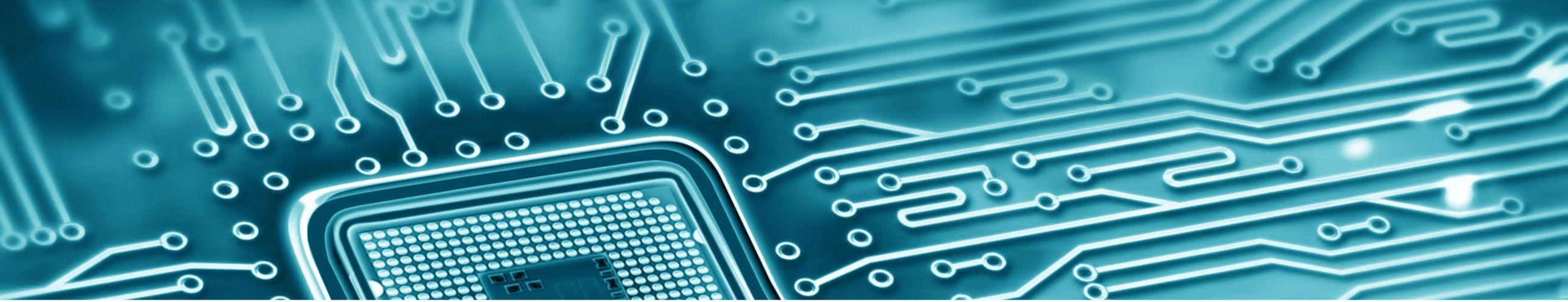
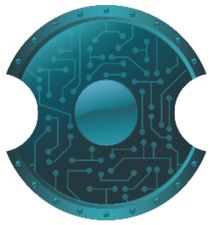
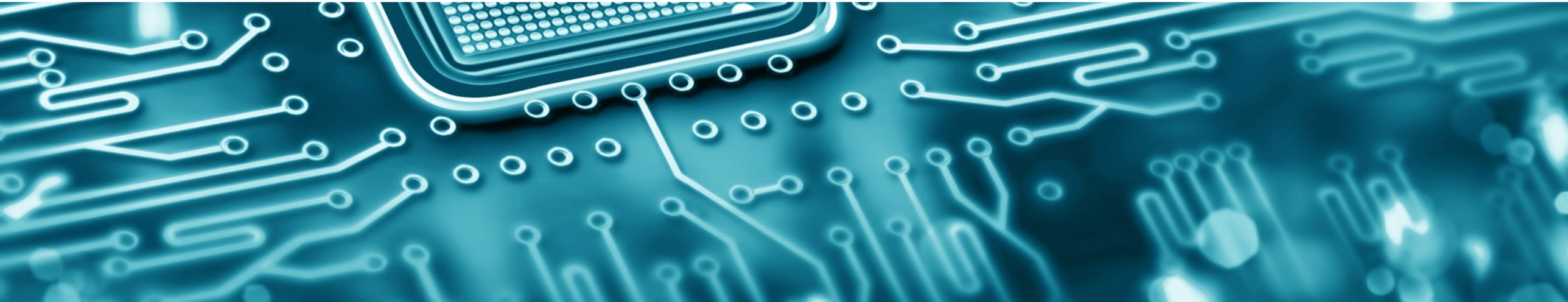
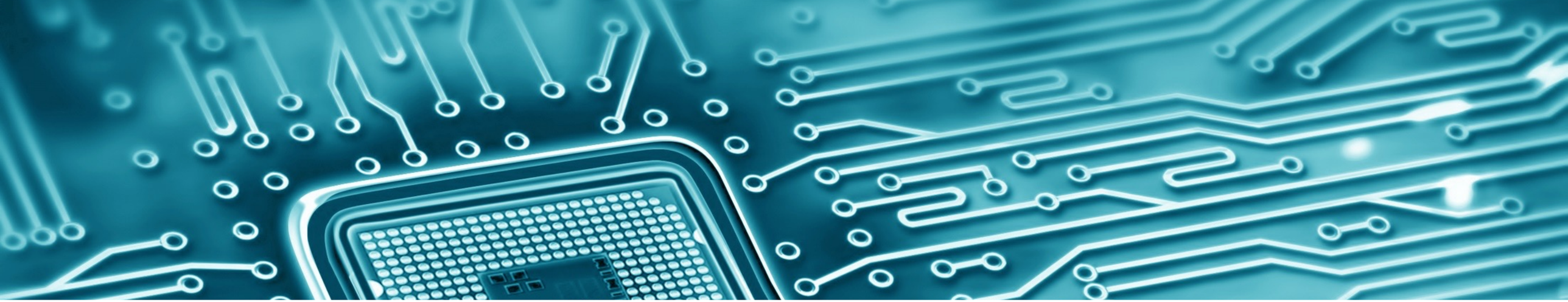




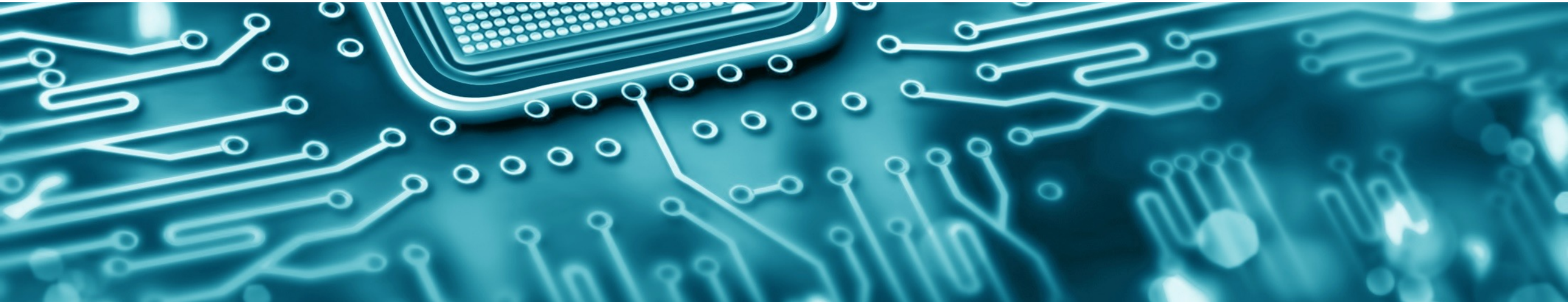
# Texplained

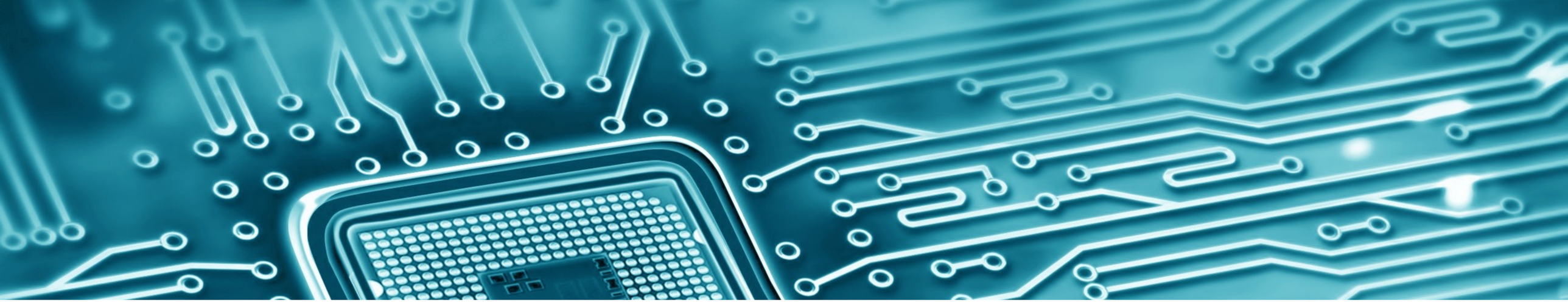
HARDWARE SECURITY INSIGHT



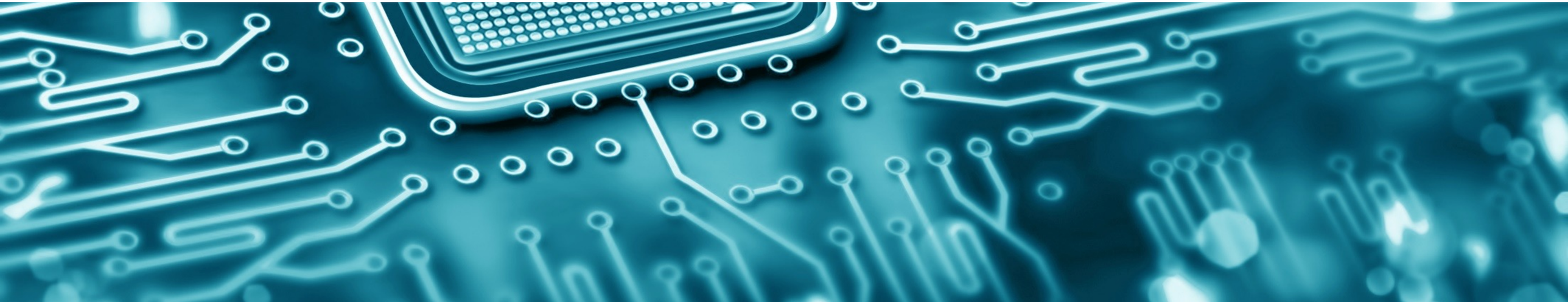


# INTEGRATED CIRCUIT OFFENSIVE SECURITY





# INTRODUCTION

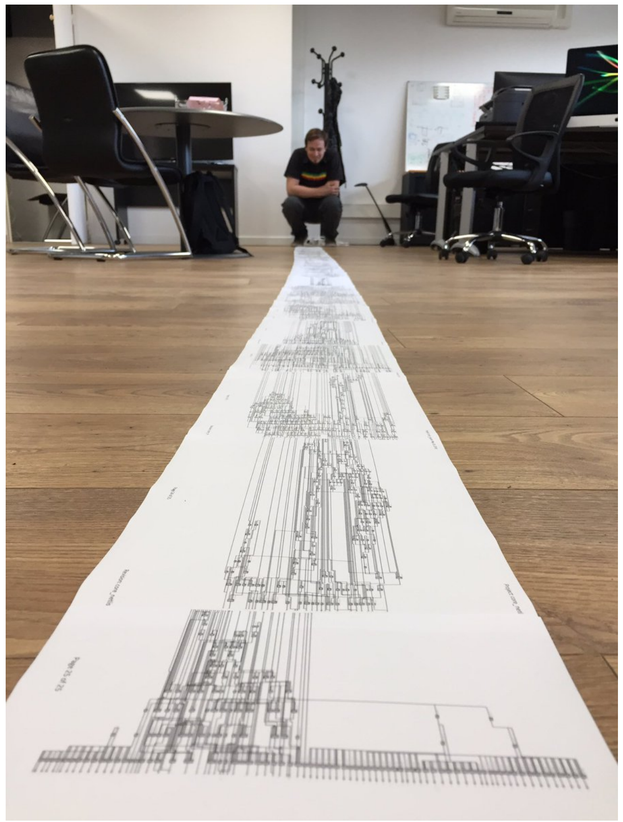


# Texplained - Overview

## R&D - Lab

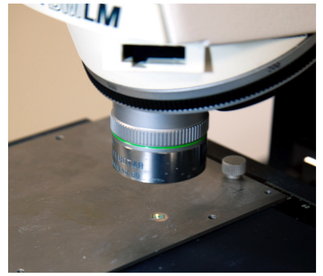
### Texplained

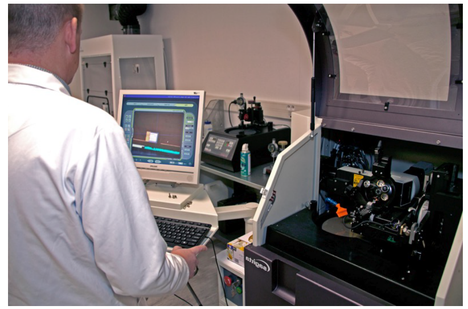
Specialty: Texplained, experts in Integrated Circuits (ICs) reverse-engineering.

