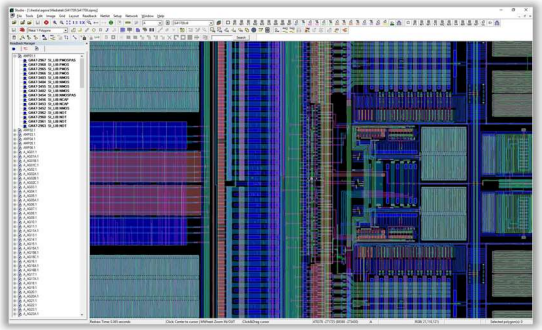
We maintain the world's largest database of semiconductor and technology analysis.

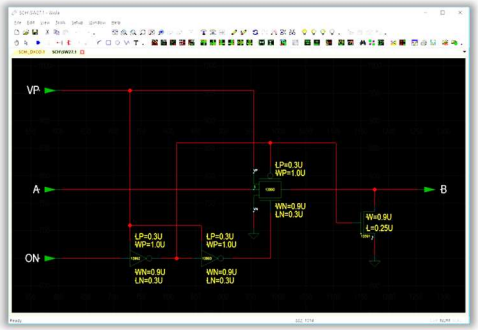
Techniques

- Market Analysis
- IP Analysis
- Physical Analysis
- Functional Analysis
- Reverse Engineering









Who do you trust?

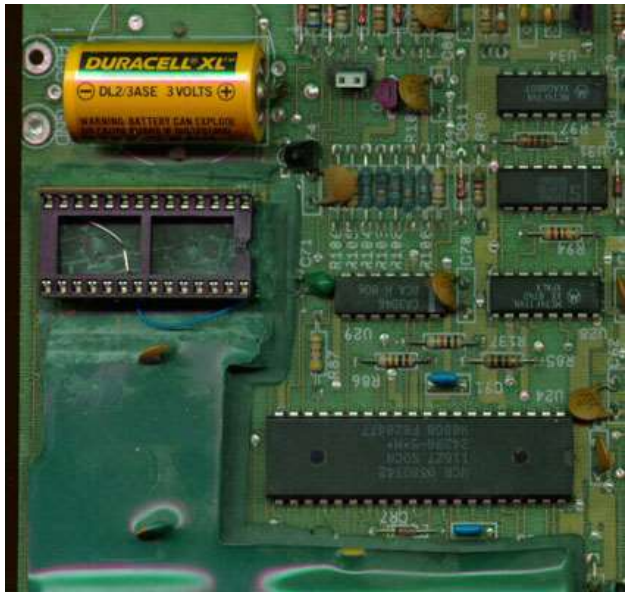
- Who do you trust?
- Satellite not trusting subscribers or owners of hardware.
- Casino does not trust players and/or staff. Regulators do not trust casino operators.
- Bank preventing fraud.

VideoCipherII – Early Anti-Tamper Example

- Cable and Satellite TV systems where among the first consumer devices requiring anti-tamper security.

Source:
https://commons.wikimedia.org/wiki/File:General_Instruments_VideoCipher_II_2100E_satellite_descrambler.png

VideoCipherII – Mechanical Protection



- Security was provided by epoxy resin covering the ROM, RAM and CPU. The “Hack” was to expose the rom, replace with socket and manipulate keys from SRAM.

Casino Gaming Security

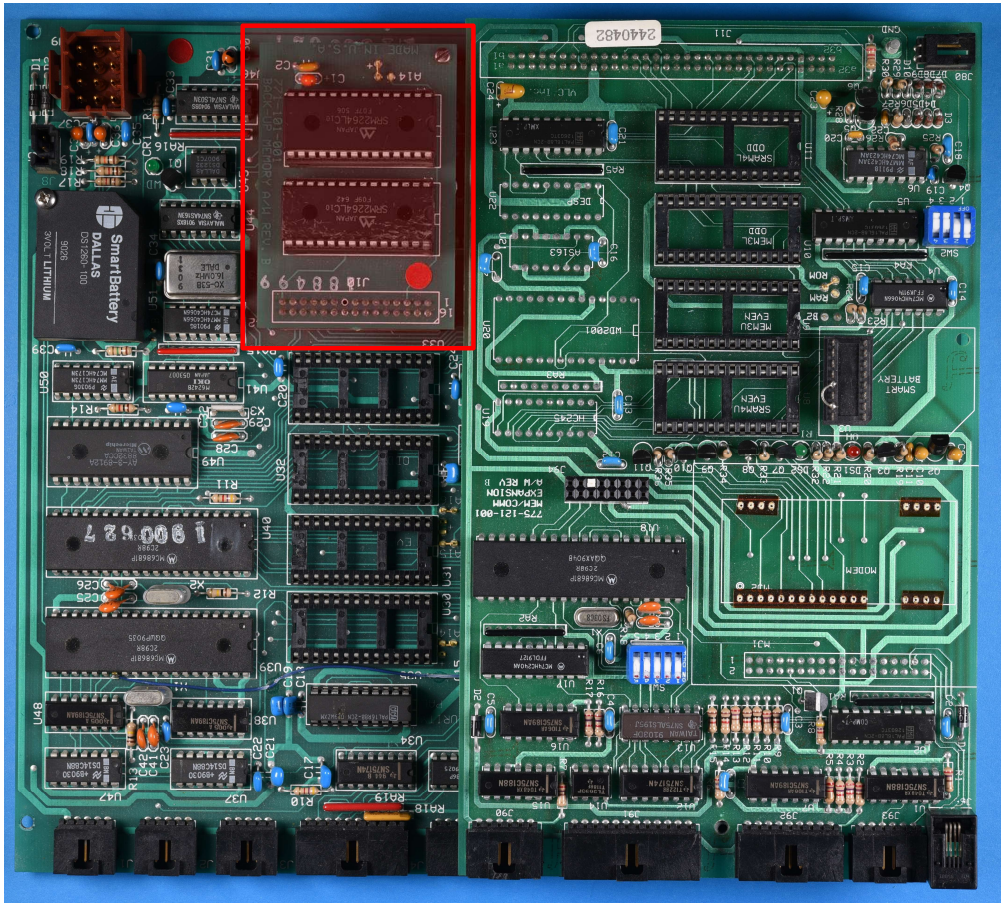
- Casino machines have features that protect the integrity of the accounting data called meters.
- Some scrambling is used along with canary values in SRAM.
- Programmable Logic Devices (PLDS) used to encode

Source: https://commons.wikimedia.org/wiki/File:Video_Poker_Machines.jpg

Video Poker Platform

- The early platform from the 1990s contained mostly off the shelf parts such as the Motorola 68000 with 27512 EEPROM devices.

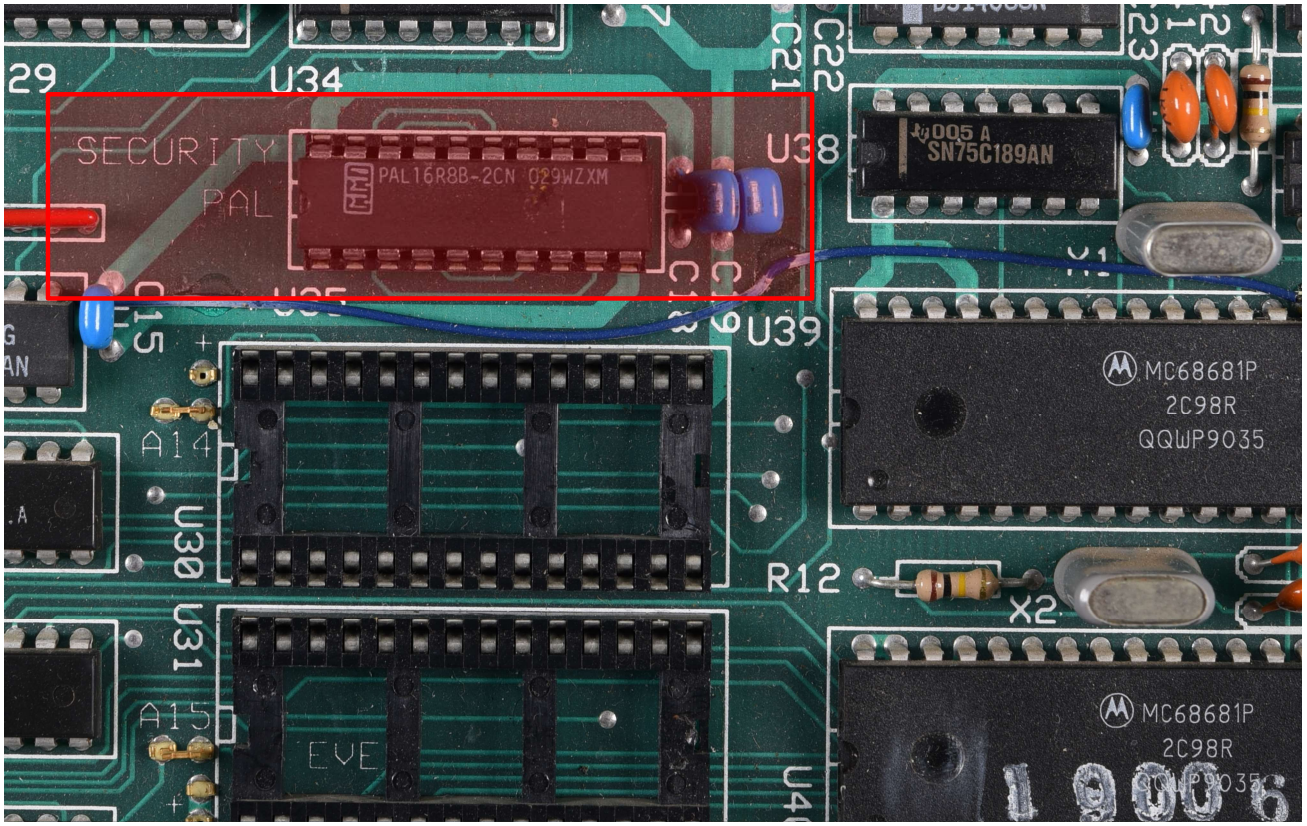
- Critical Accounting Data was held in daughterboard using battery backup.



Security PAL

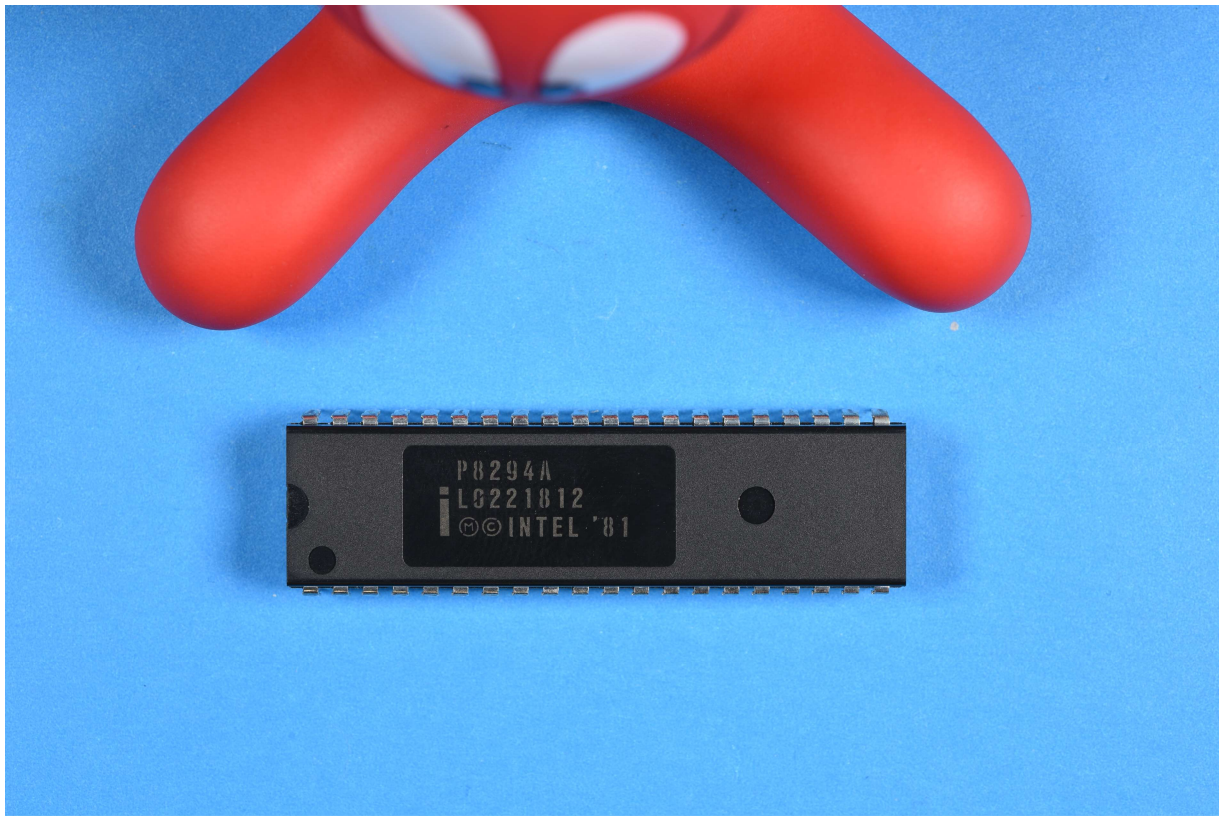
- The “Security PAL” on this machine generates the unique terminal ID and SRAM personalization data.