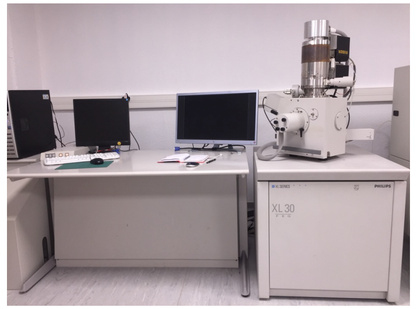


### IC INSIDE

Speciality: IC Inside Lab is a Failure Analysis Laboratory dedicated to Integrated Circuits sample preparation and imagery



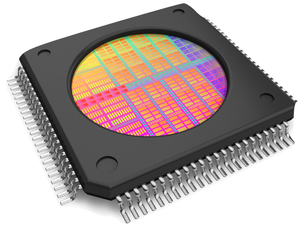




# Texplained - Overview

Texplained

## R&D - Lab



**Architecture => Layout**

- Design Review / Trainings
- Hw countermeasure

**Manufacturing**

- Backdoor Research

**In the field**

- In-depth Explorations
- Pirated Devices analysis
- IP Infringement proof

**End of life**

- Obsolescence Management

**Lifecycle of an Integrated Circuit**

- Custom Analyses
- Backdoor Research
- IP Infringement proof

CHIPJUICE

AUTOMATED REVERSE ENGINEERING SOFTWARE

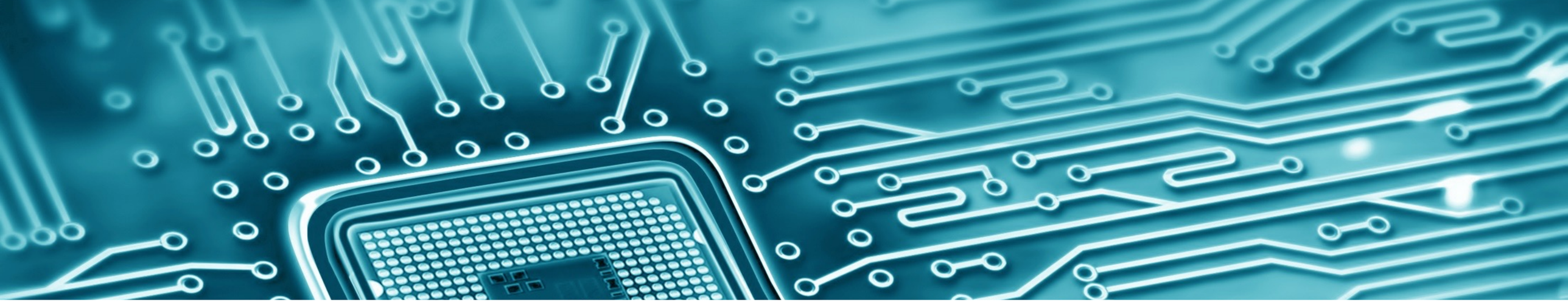
## Summary :

Goal : Let's discuss the following

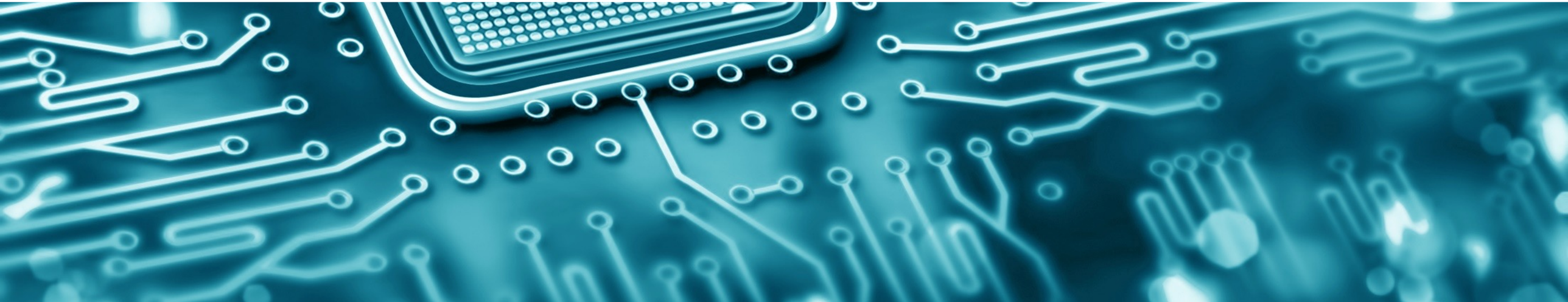
- IC RE and invasive attacks are often considered as a residual threat by certification schemes / Chip vendors
- In a number of applications, REing a chip and extracting its embedded data is common practice
- IC security seems to be used in an offensive context only

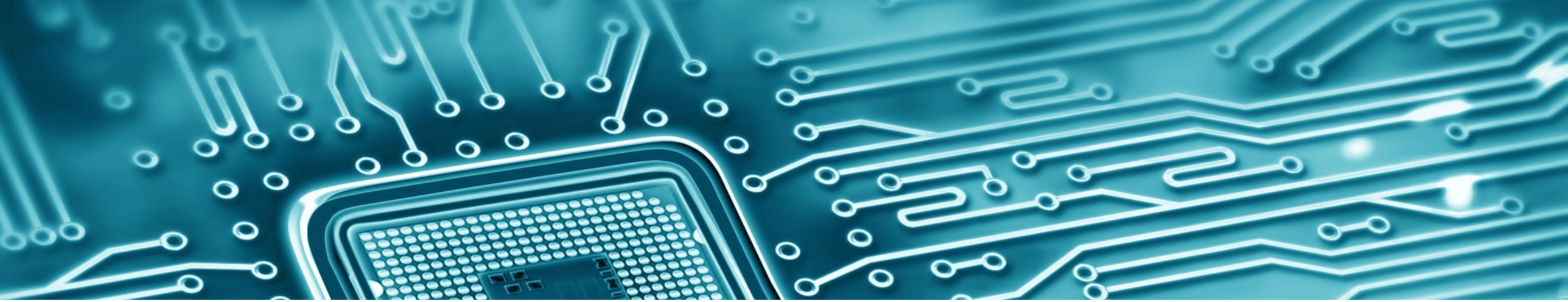
Summary :

- Integrated Circuit Reverse-Engineering
  - Equipments
  - Delayering
  - Imagery
  - Netlist Reconstruction
- Working With The Model
  - Netlist Navigation
  - Simulating Functional Blocs
- Reverse-Engineering Based Attacks
  - Clk Glitch From The Inside
  - Impact on Semi-Invasive Attacks
- Integrated Circuit Security Evaluation
- Integrated Circuit Reverse-Engineering Applications

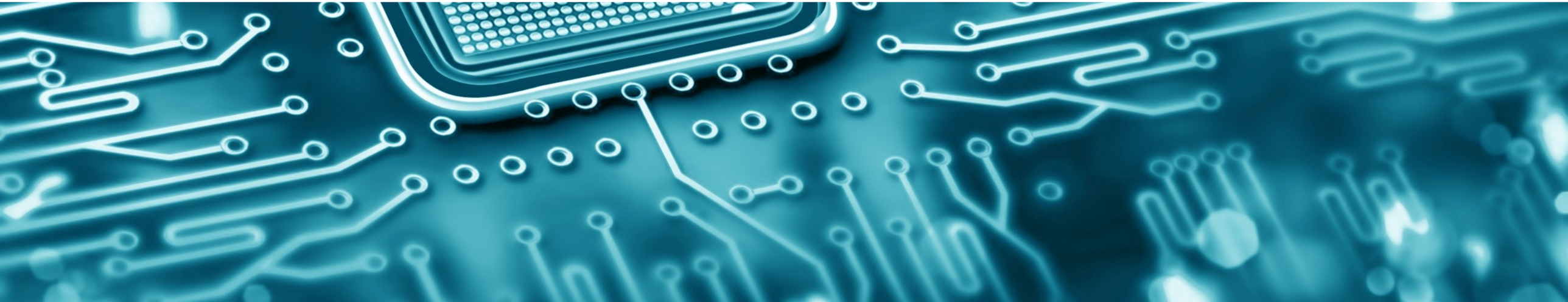


# INTEGRATED CIRCUIT REVERSE-ENGINEERING





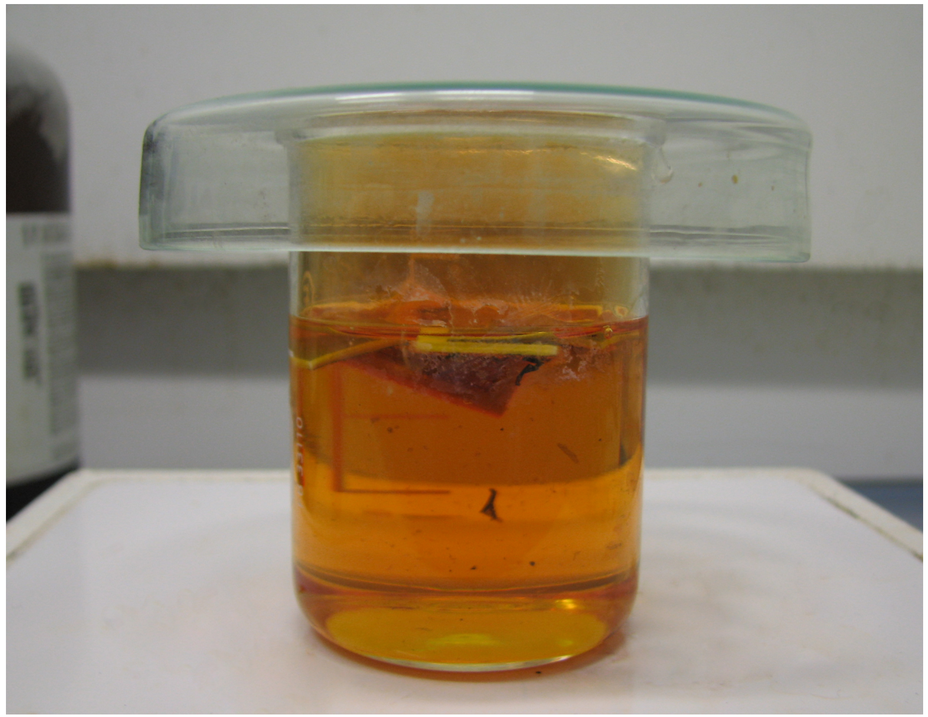
# EQUIPMENTS



# Equipments

## Wet Chemicals

- $HNO_3$ dissolves plastic and epoxy. It can be used in conjunction with other chemicals to remove metal.
- HF dissolves glass
- TMAH is good for bulk removal.



*Smart card modules in $HNO_3$ bath*

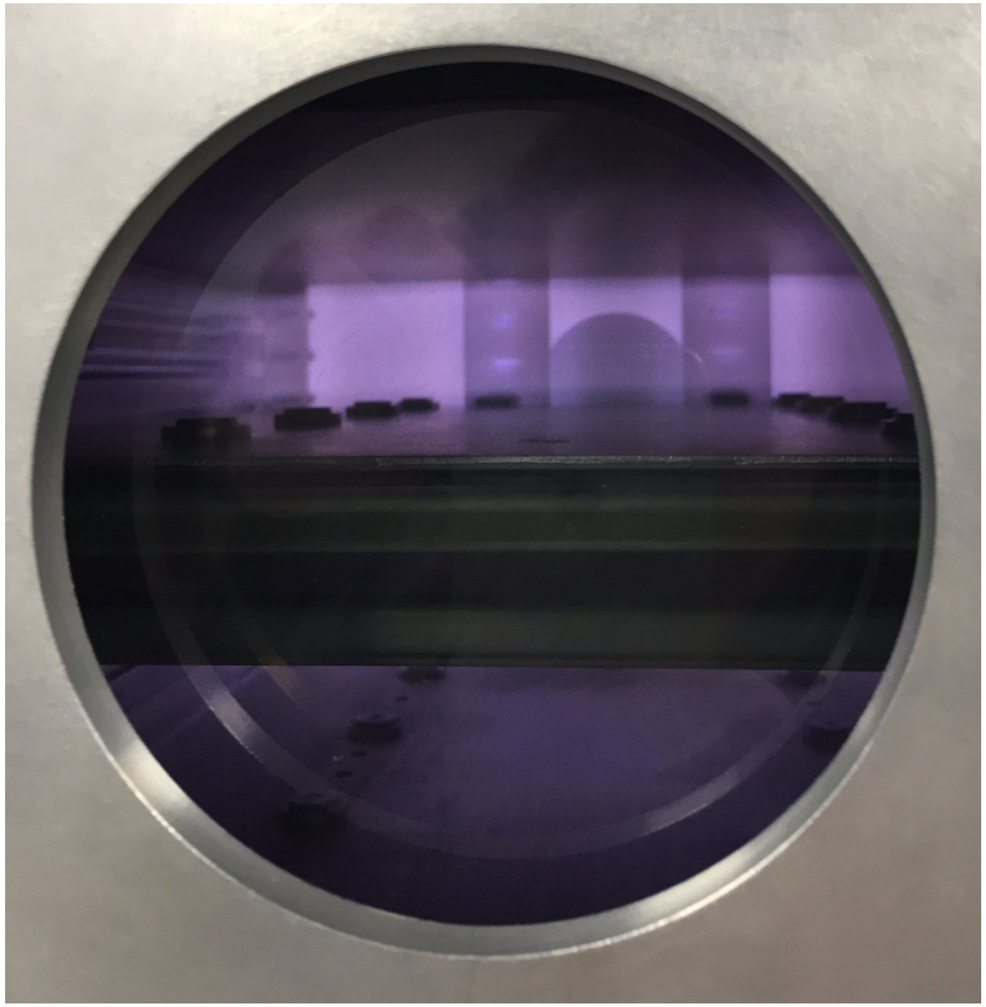

*Ultrasonic bath*

*Drying the isopropanol*

# Delayering / Deprocessing

## Dry Chemicals

- Also called Reactive Ion Etching
- Selective depending on used gaz
  - Oxide etch
  - Metal etch

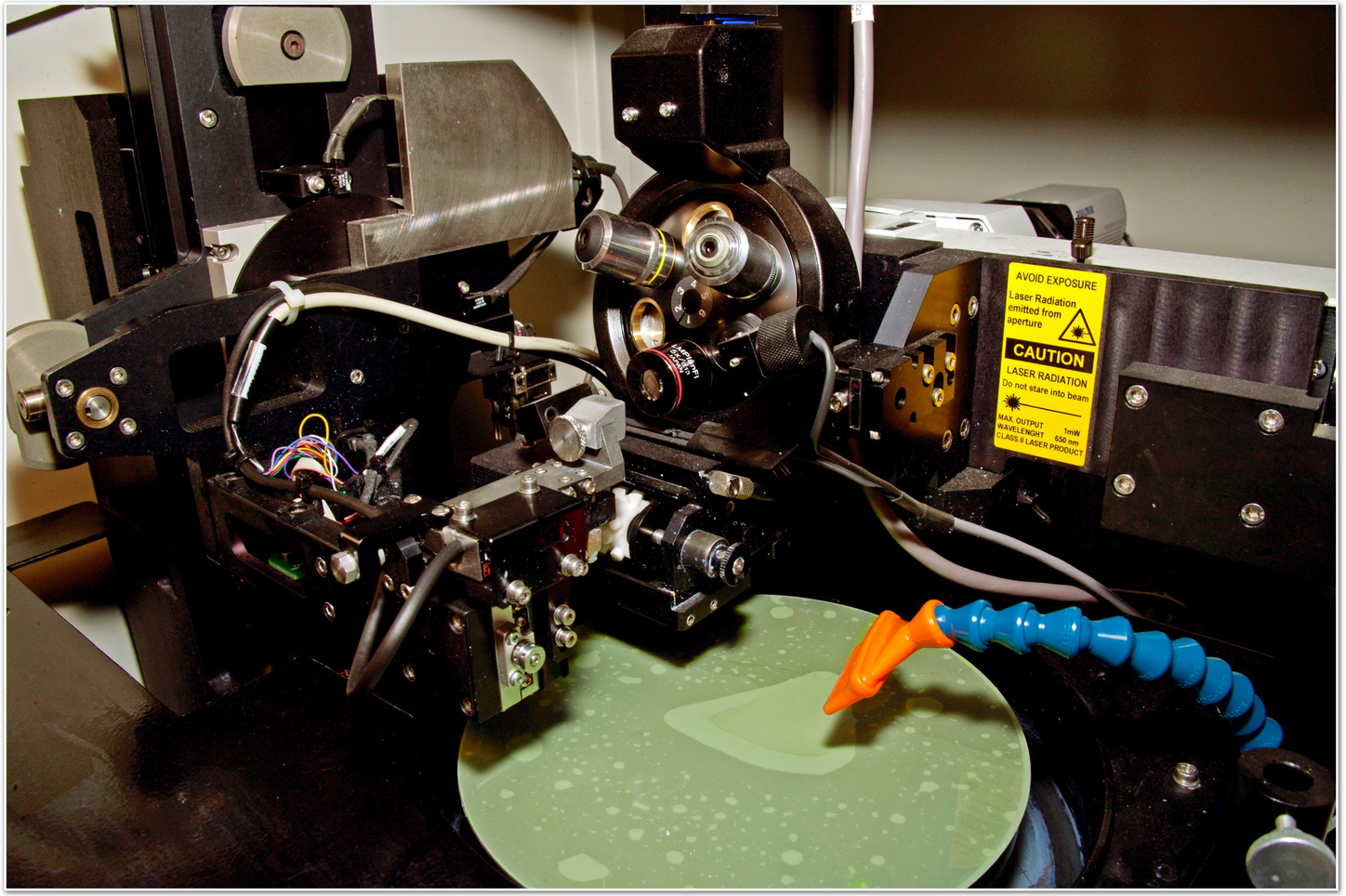


*Plasma*

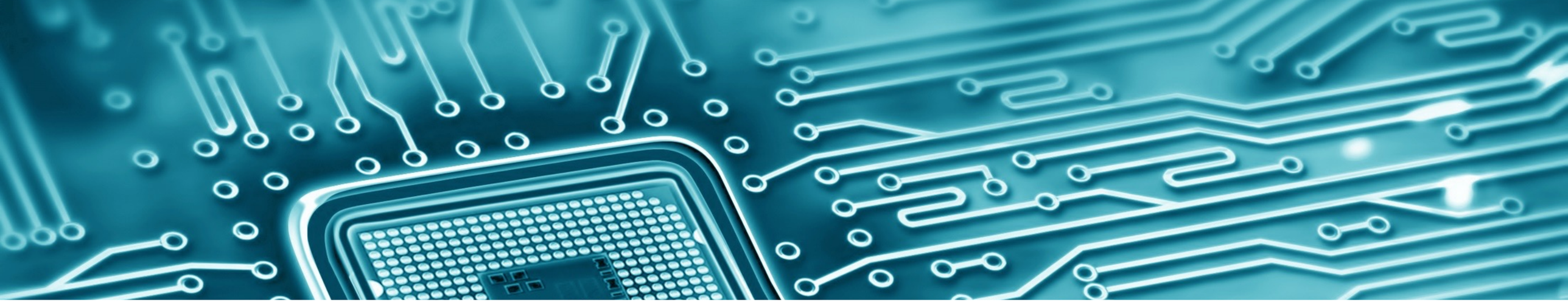
# Delayering / Deprocessing

## (Chemical) Mechanical Polishing

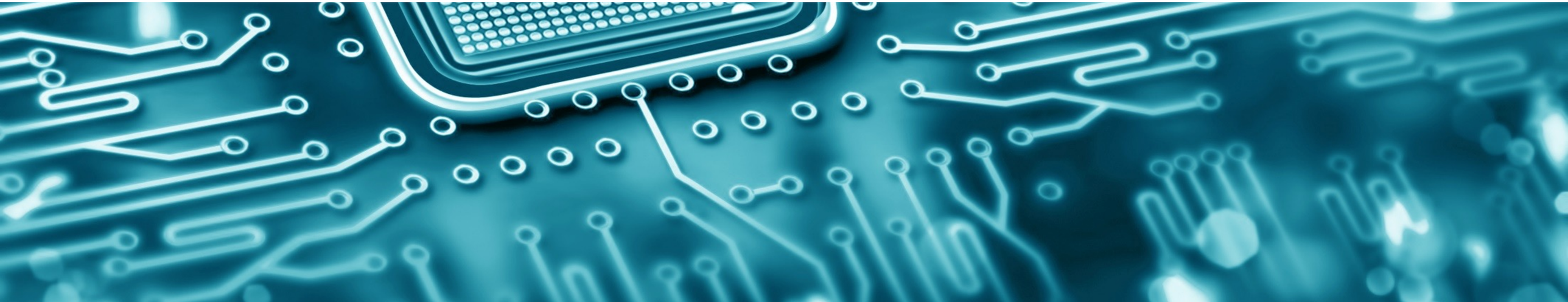
- High-end motorized polisher
- 2 techniques
  - Polishing
  - Lapping




*Polisher*



# DELAYERING / DEPROCESSING

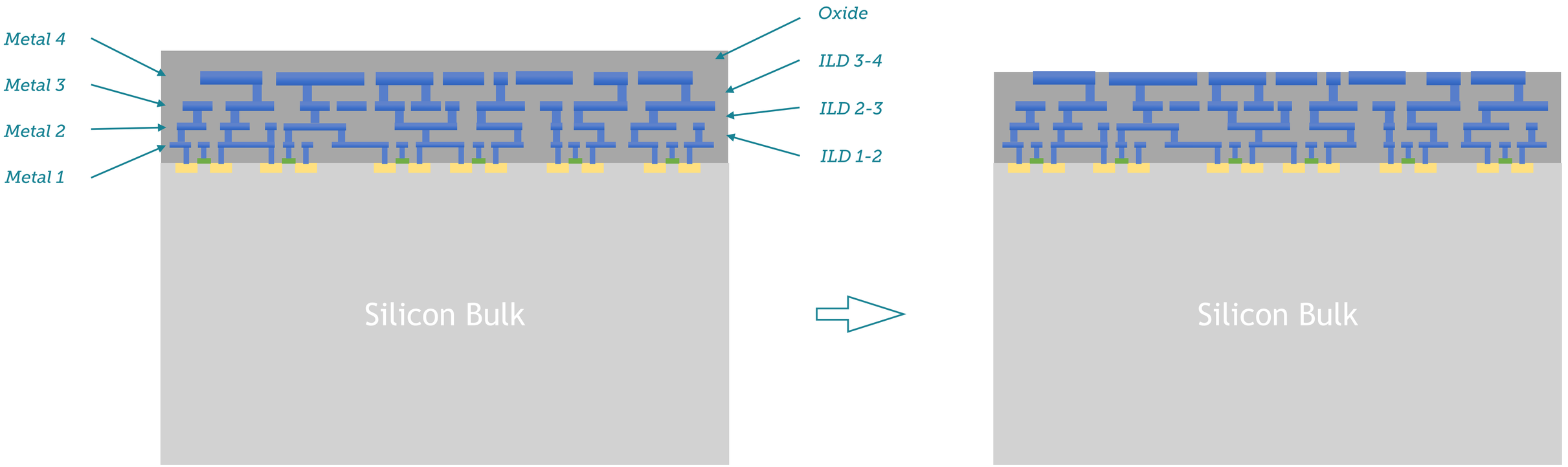


# Delayering / Deprocessing

## Deprocessing : Principle

Simplified process:

- The goal is to be able to image every feature of the chip (metal lines, vias, standard cells…)



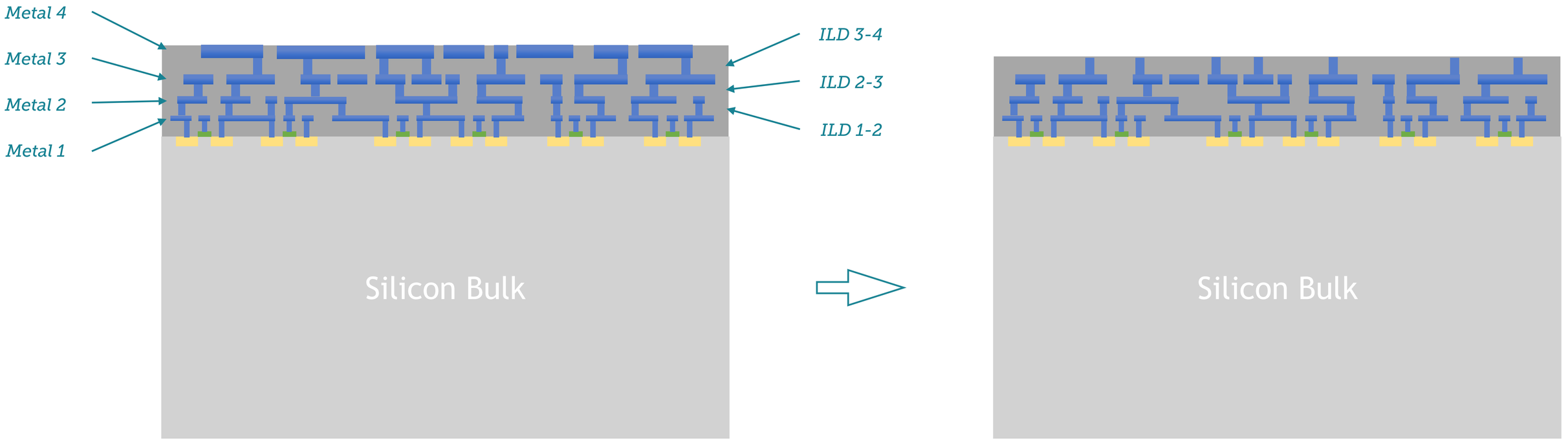

*Integrated Circuit Cross Section*

*Integrated Circuit Cross Section*

# Delayering / Deprocessing

## Deprocessing : Principle

Removing the Metal layer will make ILD 3-4 visible.