- Using the software access produced a type of cipher feedback transform.
- Programmable Array Logic



8294 Data Encryption Unit

- "Strong" cryptographic transformations were slow in software
- The 8294 Data Encryption processor was one of the earlier off the shelf encryption accelerators for DES cipher processing.



8294 Data Encryption Unit

- Bandwidth is a bit too low for real time in place memory enciphering.

- Good enough for your 300 baud modem.

intel

8294
DATA ENCRYPTION UNIT

- **Certified by National Bureau of Standards**
- **80 Byte/Sec Data Conversion Rate**
- **64-Bit Data Encryption Using 56-Bit Key**
- **DMA Interface**
- **3 Interrupt Outputs to Aid in Loading and Unloading Data**
- **7-Bit User Output Port**
- **Single 5V ± 10% Power Supply**
- **Peripheral to MCS-86™, MCS-85™, MCS-80™ and MCS-48™ Processors**
- **Implements Federal Information Processing Data Encryption Standard**
- **Encrypt and Decrypt Modes Available**

The Intel® 8294 Data Encryption Unit (DEU) is a microprocessor peripheral device designed to encrypt and decrypt 64-bit blocks of data using the algorithm specified in the Federal Information Processing Data Encryption Standard. The DEU operates on 64-bit text words using a 56-bit user-specified key to produce 64-bit cipher words. The operation is reversible: if the cipher word is operated upon, the original text word is produced. The algorithm itself is permanently contained in the 8294; however, the 56-bit key is user-defined and may be changed at any time.

The 56-bit key and 64-bit message data are transferred to and from the 8294 in 8-bit bytes by way of the system data bus. A DMA interface and three interrupt outputs are available to minimize software overhead associated with data transfer. Also, by using the DMA interface two or more DEUs may be operated in parallel to achieve effective system conversion rates which are virtually any multiple of 80 bytes/second. The 8294 also has a 7-bit TTL compatible output port for user-specified functions.

Because the 8294 implements the NBS encryption algorithm it can be used in a variety of Electronic Funds Transfer applications as well as other electronic banking and data handling applications where data must be encrypted.

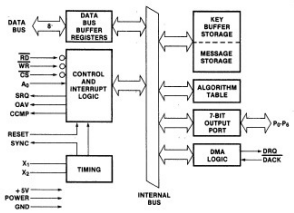


Figure 1. Block Diagram

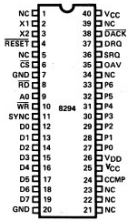


Figure 2. Pin Configuration

8-330

http://www.bitsavers.org/components/intel/_dataBooks/1981_Intel_Component_Data_Catalog.pdf

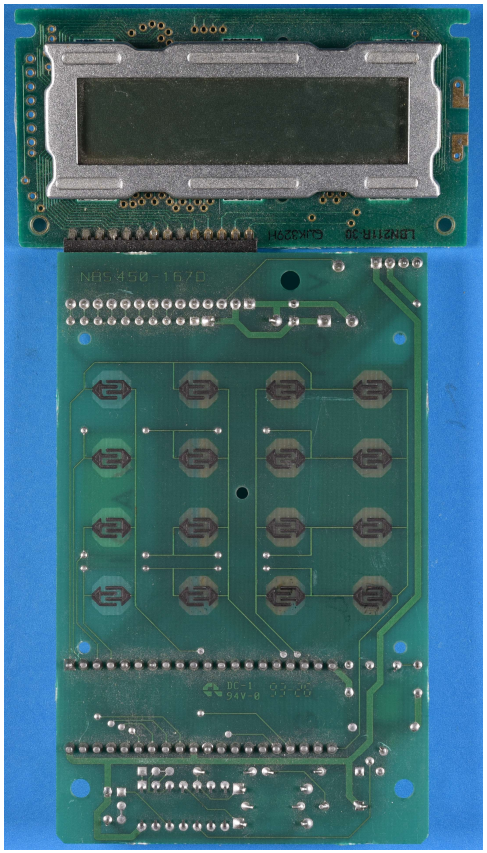
Bank Machine and Pinpad

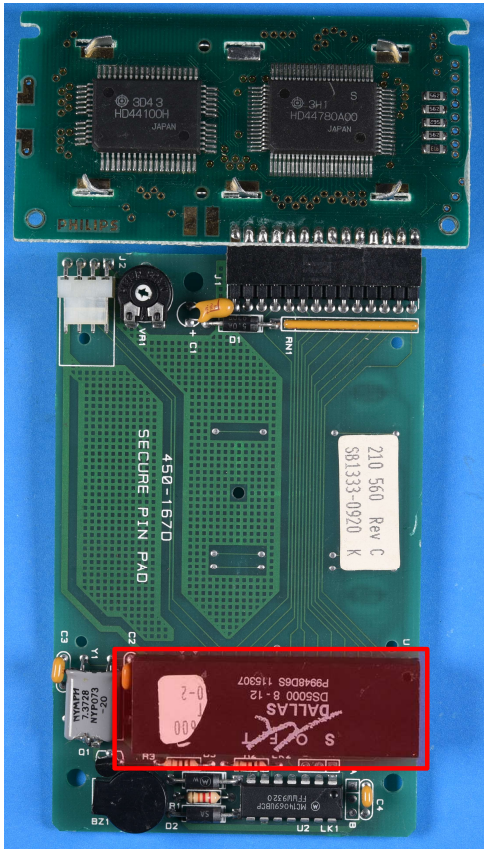
- Bank machines located in retailers requires a higher level of security than epoxy!
- Fake machine hardware could be engineered to capture banking secrets such as PIN and card numbers.
- Tapping that cable connection would be an obvious target.

Pinpad Anti-Tamper Seal

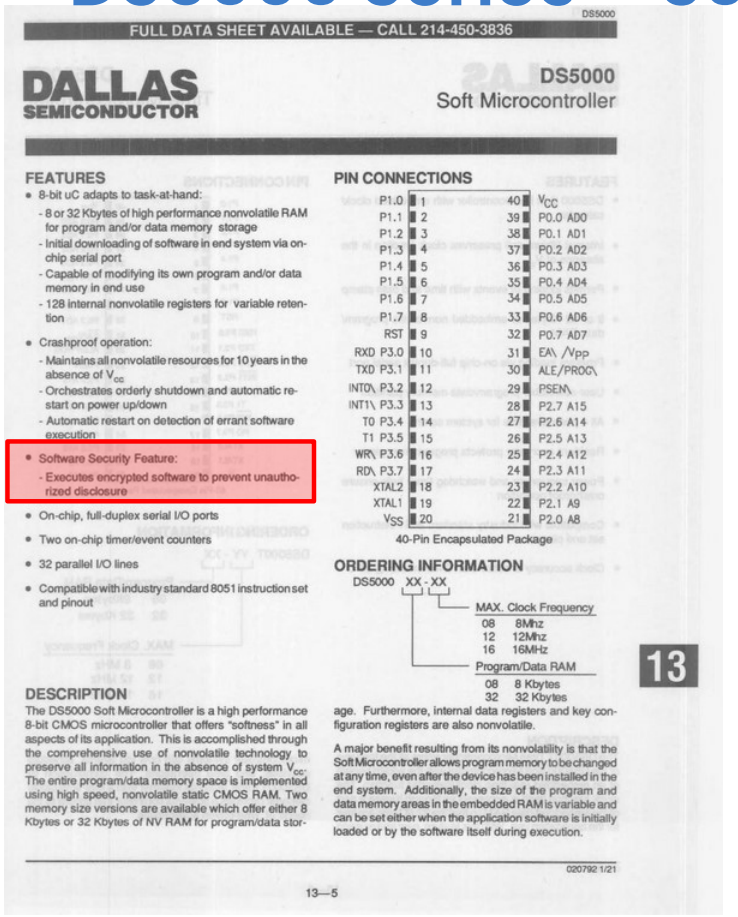
- PIN pad device contains an anti-tamper hologram seal.
- Who flips this over and verifies its presence prior to interaction?

Inside Early Generation Pin Pad





DS5000 Series – 30 Years In Production!



DS5000

FULL DATA SHEET AVAILABLE — CALL 214-450-3836

DALLAS SEMICONDUCTOR

DS5000
Soft Microcontroller

FEATURES

- 8-bit uC adapts to task-at-hand:
  - 8 or 32 Kbytes of high performance nonvolatile RAM for program and/or data memory storage
  - Initial downloading of software in end system via on-chip serial port
  - Capable of modifying its own program and/or data memory in end use
  - 128 internal nonvolatile registers for variable retention
- Crashproof operation:
  - Maintains all nonvolatile resources for 10 years in the absence of V_{cc}
  - Orchestrates orderly shutdown and automatic restart on power up/down
  - Automatic restart on detection of errant software execution
- Software Security Feature:
  - Executes encrypted software to prevent unauthorized disclosure
- On-chip, full-duplex serial I/O ports
- Two on-chip timer/event counters
- 32 parallel I/O lines
- Compatible with industry standard 8051 instruction set and pinout

PIN CONNECTIONS

P1.0	1	40	V_{CC}
P1.1	2	39	P0.0 AD0
P1.2	3	38	P0.1 AD1
P1.3	4	37	P0.2 AD2
P1.4	5	36	P0.3 AD3
P1.5	6	35	P0.4 AD4
P1.6	7	34	P0.5 AD5
P1.7	8	33	P0.6 AD6
RST	9	32	P0.7 AD7
RXD P3.0	10	31	EA\ /V_{PP}
TXD P3.1	11	30	ALE/PROG\
INT0\ P3.2	12	29	PSEN\
INT1\ P3.3	13	28	P2.7 A15
T0 P3.4	14	27	P2.6 A14
T1 P3.5	15	26	P2.5 A13
WR\ P3.6	16	25	P2.4 A12
RD\ P3.7	17	24	P2.3 A11
XTAL2	18	23	P2.2 A10
XTAL1	19	22	P2.1 A9
V_{SS}	20	21	P2.0 A8

40-Pin Encapsulated Package

ORDERING INFORMATION

DS5000 XX - XX

MAX. Clock Frequency
- 08 8Mhz
- 12 12Mhz
- 16 16MHz

Program/Data RAM
- 08 8 Kbytes
- 32 32 Kbytes

13

DESCRIPTION

The DS5000 Soft Microcontroller is a high performance 8-bit CMOS microcontroller that offers "softness" in all aspects of its application. This is accomplished through the comprehensive use of nonvolatile technology to preserve all information in the absence of system V_{cc}. The entire program/data memory space is implemented using high speed, nonvolatile static CMOS RAM. Two memory size versions are available which offer either 8 Kbytes or 32 Kbytes of NV RAM for program/data storage. Furthermore, internal data registers and key configuration registers are also nonvolatile.

A major benefit resulting from its nonvolatility is that the Soft Microcontroller allows program memory to be changed at any time, even after the device has been installed in the end system. Additionally, the size of the program and data memory areas in the embedded RAM is variable and can be set either when the application software is initially loaded or by the software itself during execution.

020792 1/21

13—5

Source: https://archive.org/details/DallasSemiconductor-1992-1993ProductDataBookOCR/page/n1203/mode/2up

DALLAS SEMICONDUCTOR MAXIM

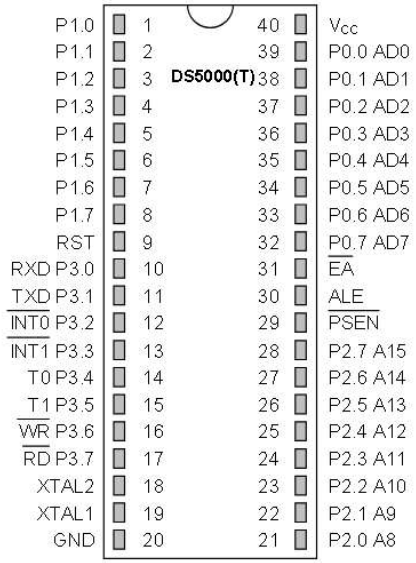
DS5000(T)
Soft Microcontroller Module

www.maxim-ic.com

FEATURES

- **8-Bit 8051-Compatible Microcontroller Adapts to Task at Hand**
  - 8 or 32 kbytes of Nonvolatile RAM for Program and/or Data Memory Storage
  - Initial Downloading of Software in End System via On-Chip Serial Port
  - Capable of Modifying Its Own Program and/or Data Memory in End Use
- **Crashproof Operation**
  - Maintains All Nonvolatile Resources for 10 Years in the Absence of V_{CC} at Room Temperature
  - Power-Fail Reset
  - Early Warning Power-Fail Interrupt
  - Watchdog Timer
- **Software Security Feature**
  - Executes Encrypted Software to Prevent Unauthorized Disclosure
- **On-Chip, Full-Duplex Serial I/O Ports**
- **Two On-Chip Timer/Event Counters**
- **32 Parallel I/O Lines**
- **Compatible with Industry Standard 8051 Instruction Set and Pinout**
- **Optional Permanently Powered Real-Time Clock (DS5000T)**

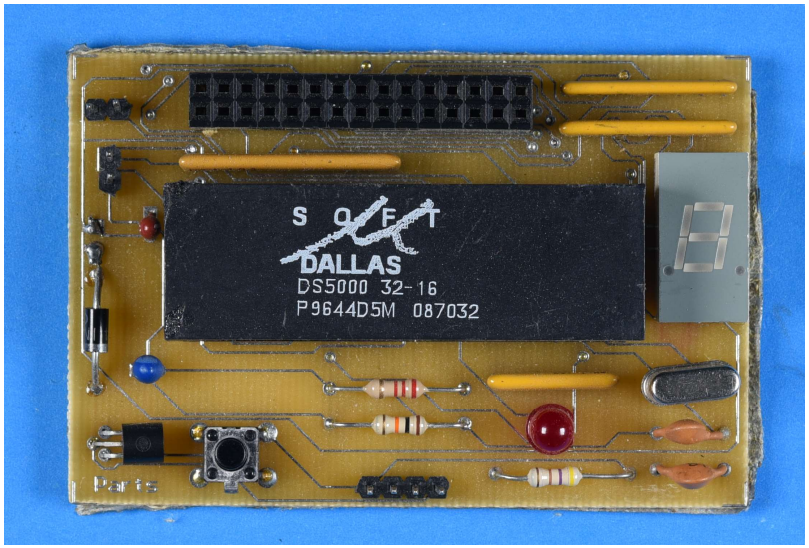
PIN ASSIGNMENT

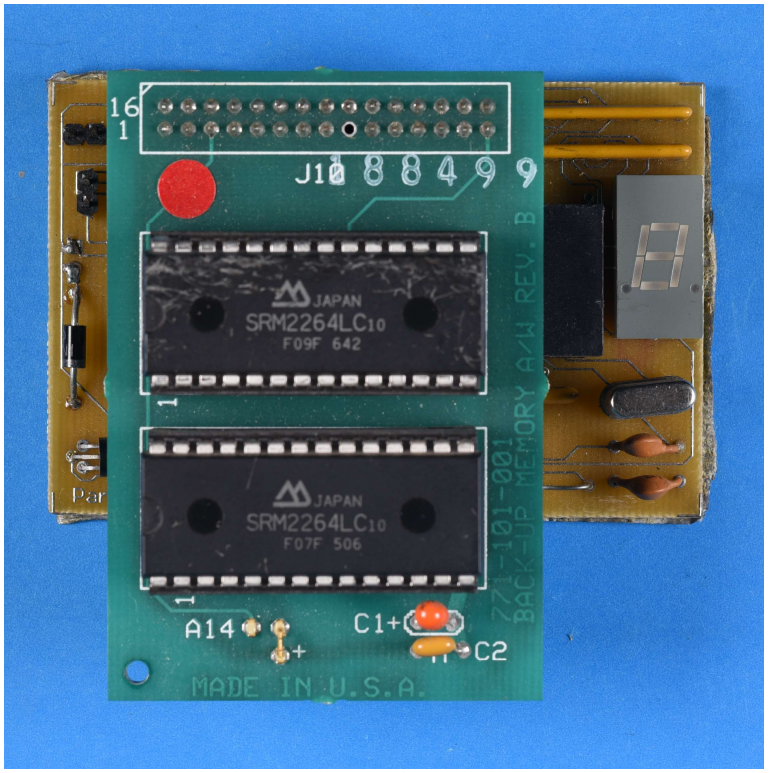


40-Pin Encapsulated Package

Source: https://www.analog.com/media/en/technical-documentation/data-sheets/DS5000-DS5000T.pdf P1

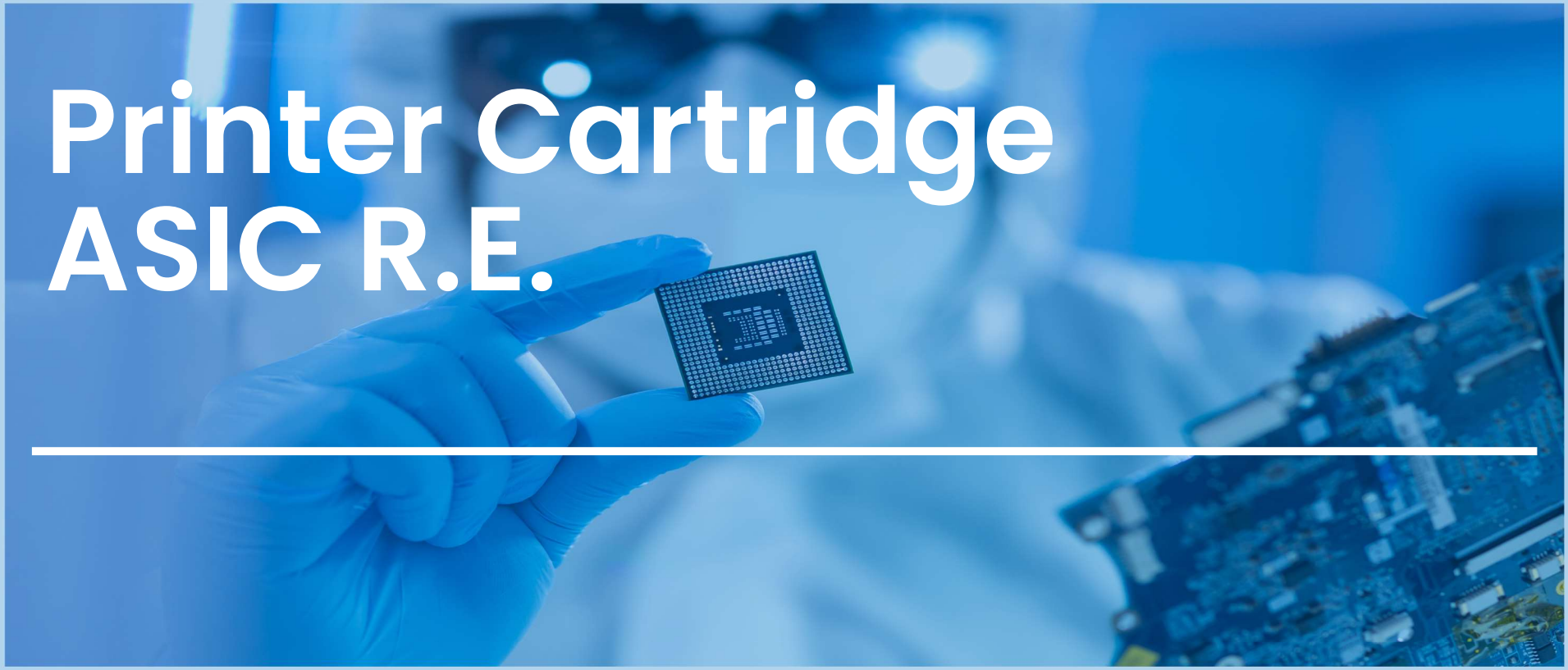
Secure your Reverse-Engineering





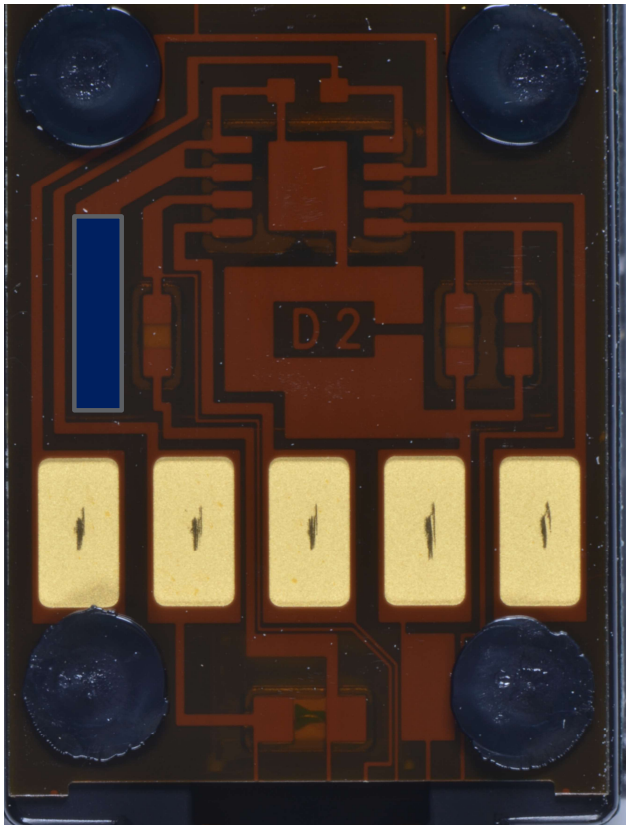
- Using the DS5000 device to secure my RE effort.
- Built and sold these devices to backup, edit and over-write SRAM modules

Printer Cartridge ASIC R.E.