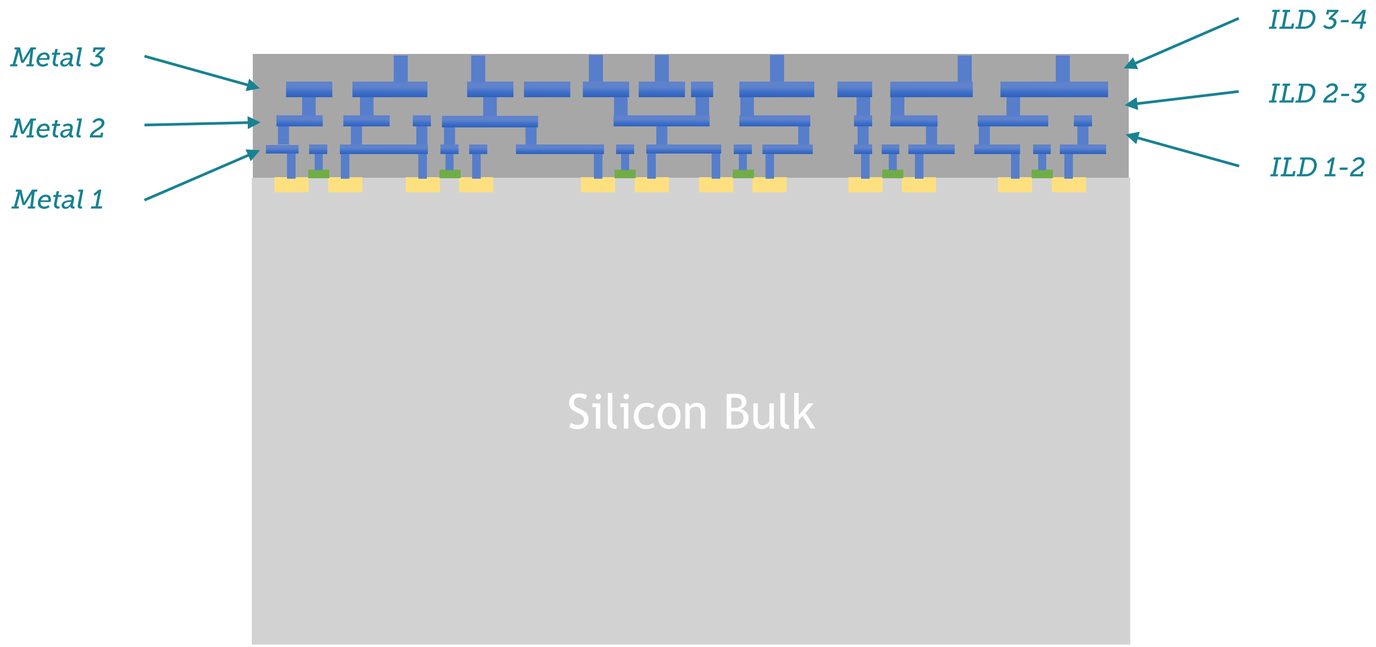



*Integrated Circuit Cross Section*

*Integrated Circuit Cross Section*

## Deprocessing : Principle

From this point, the process will be repeated to get access to all layers.

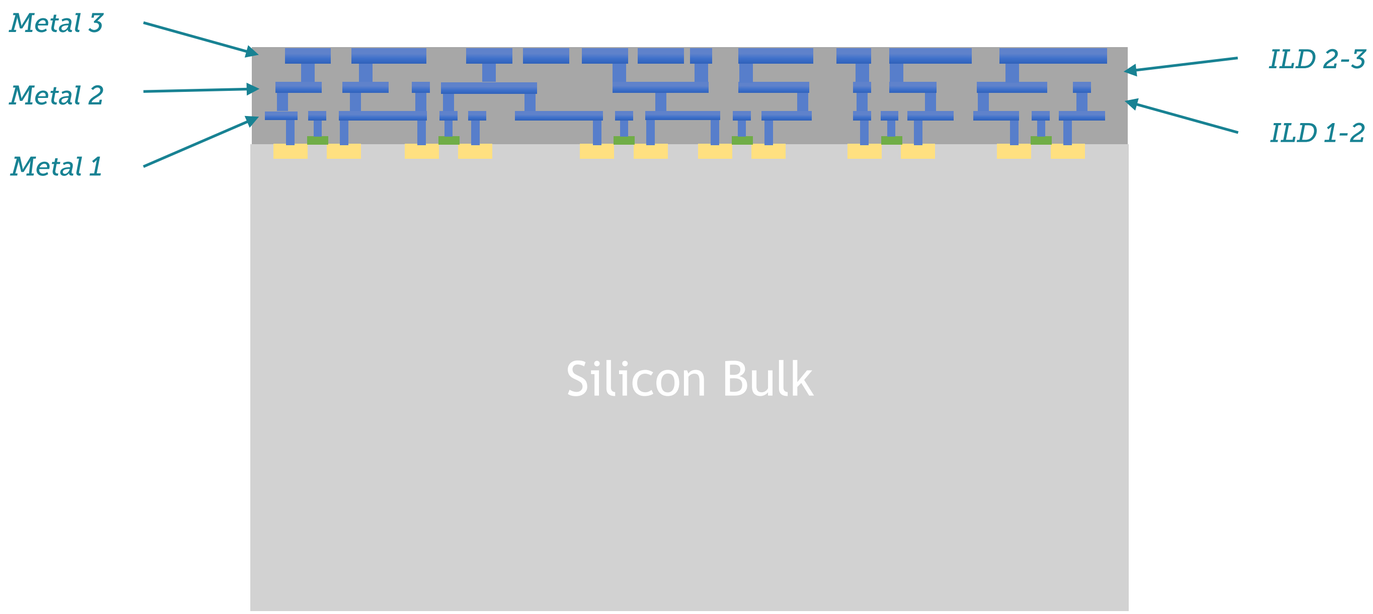



*Integrated Circuit Cross Section*

Texplained

## Deprocessing : Principle

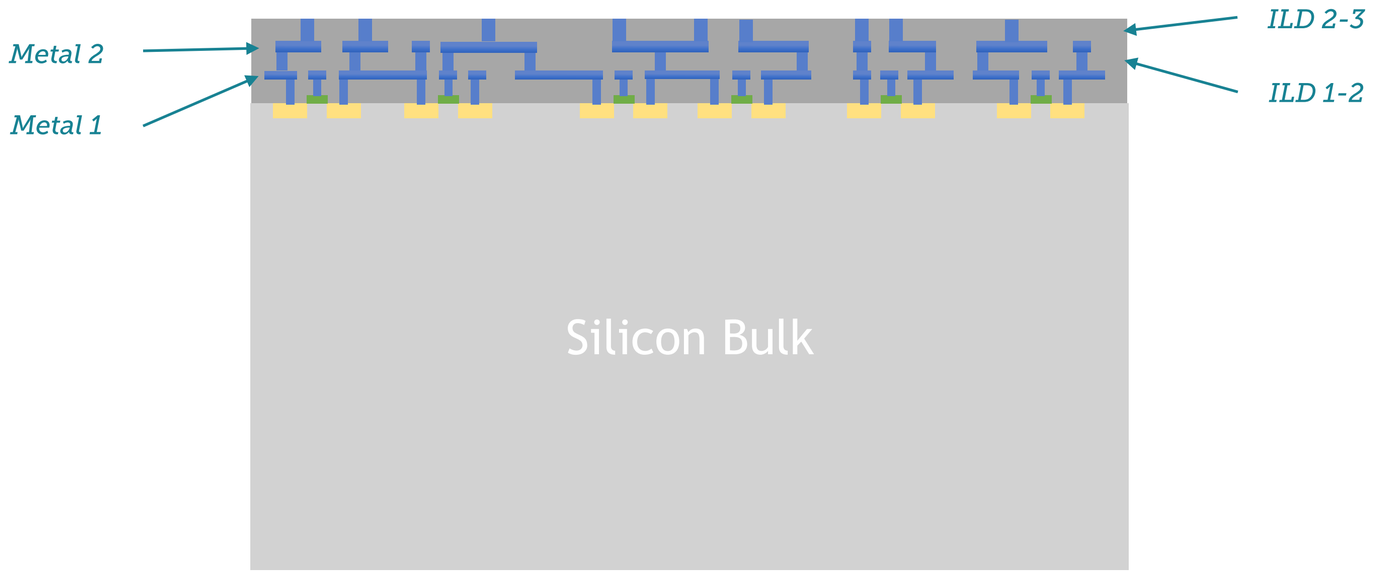
Metal 3 can be imaged.




*Integrated Circuit Cross Section*

## Deprocessing : Principle

ILD 2-3 can be imaged.

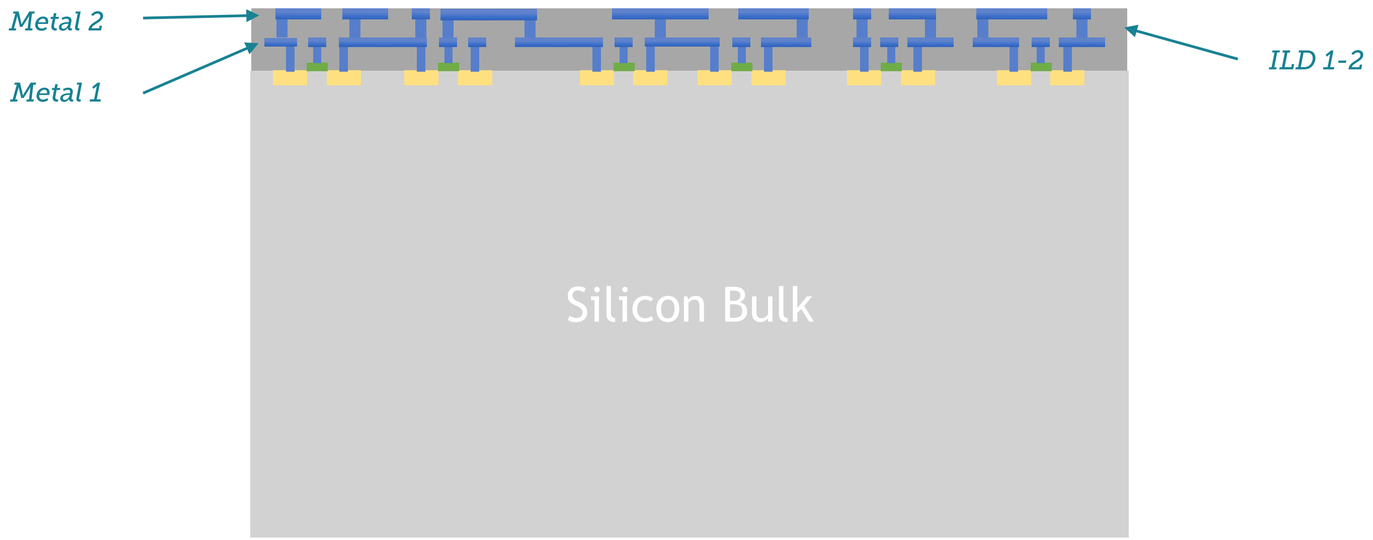



*Integrated Circuit Cross Section*

Texplained

## Deprocessing : Principle

Metal 2 can be imaged.