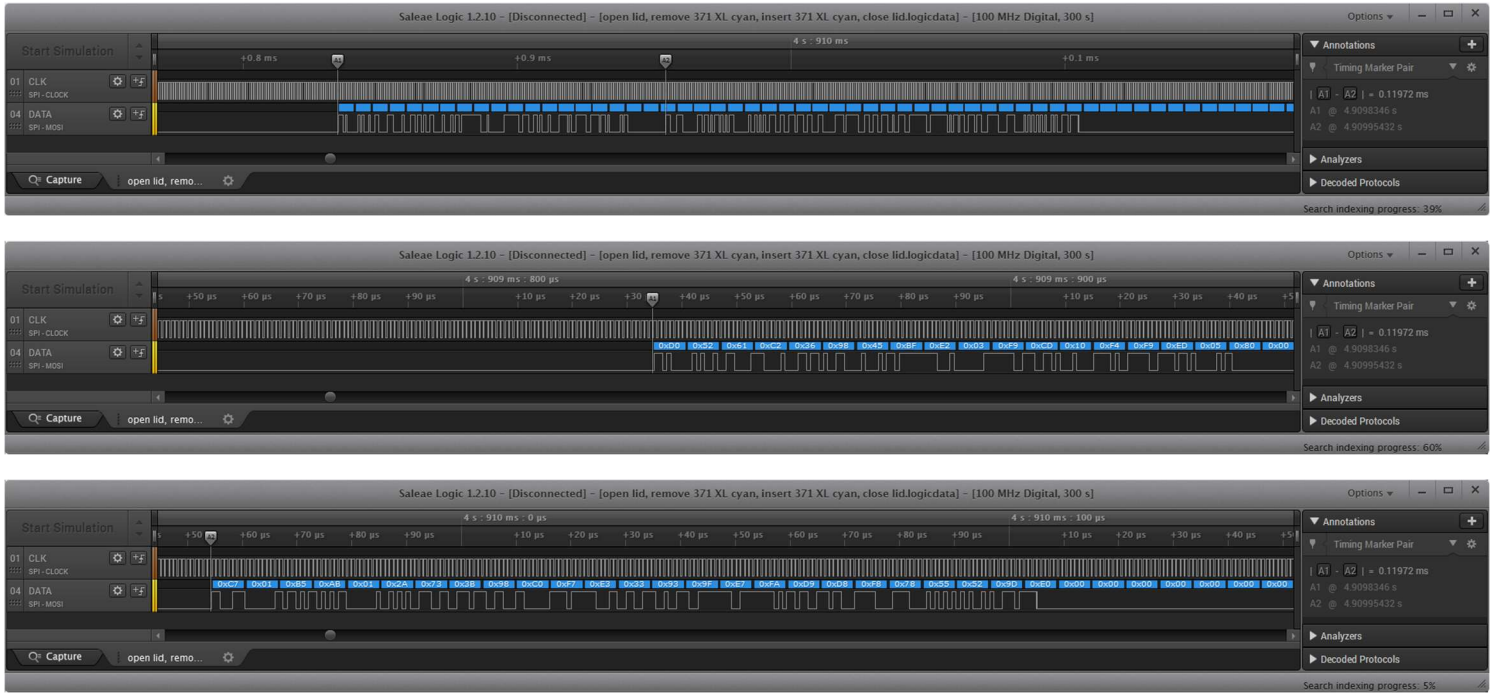


Printer Cartridge – Photo of Flex PCB

- Photographs of the device showing the contact points on the flex PCB.
- Contact points terminate at 8 pin device.



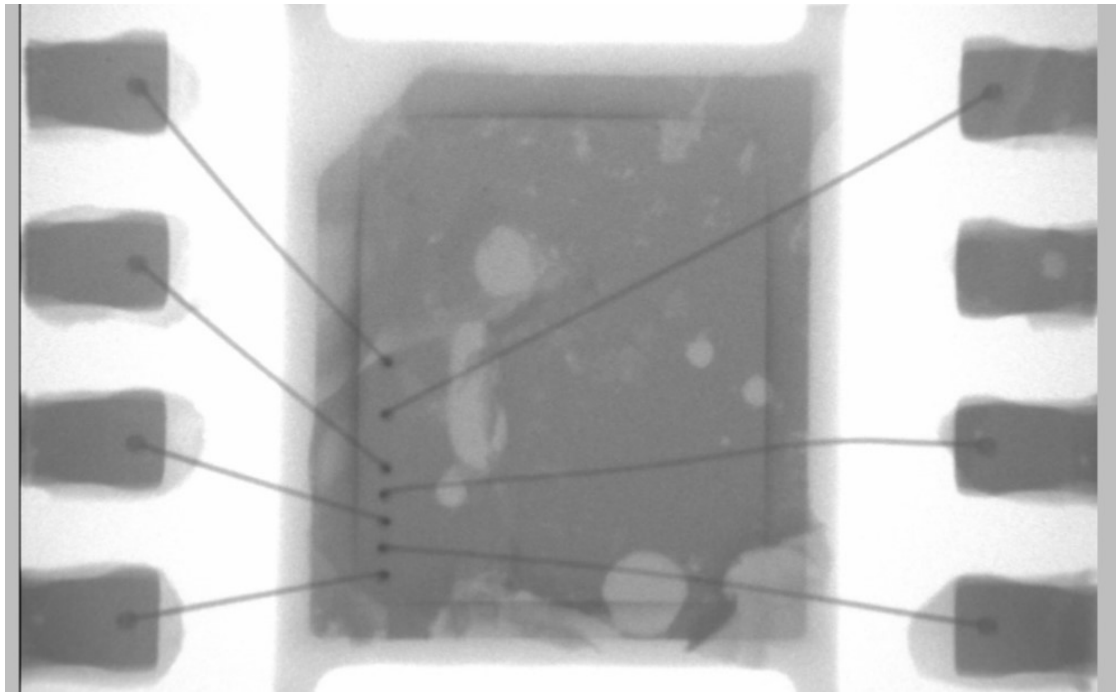
Communications Sniffing and Replay



- Three types of packets observed. Long command with payload, short command and response. Different Ink cartridges logged under various conditions.

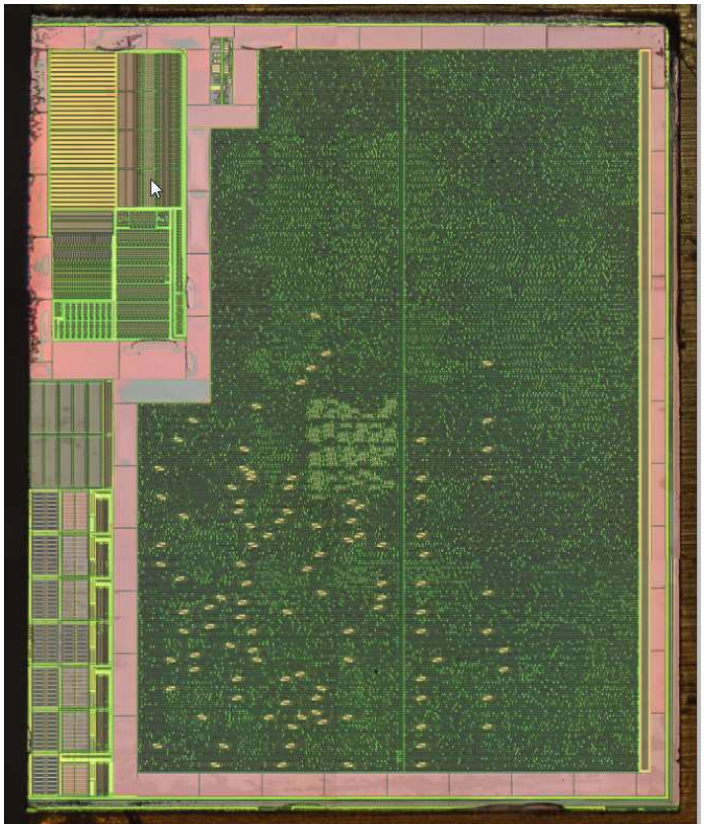
X-Ray Image of Die and Bond Wires

- X-Ray image used to see bond wires and assigned pads.



Topside and Backside Poly Images

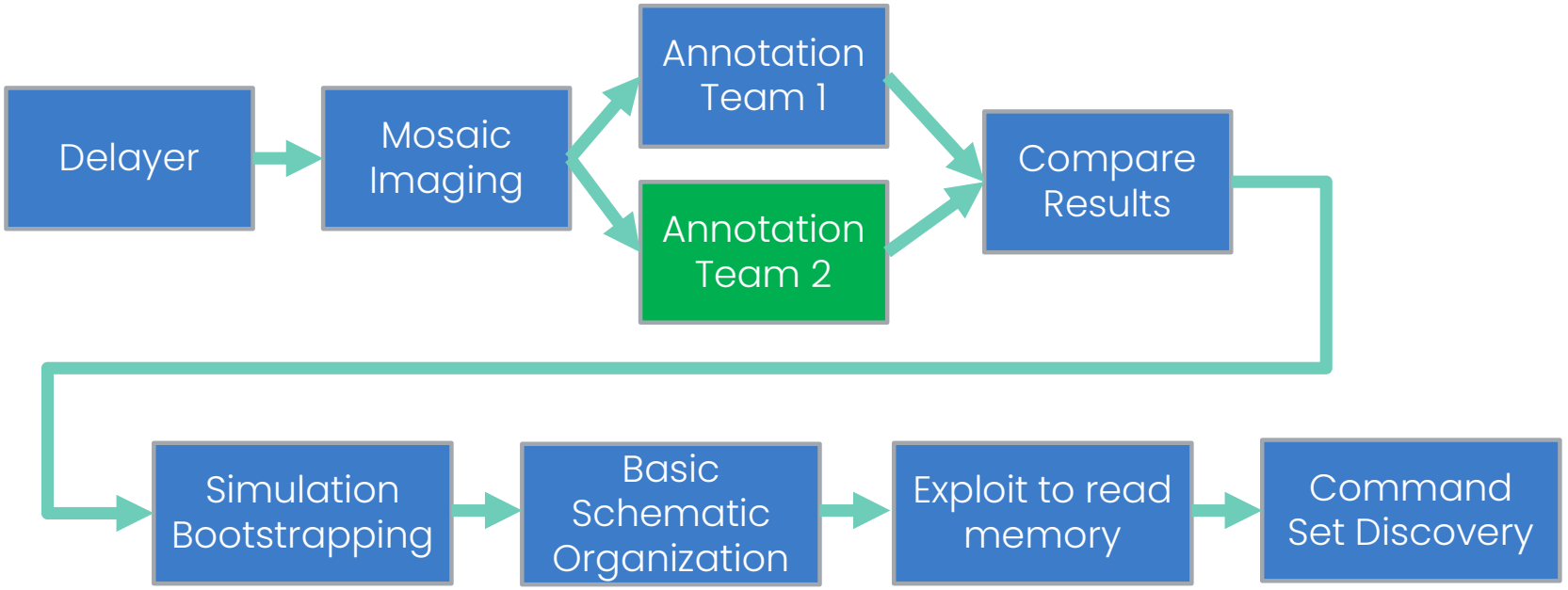
- Die appears to be memory and digital logic. Not CPU



Process Sequence

Extract full chip netlist

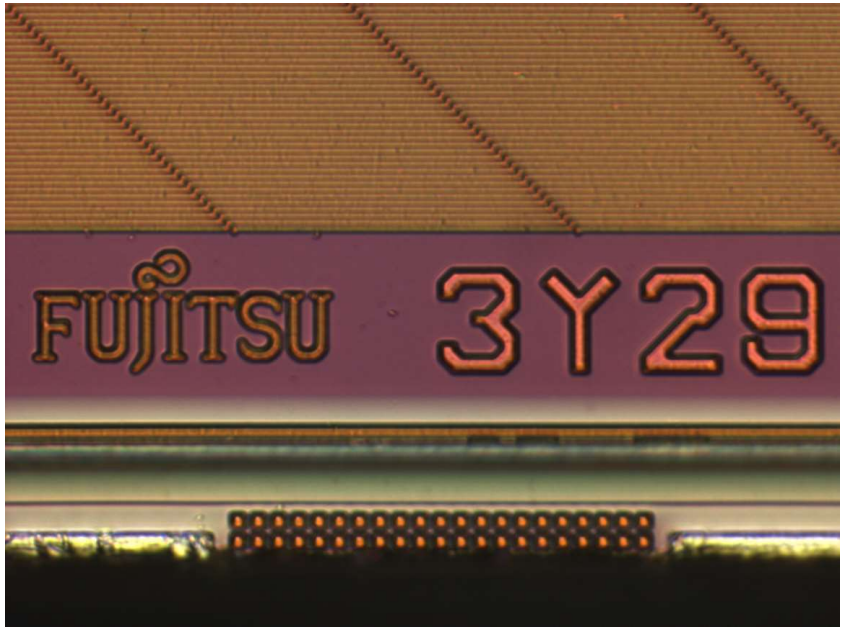
- 30K Gates approx



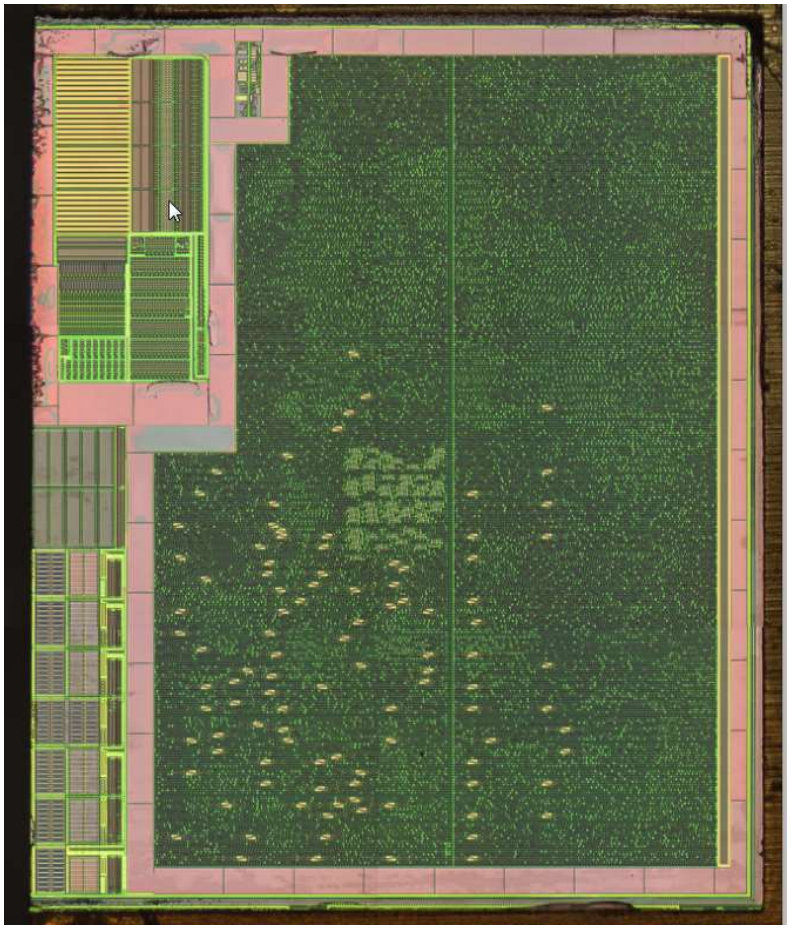
VERILOG MODEL

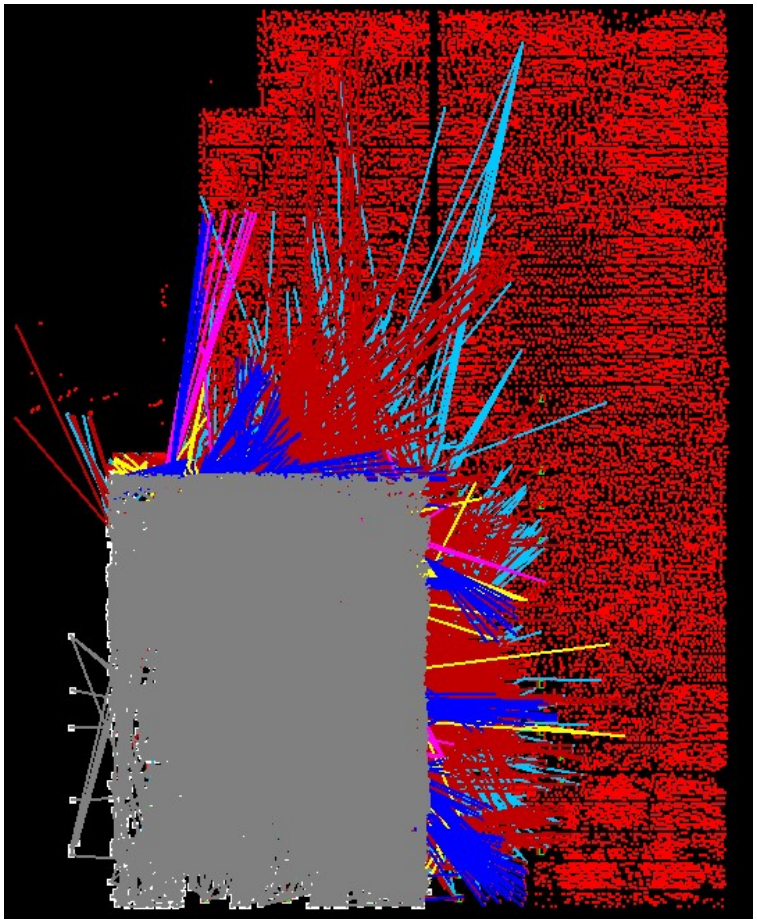
Die Markings

- Die Markings indicate that all samples are the same die.



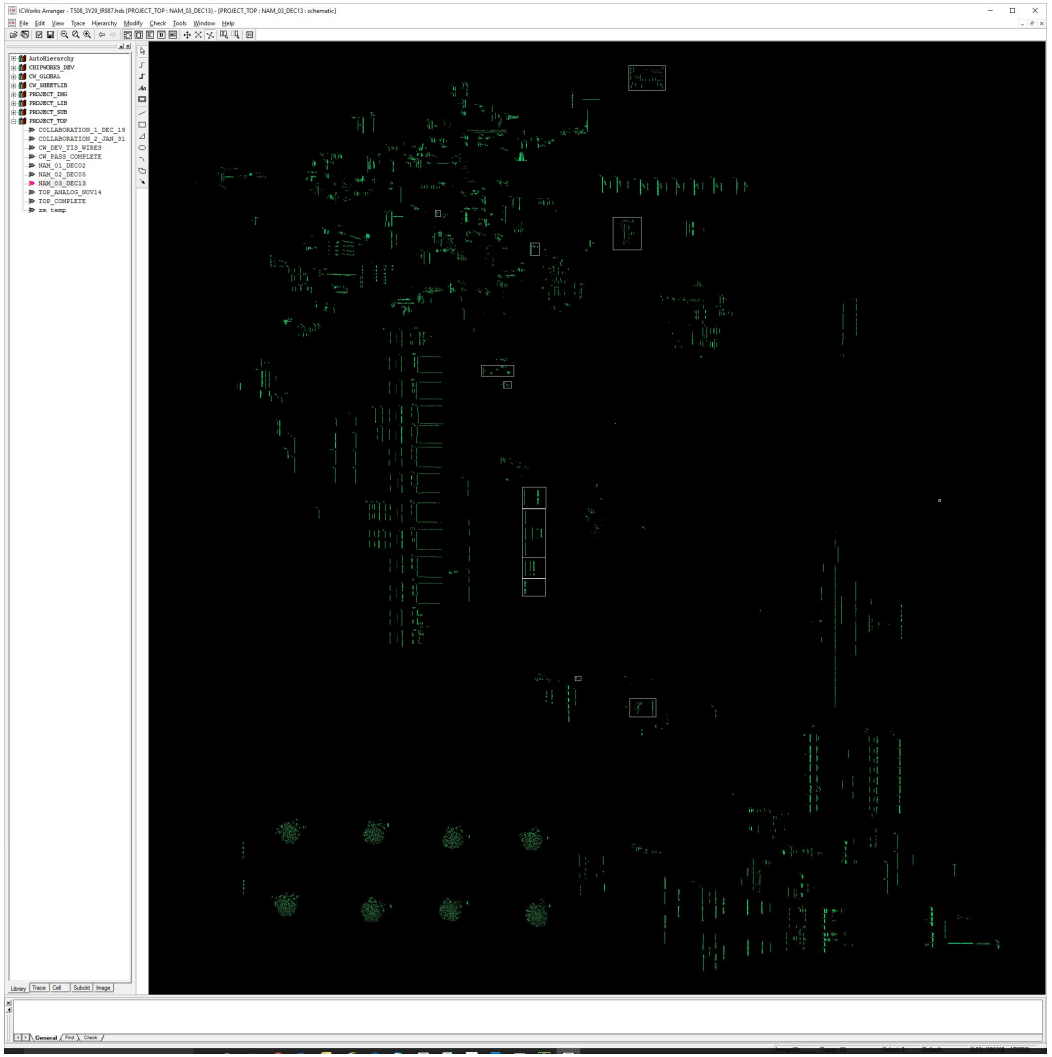
Netlist Generation and Visualization Tool



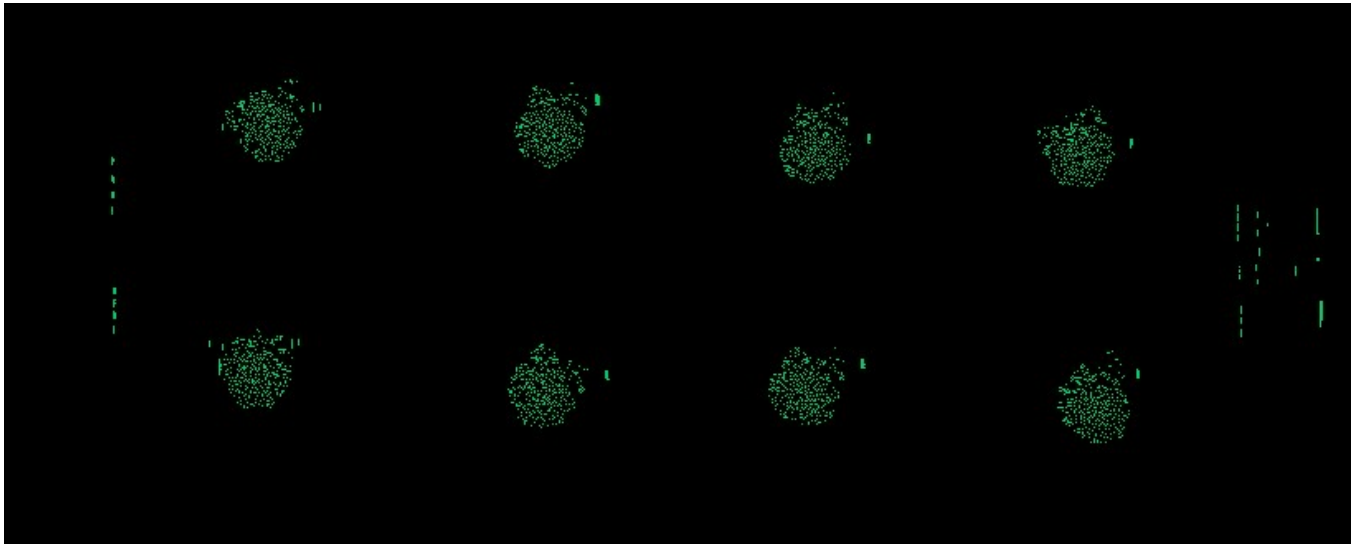


Netlist Cluster

- Cells are organized in groups based on interconnect statistics using in house software tool.