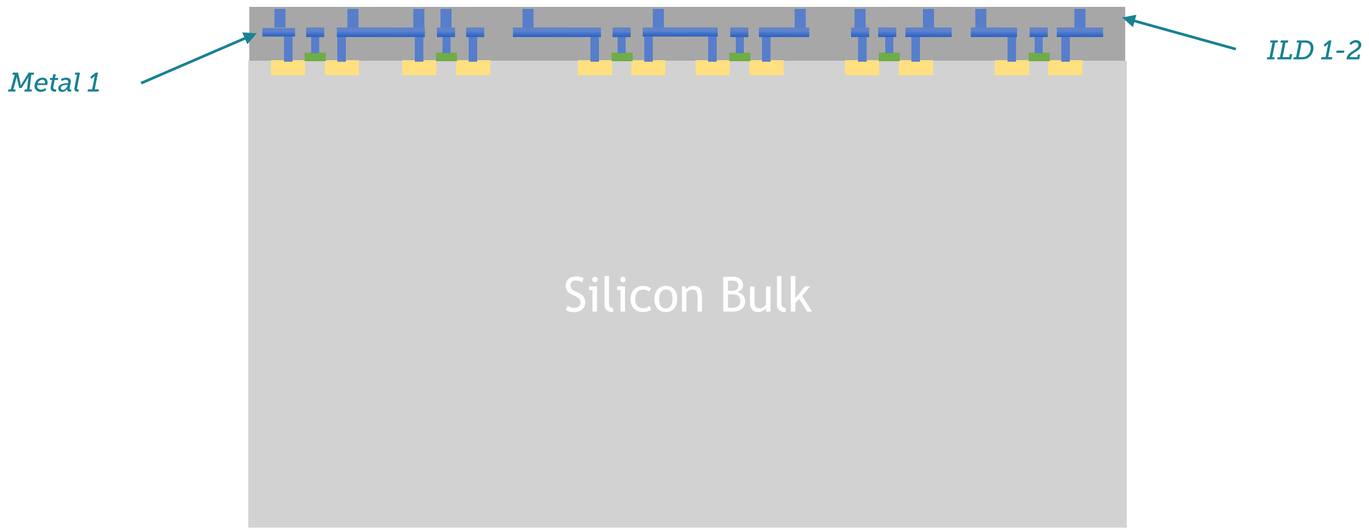



*Integrated Circuit Cross Section*

Texplained

## Deprocessing : Principle

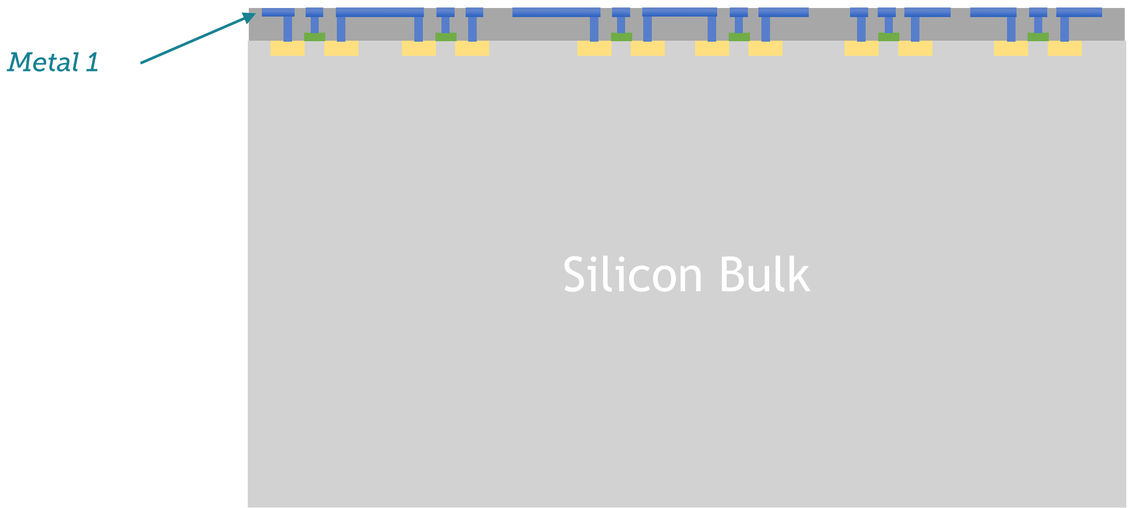
ILD 1-2 can be imaged.




*Integrated Circuit Cross Section*

## Deprocessing : Principle

Metal 1 can be imaged.

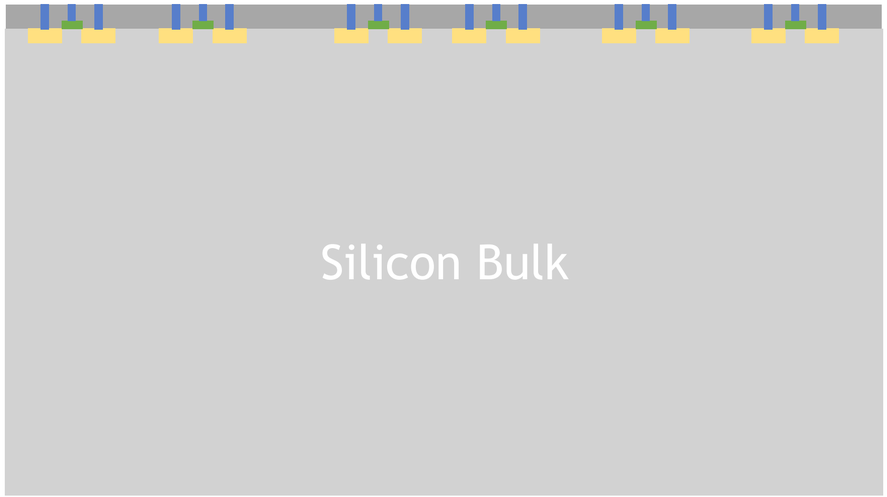



*Integrated Circuit Cross Section*

Texplained

## Deprocessing : Principle

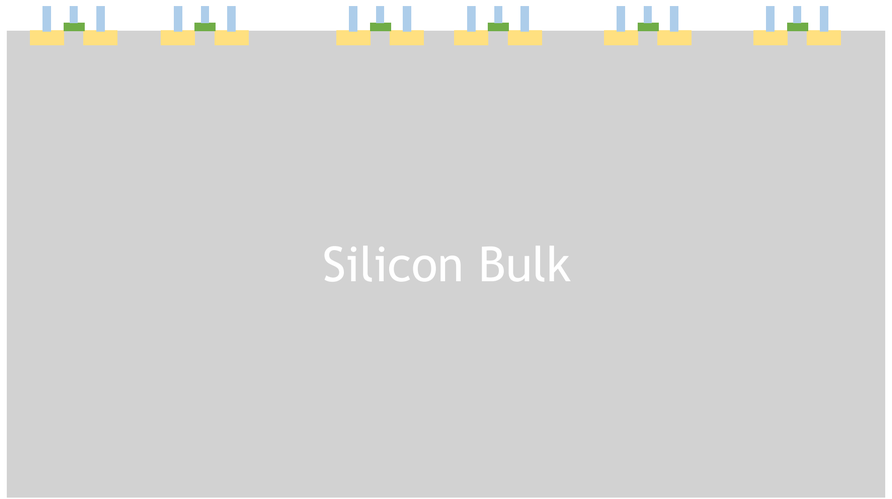
At this stage, Contacts can be imaged.



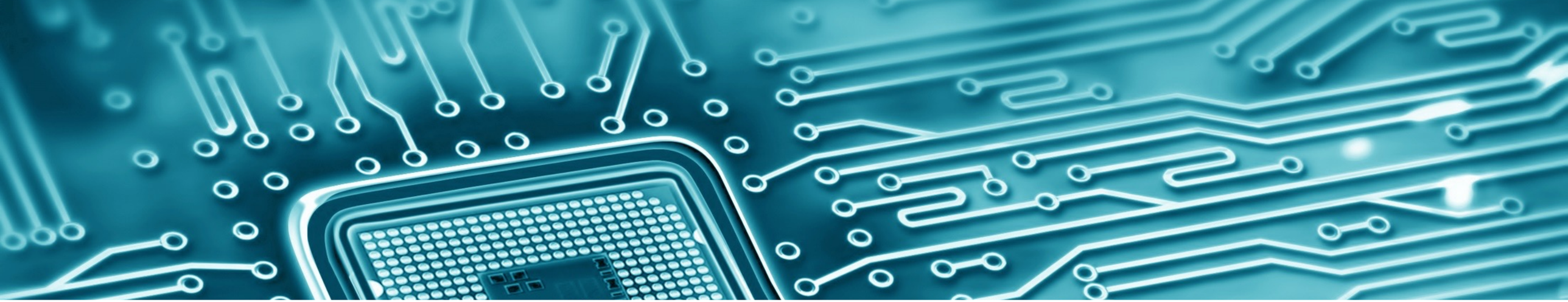

*Integrated Circuit Cross Section*

## Deprocessing : Principle

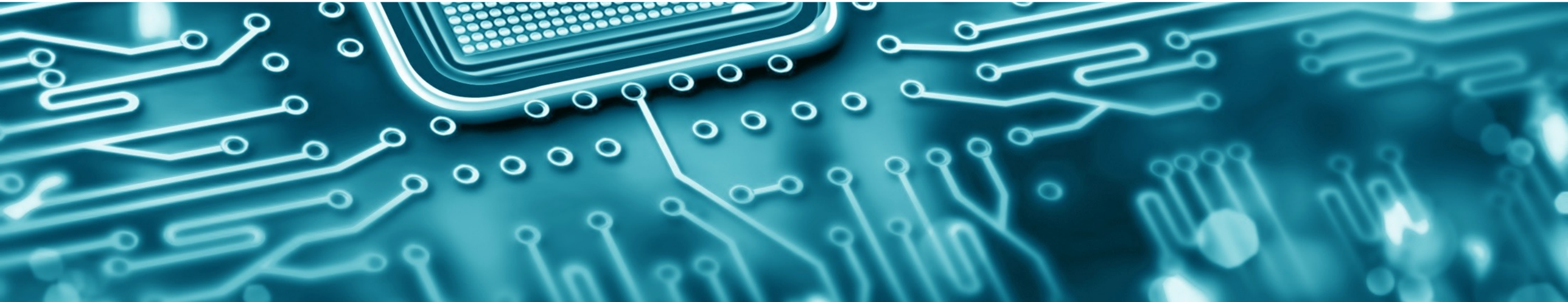
Last step of the deprocessing is made for making contacts, polysilicon gate and active area visible.