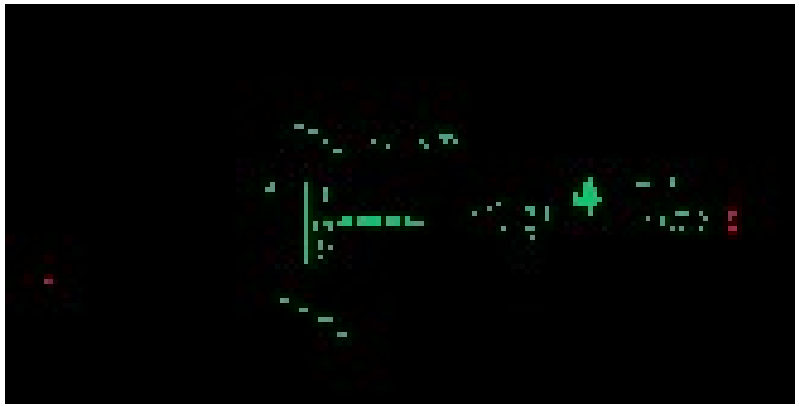


Transformation Block



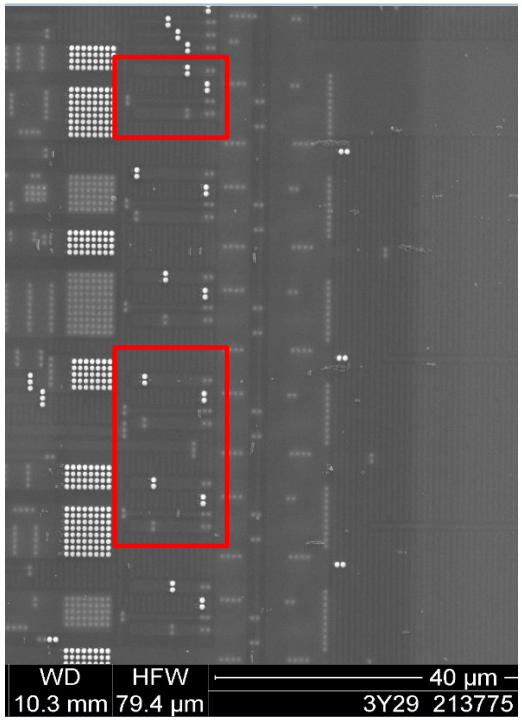
Active Shield Protection Block

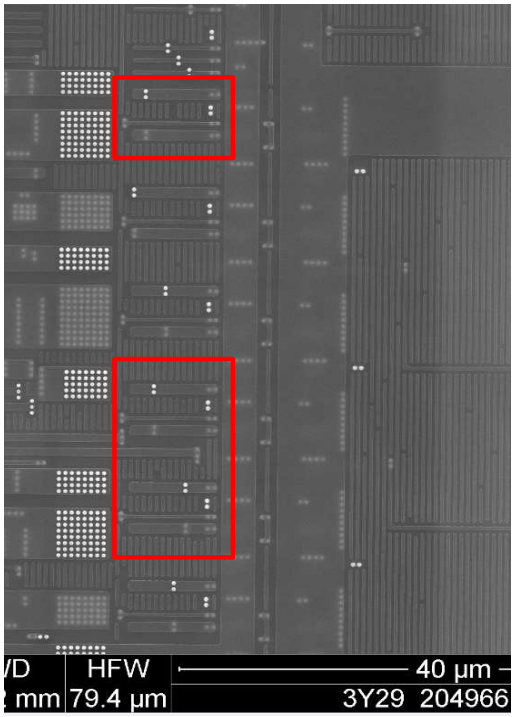
- Red dots are the input/output connections to the gate cluster.



Mismatched Via Locations

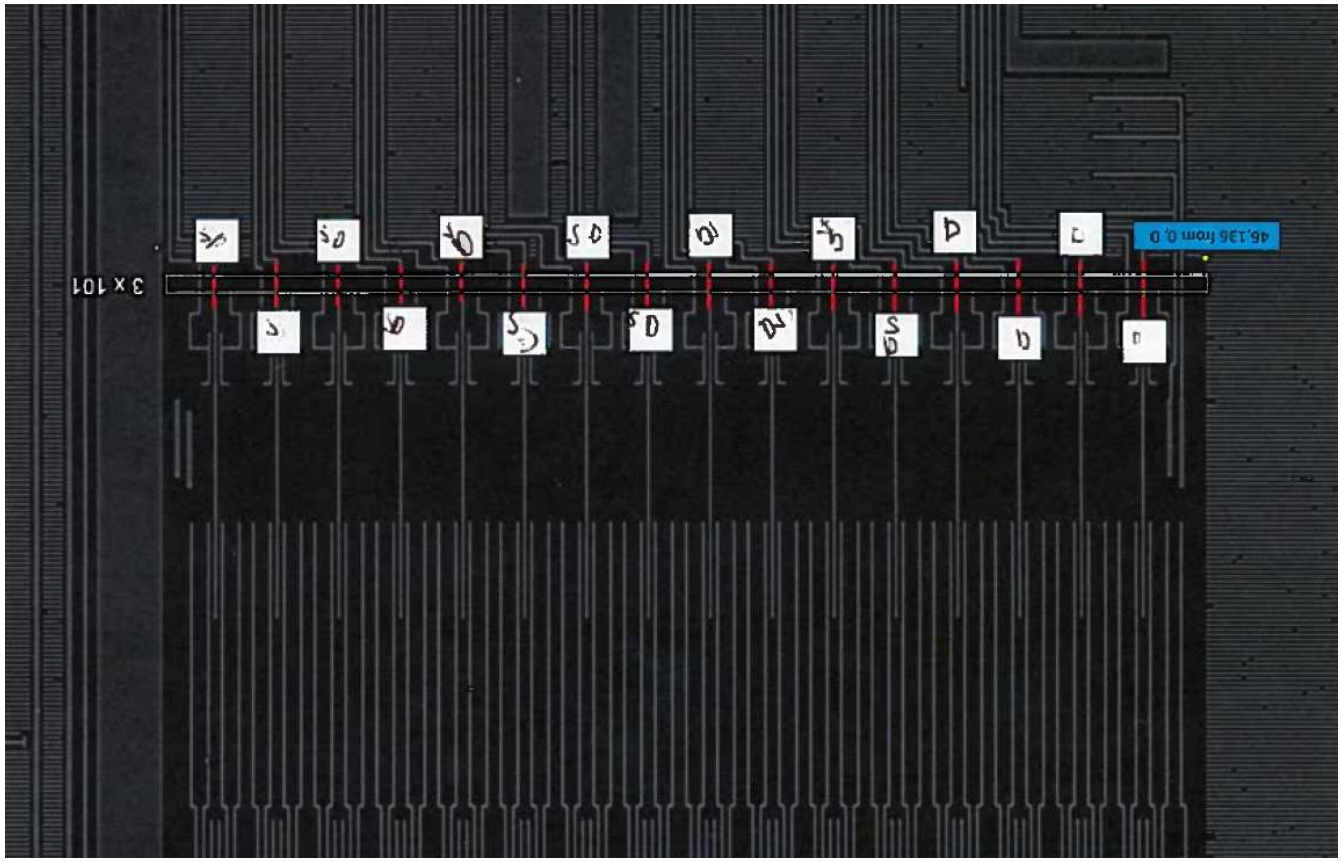
- Despite identical die markings, it was found that the via positioning between metal layers was different.
- This was not significant as it did not affect the overall logic as they were found to connect address lines in different places.





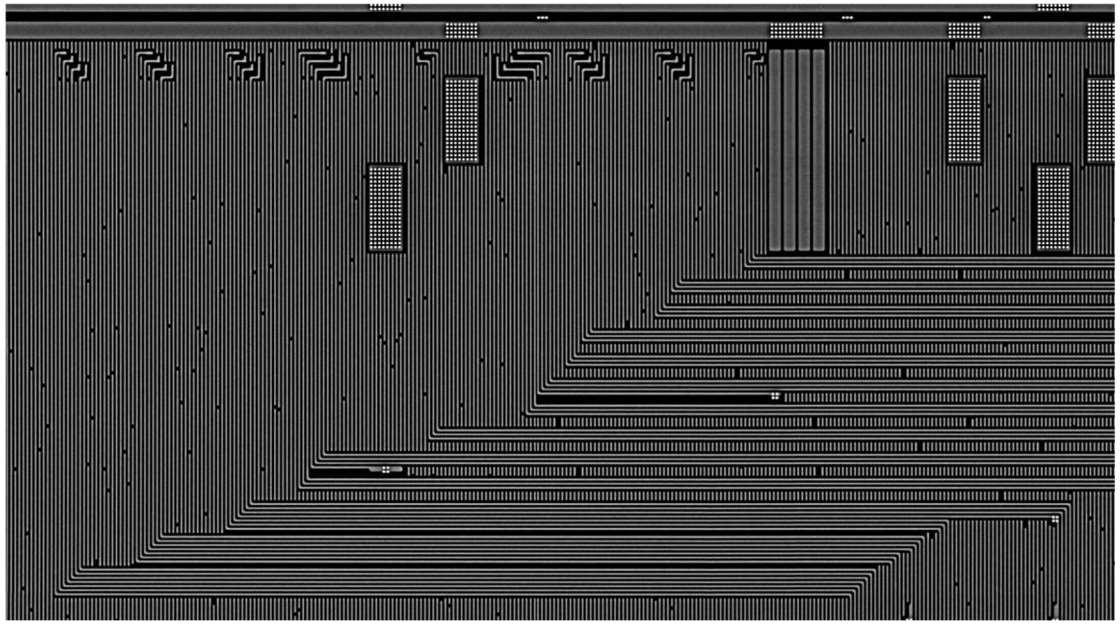
Data Lines Connected to NV Memory Array

- This appears to be a great spot to probe, however reaching it at his position is not feasible though the layers. The lines must be traced to an area that resides under “null” space in each metal layer above it.



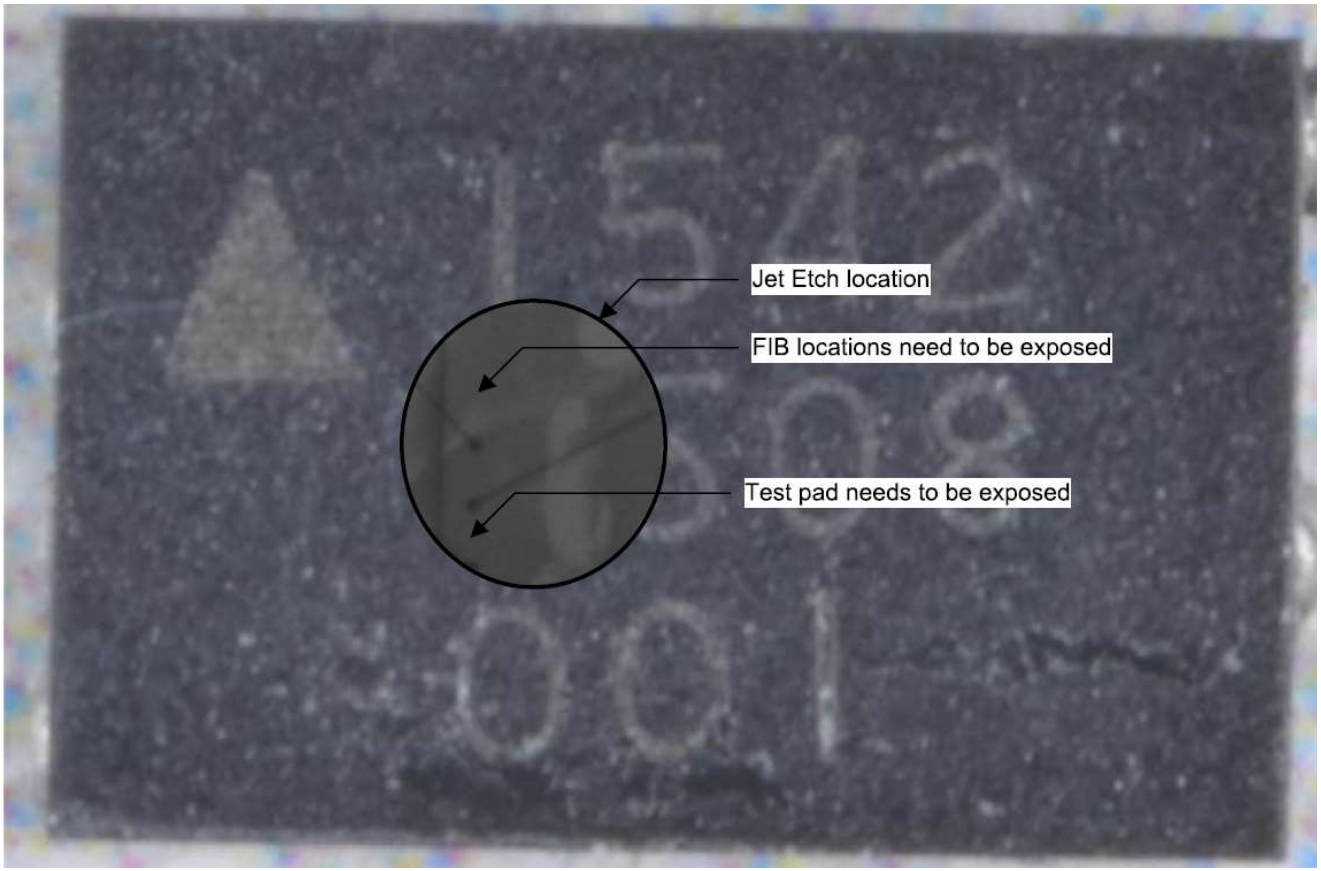
Data Bit Lines On M2 Layer

- Found a prospective spot on the M2 layer that can be reached from top though M5,4 and 3 layers.

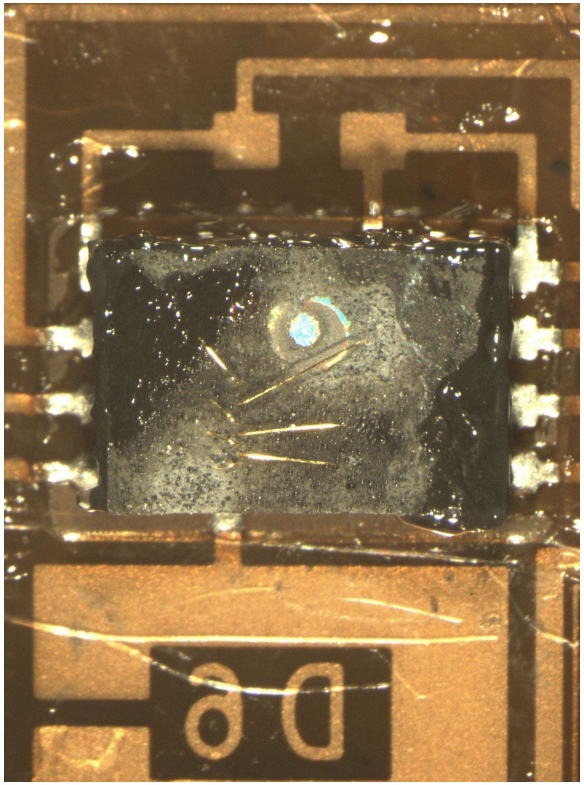


Jet Etch – Entering the Package

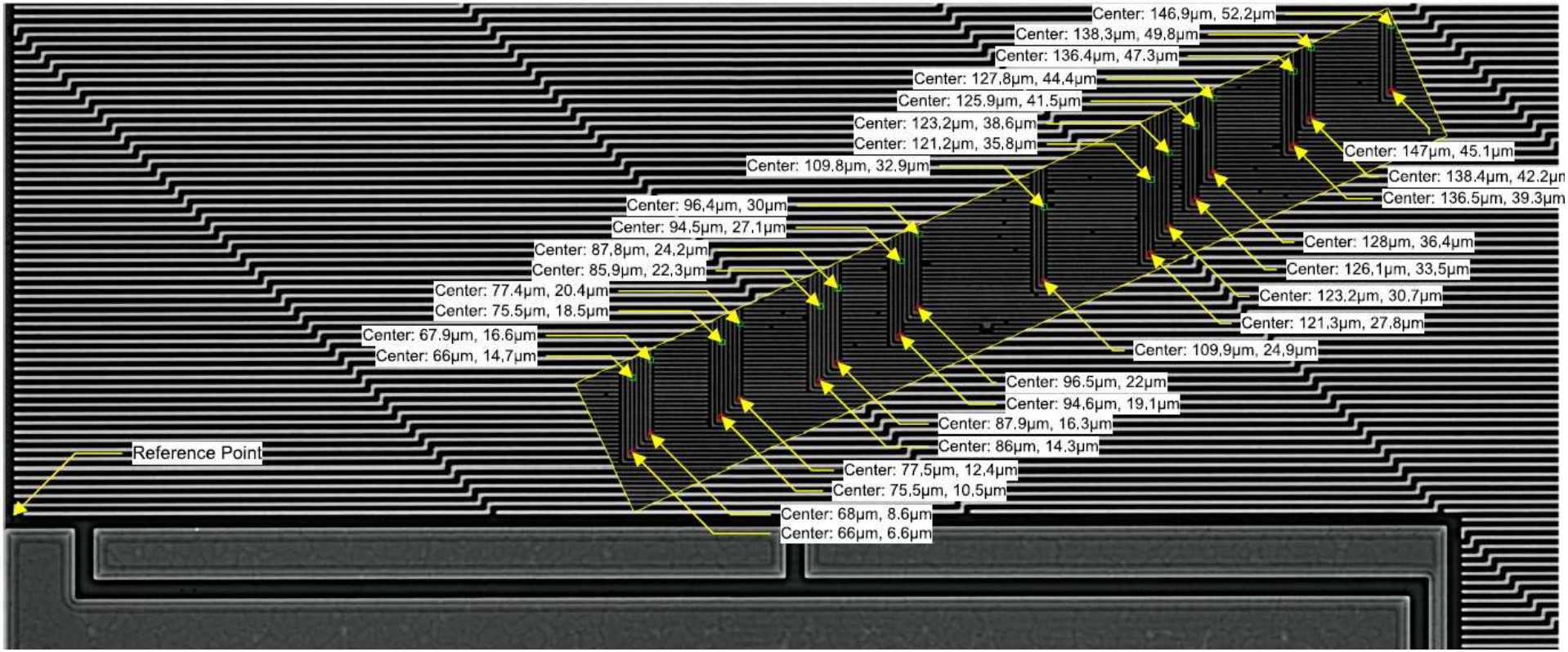
- Jet Etching away a hole in the package exposing the die in the area of interest.