*Integrated Circuit Cross Section*



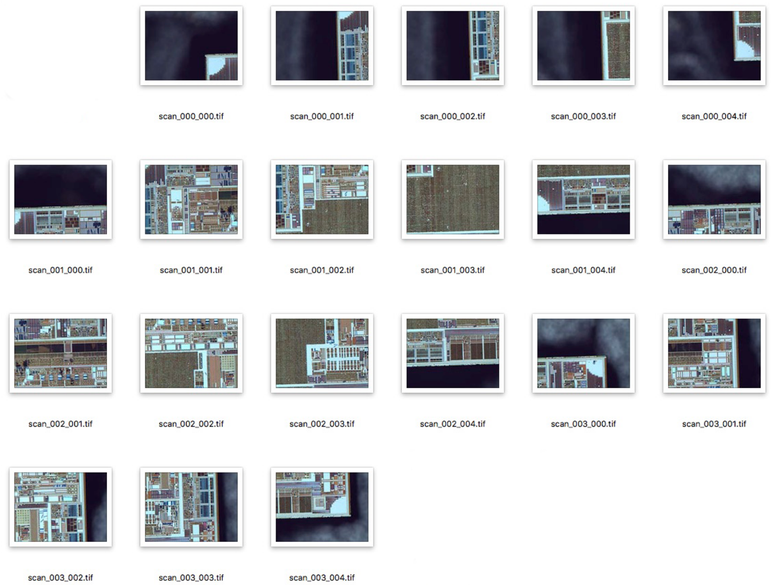
# IMAGERY

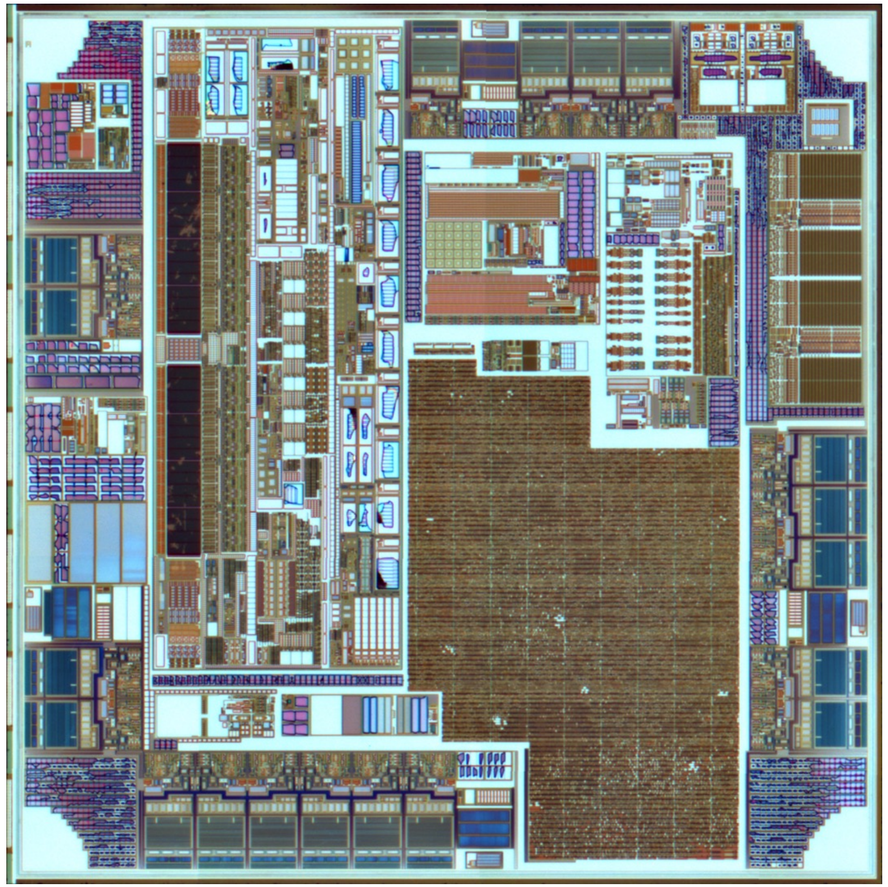


Texplained

## Optical Imagery

- Usable on older technology nodes (>130nm)
- Fast overview creation

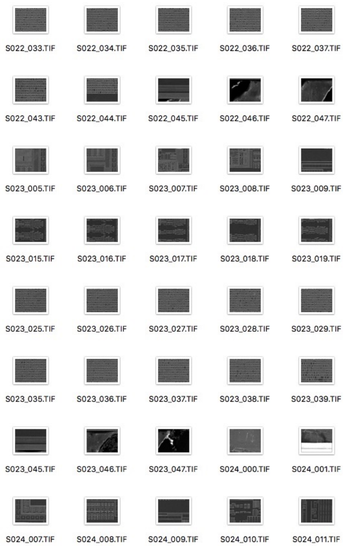


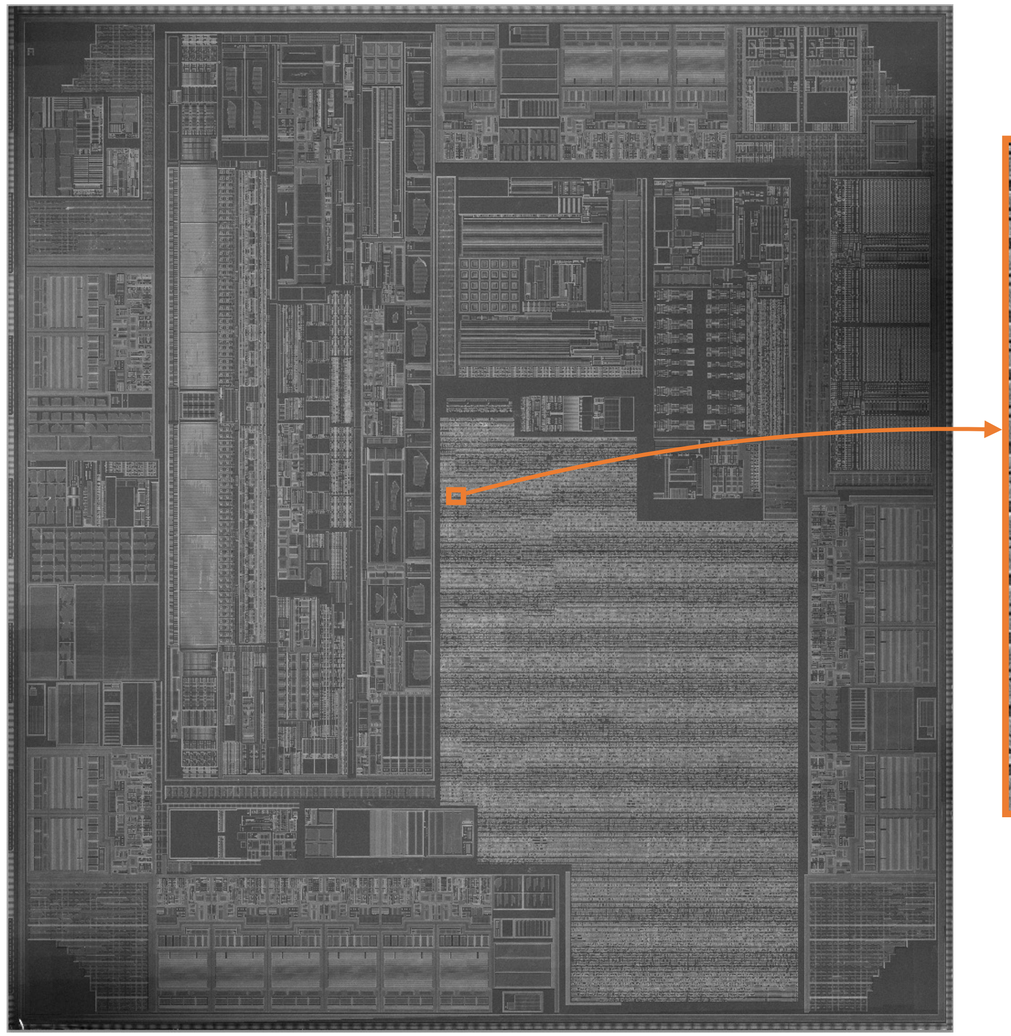



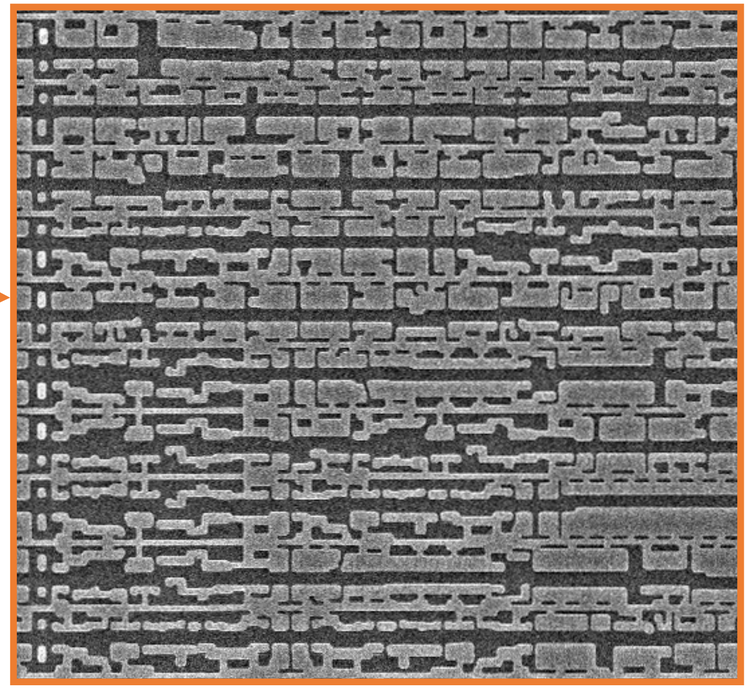
# Imagery

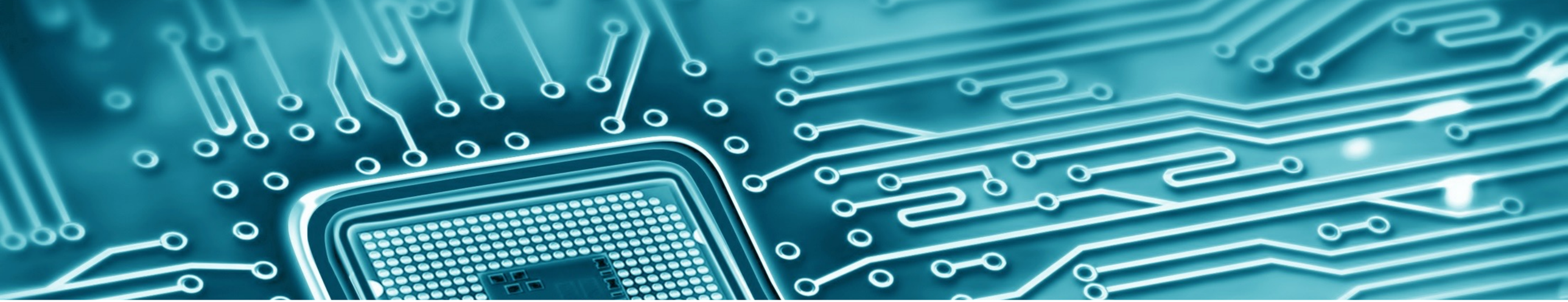
## SEM (Scanning Electron Microscope) Imagery

- Enough resolution to work on the smallest nodes.

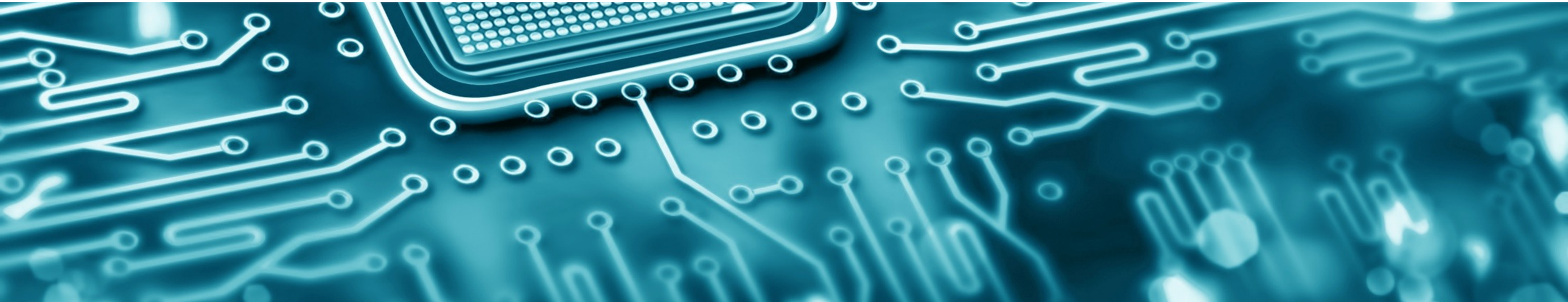






# NETLIST RECONSTRUCTION



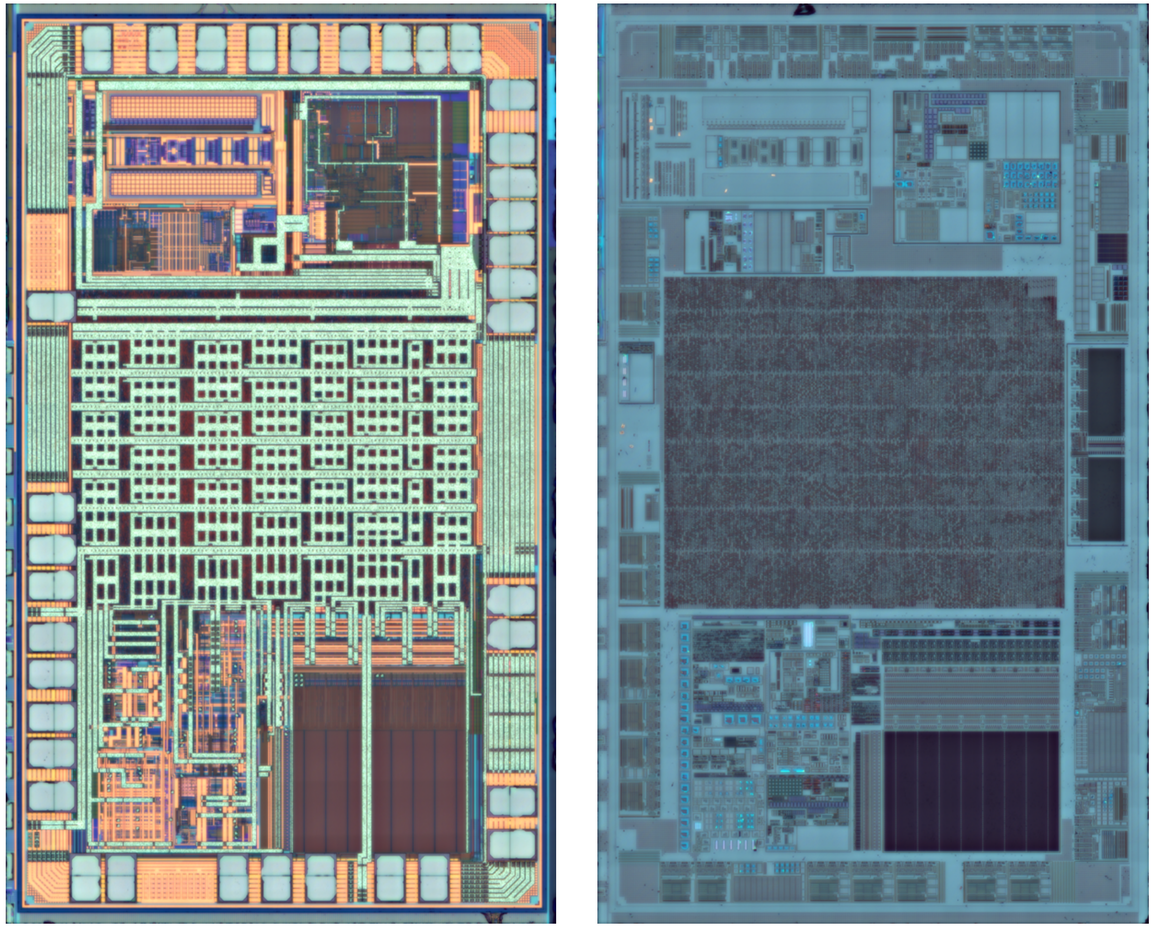
# Netlist Reconstruction

Texplained

## Example

- From SEM pictures, an HDL model of the digital circuit can be created.