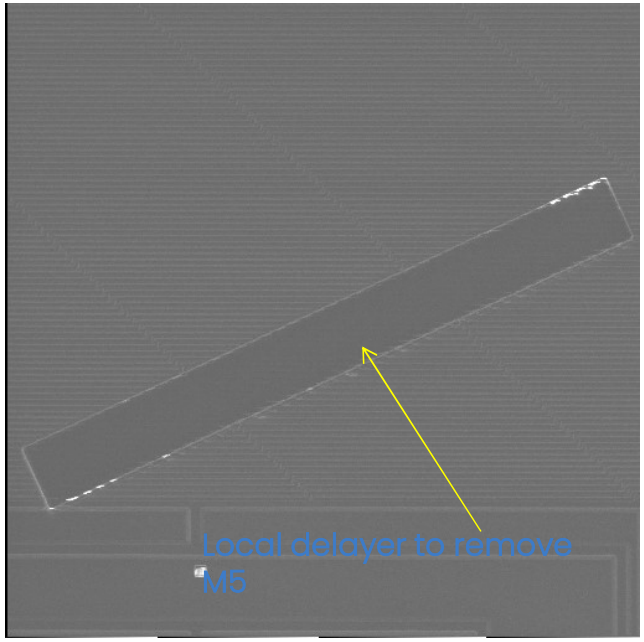
Jet Etch – Entering the Package

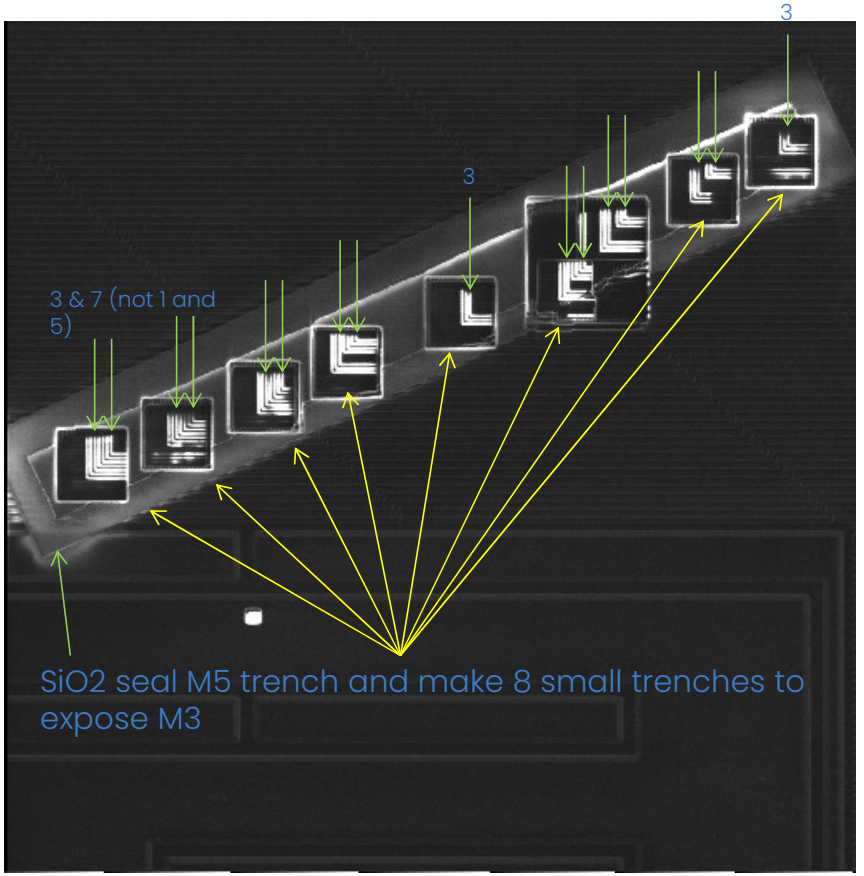


FIB Edit Planning

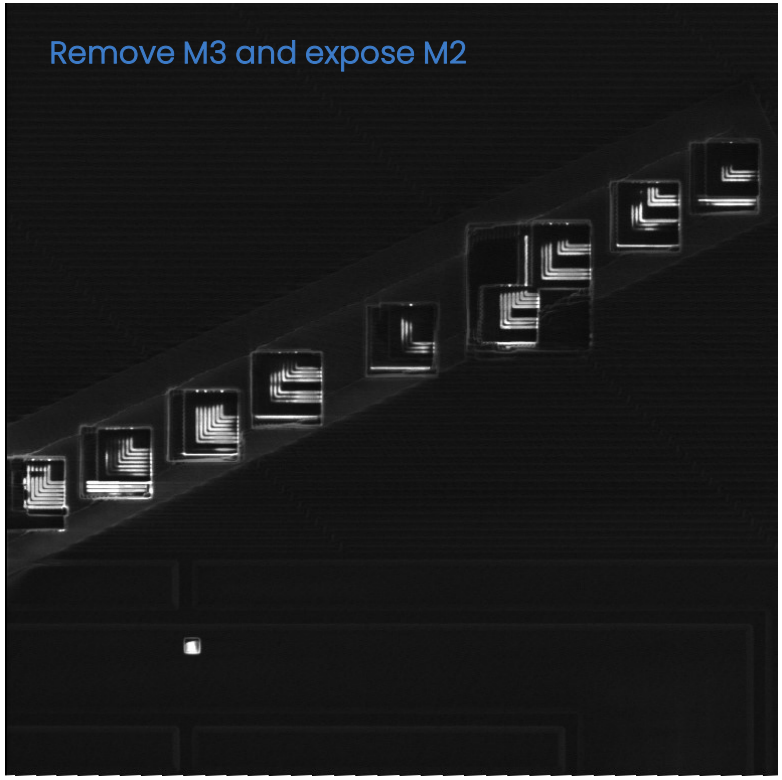


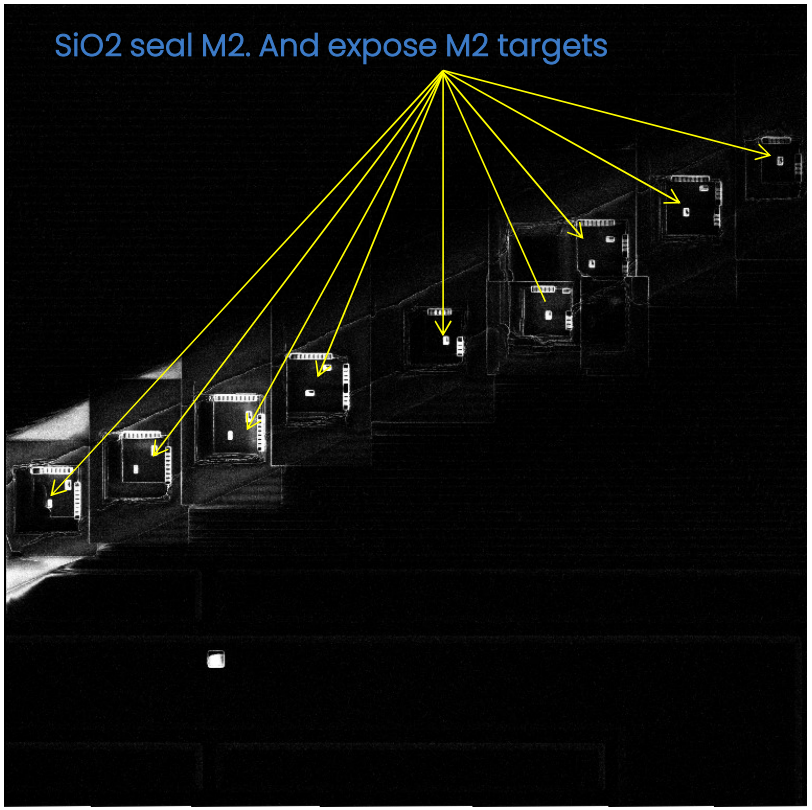
Delayer / Remove M5 Section





Delayer - Remove M3

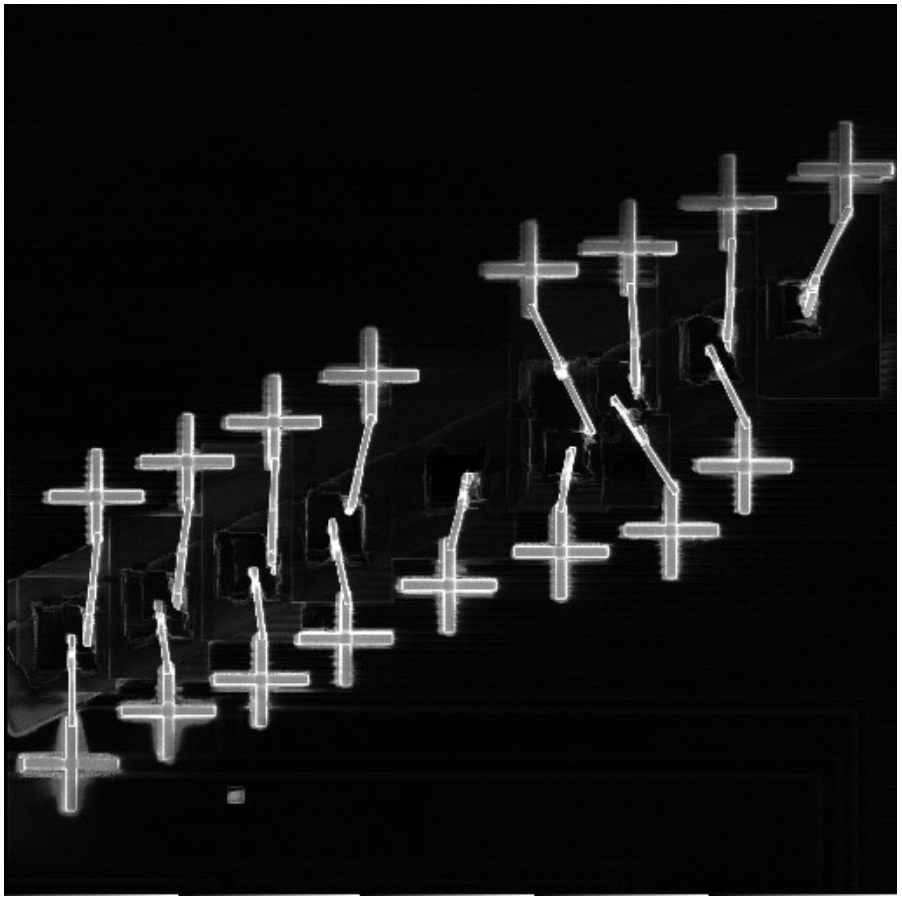




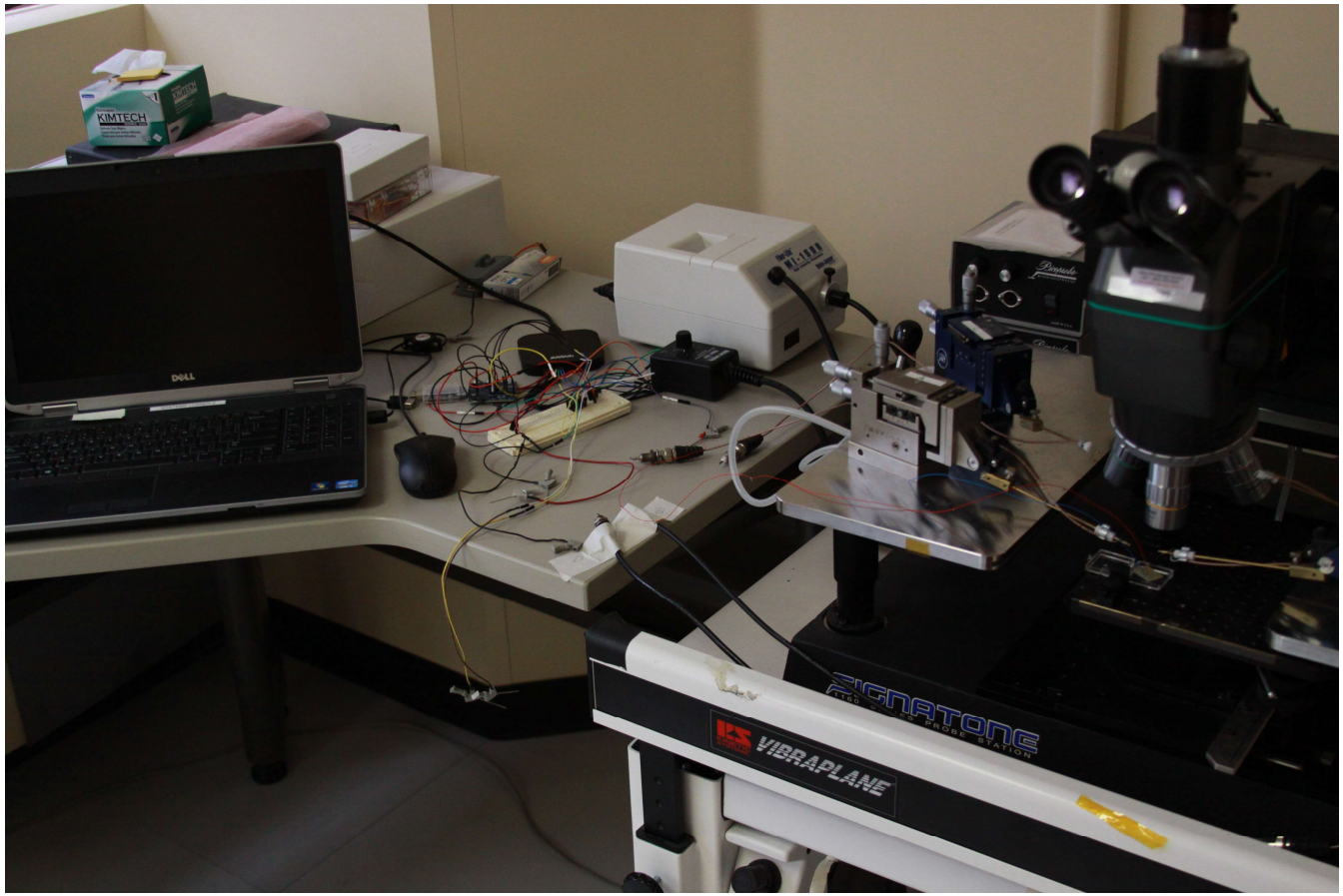
Exposed Connections

SiO2 seal the reference

Pad Placement for Probes

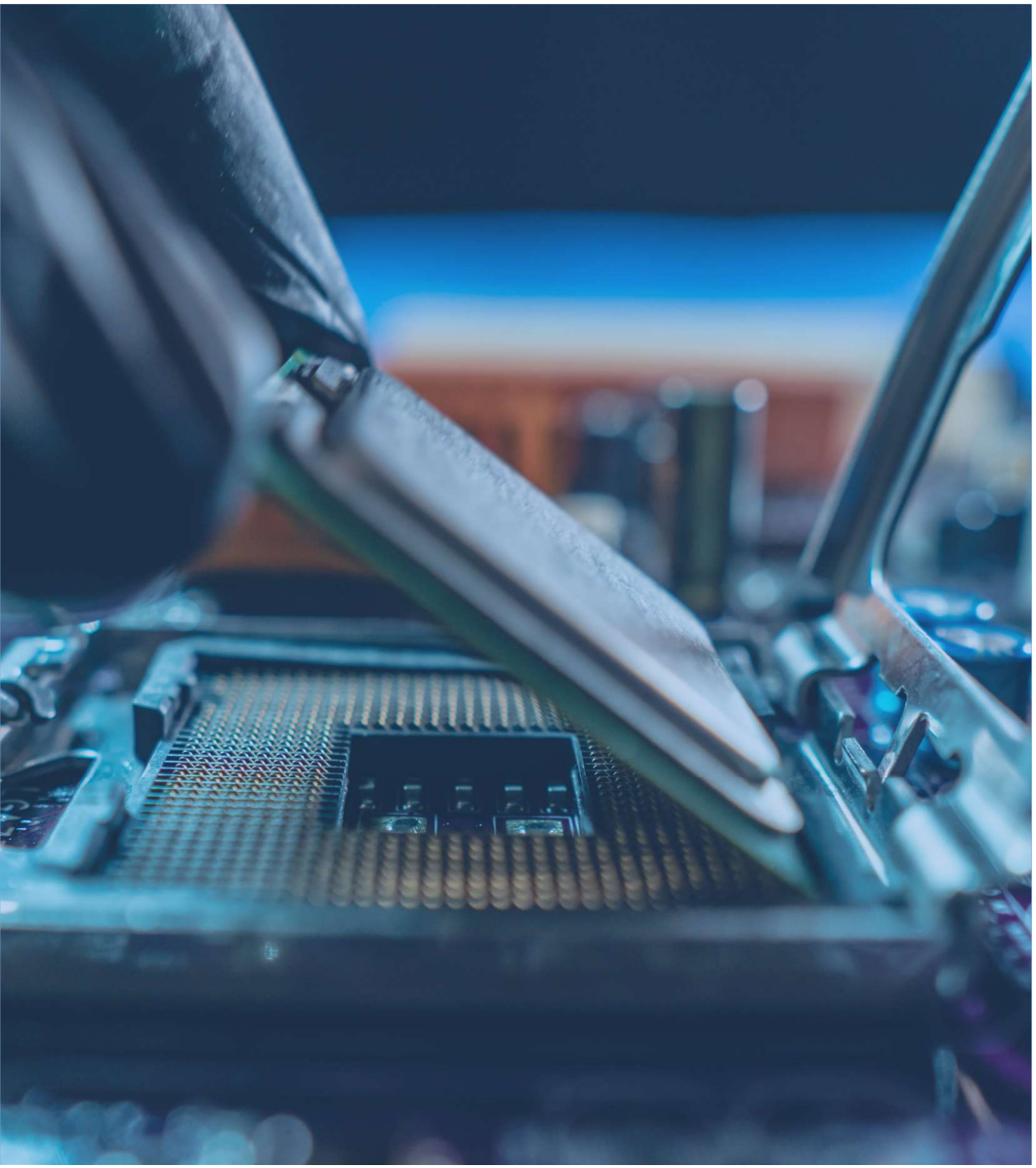


Memory Read Out Setup



8 clocks to enter test mode
1 clock for a don't care
10 clocks per memory read * 64 reads = 640 clocks

Break Section



About TechInsights

TechInsights is the information platform for the semiconductor industry.

Regarded as the most trusted source of actionable, in-depth intelligence related to semiconductor innovation and surrounding markets, TechInsights' content informs decision makers and professionals whose success depends on accurate knowledge of the semiconductor industry—past, present, or future.

Over 650 companies and 100,000 users access the TechInsights Platform, the world's largest vertically integrated collection of unmatched reverse engineering, teardown, and market analysis in the semiconductor industry. This collection includes detailed circuit analysis and imagery, process flows, device teardowns, illustrations, costing and pricing information, forecasts, market analysis, and expert commentary. TechInsights' customers include the most successful technology companies who rely on TechInsights' analysis to make informed business, design, and product decisions faster and with greater confidence. For more information, visit www.techinsights.com.

TechInsights

1891 Robertson Road
Suite 500
Ottawa, Ontario K2H 5B7
Canada

T 1-613-599-6500
F 1-613-599-6501
Web site: www.techinsights.com
Email: support@techinsights.com

Tech Insights