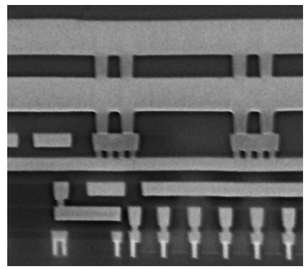

*Imported Layers into ChipJuice*



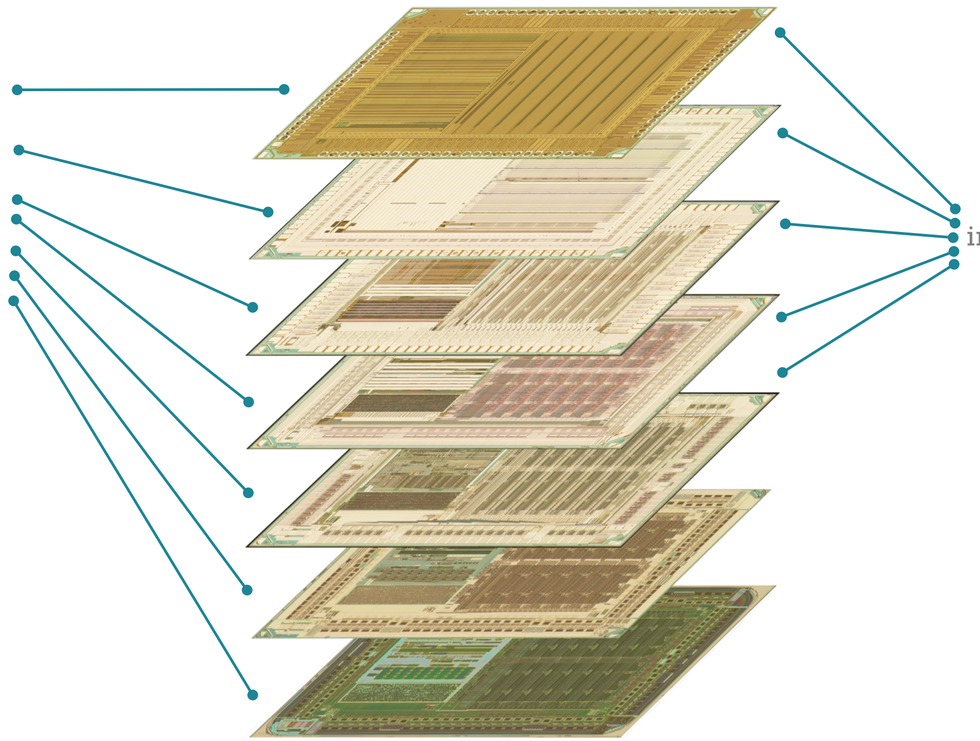
*Top & Substrate Optical Overviews*

# Netlist Reconstruction

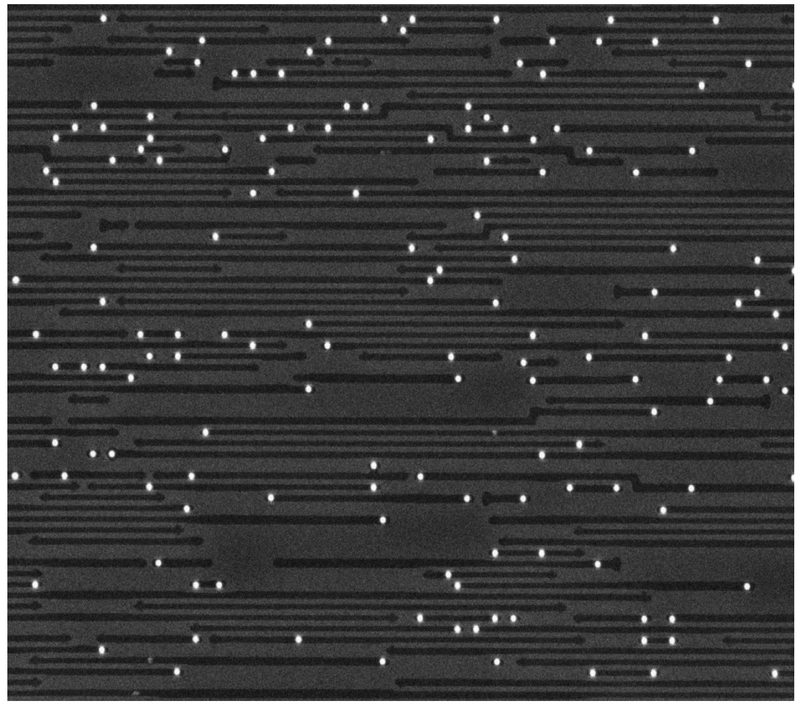
## Interconnect Layers



*SEM (Scanning Electron Microscope) cross-section of an IC (Integrated Circuit)*

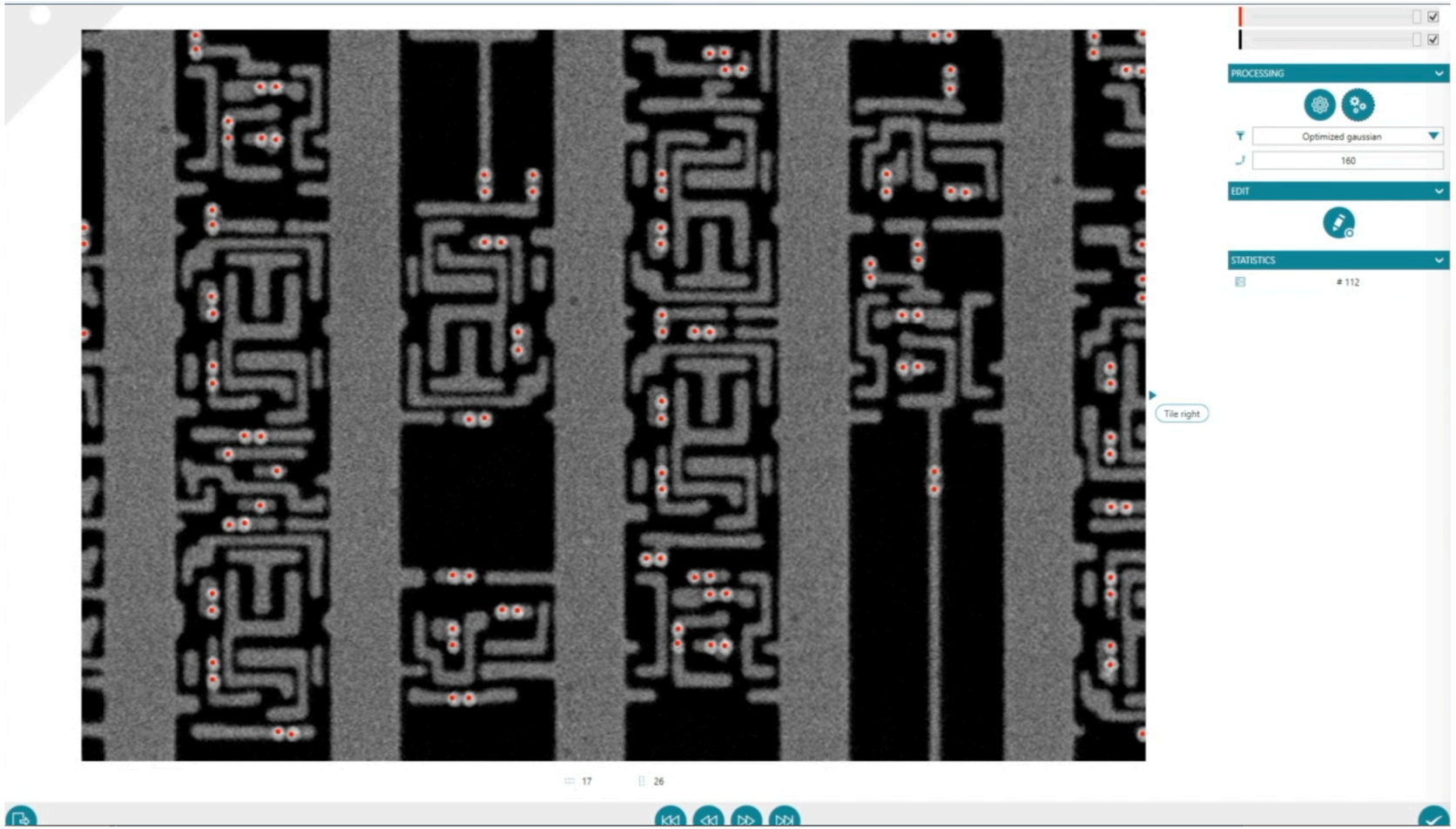



*Optical scans of each metal layer.*



*Close-up of an interconnect layer:*
*Horizontal interconnect : metal tracks*
*Vertical interconnect : vias*

## Vias Extraction




*ChipJuice Screen Capture - Vias Extraction*

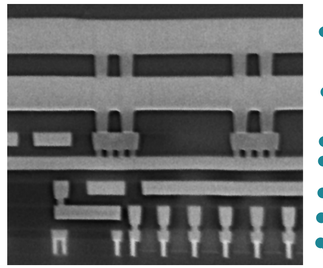
# Netlist Reconstruction

## Tracks Extraction

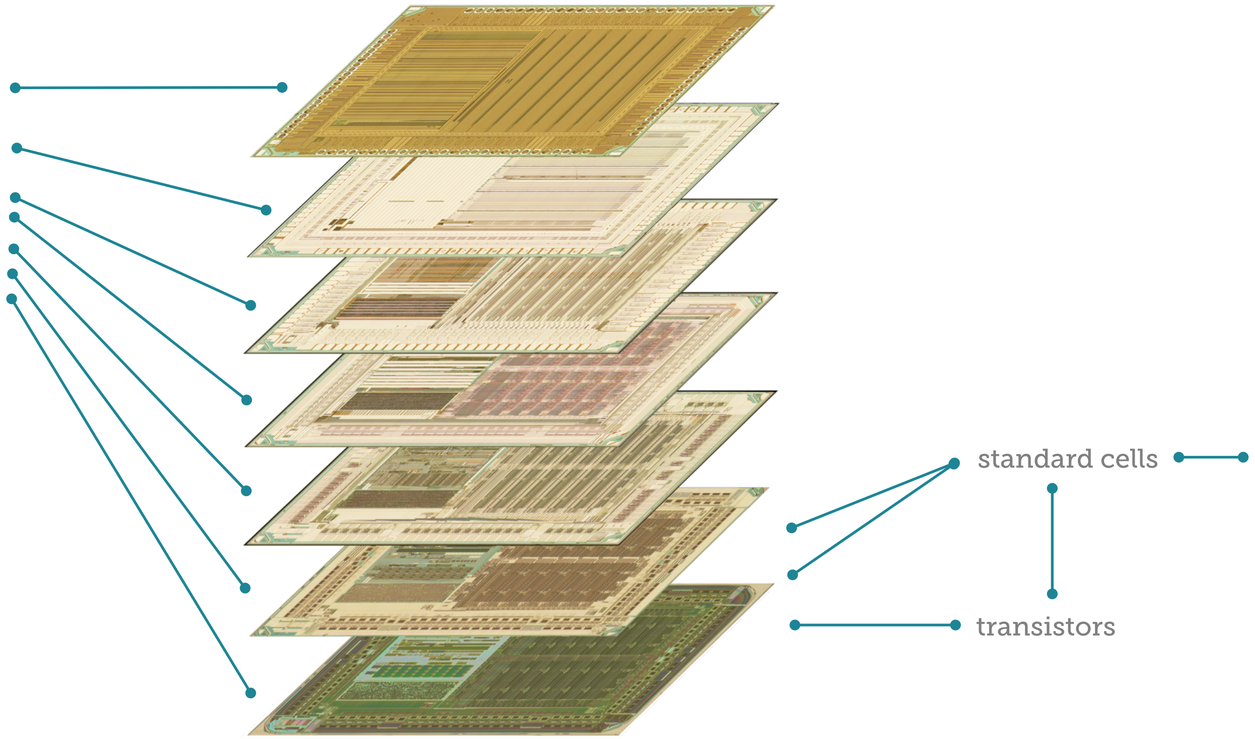

*ChipJuice Screen Capture - Tracks Extraction*

# Netlist Reconstruction

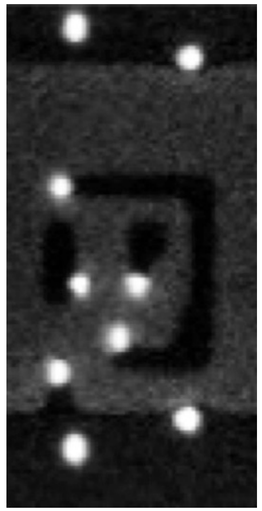
## Standard Cell Library Reconstruction



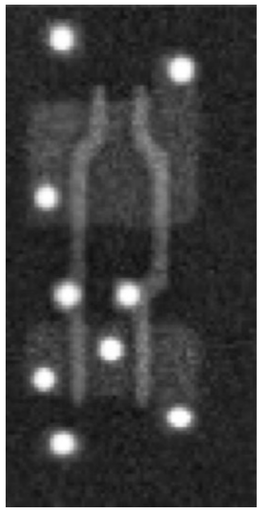
*SEM (Scanning Electron Microscope) cross-section of an IC (Integrated Circuit)*




*Optical scans of each metal layer.*



*Metal 1*



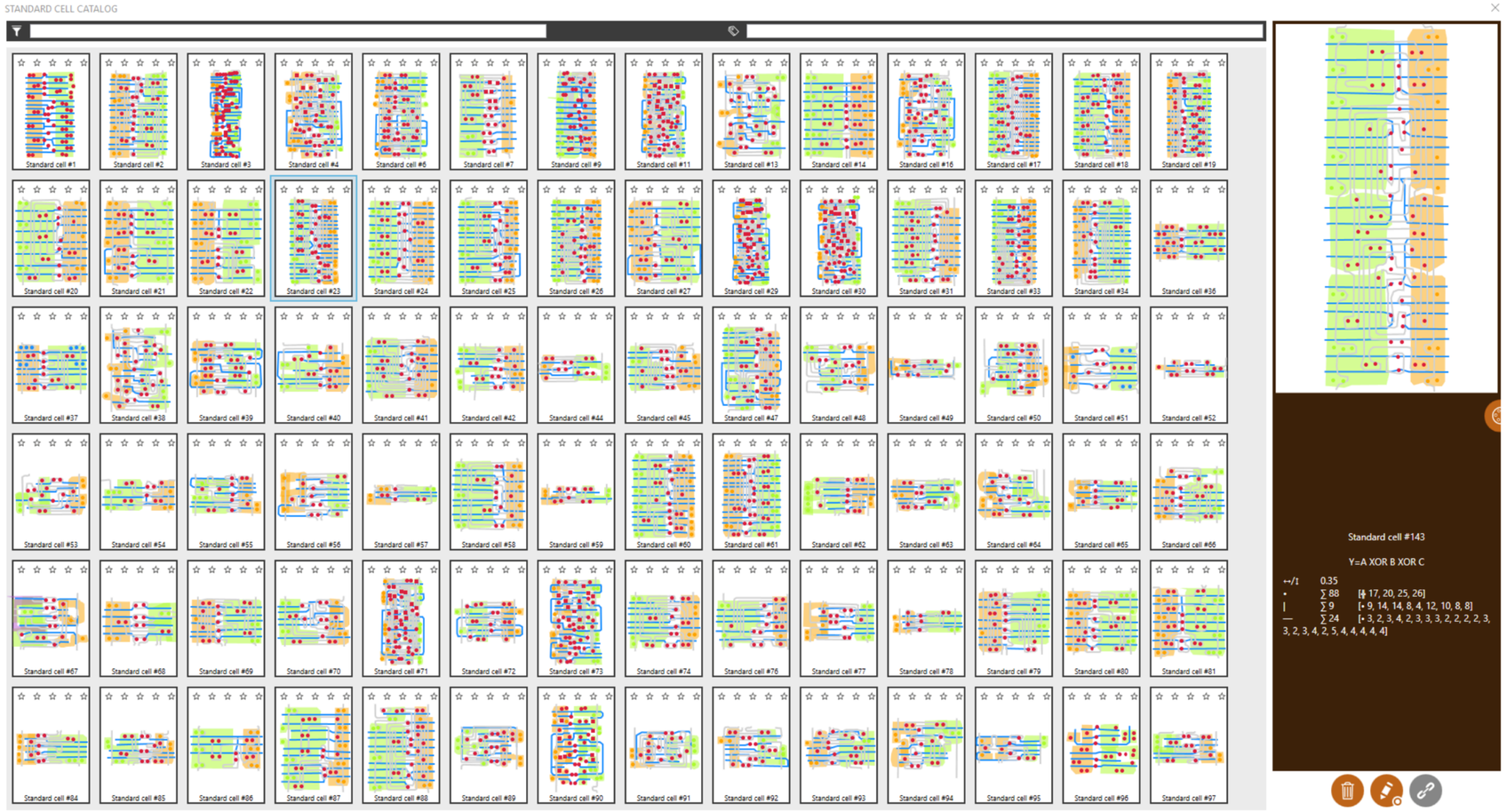
*Poly / diffusion*

*4 transistors forming a NOR standard cell.*
*Output = not (InputA or InputB)*

Texplained

## Standard Cell Library Reconstruction

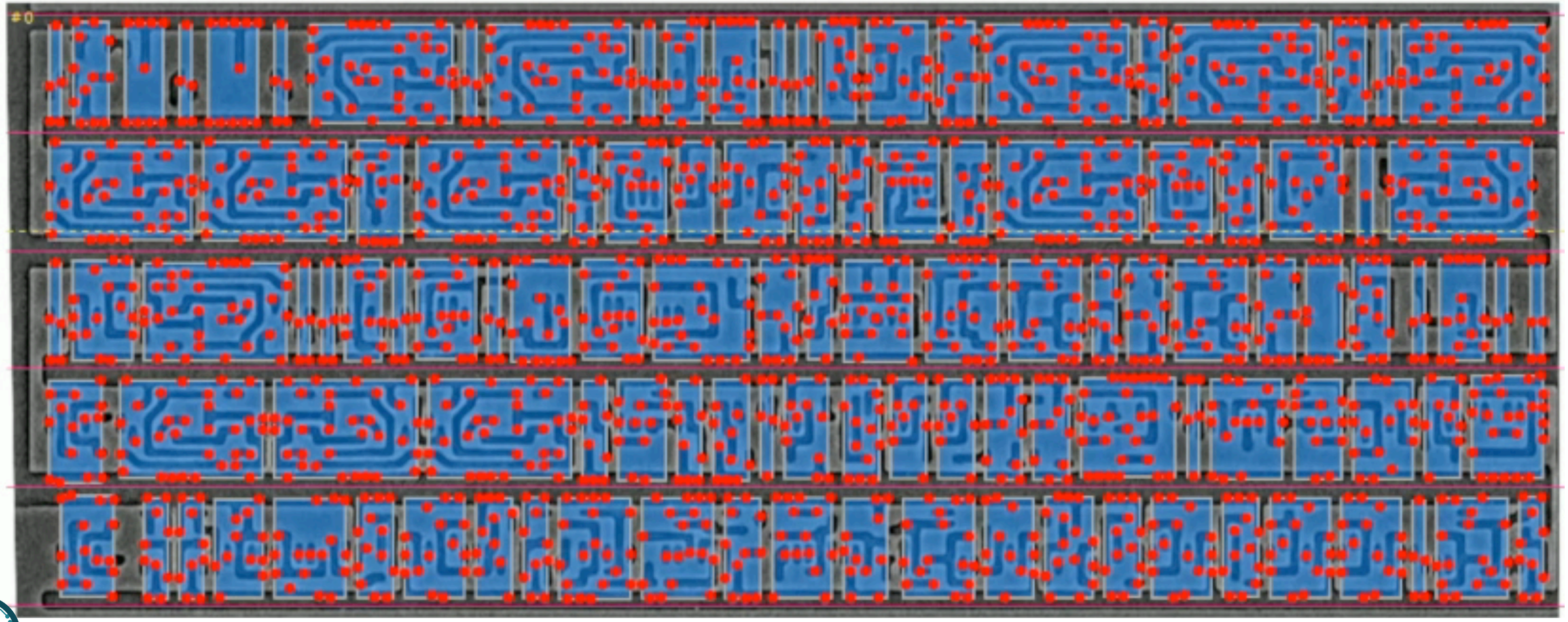
- The SCL catalog can be re-used on ICs that would use the same fabrication process.




*ChipJuice Screen Capture - SCL Catalog*

# Netlist Reconstruction

## Standard Cell Library Instances Detection



*ChipJuice Screen Capture - SCL Instances Extraction*

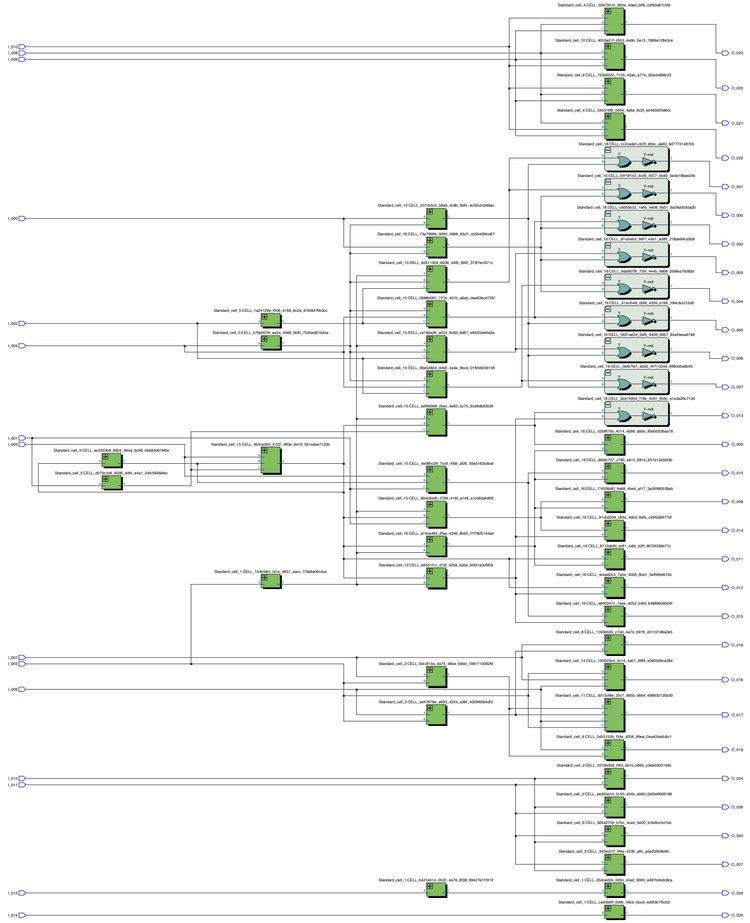
# Netlist Reconstruction

## Conversion of Extracted Features to HDL Netlist

```
architecture structure of netlist is

component Standard_cell_16
port  (A: in std_logic;
       B: in std_logic;
       Y: out std_logic);
end component;
component Standard_cell_15
port  (A: in std_logic;
       B: in std_logic;
       C: in std_logic;
       Y: out std_logic);
end component;
component Standard_cell_12
port  (A: in std_logic;
       B: in std_logic;
       Y: out std_logic);
end component;
component Standard_cell_1
port  (A: in std_logic;
       Y: out std_logic);
end component;
component Standard_cell_5
port  (A: in std_logic;
       Y: out std_logic);
end component;
component Standard_cell_2
port  (A: in std_logic;
       B: in std_logic;
       Y: out std_logic);
end component;
component Standard_cell_14
port  (A: in std_logic;
       B: in std_logic;
       C: in std_logic;
       Y: out std_logic);
end component;
component Standard_cell_11
port  (A: in std_logic;
       B: in std_logic;
       C: in std_logic;
       D: in std_logic;
       Y: out std_logic);
end component;
component Standard_cell_8
port  (A: in std_logic;
       B: in std_logic;
       Y: out std_logic);
end component;
component Standard_cell_10
port  (A: in std_logic;
       B: in std_logic;
       C: in std_logic;
       Y: out std_logic);
end component;
component Standard_cell_9
port  (A: in std_logic;
       B: in std_logic;
       C: in std_logic;
       Y: out std_logic);
end component;
```

*Netlist VHDL export*

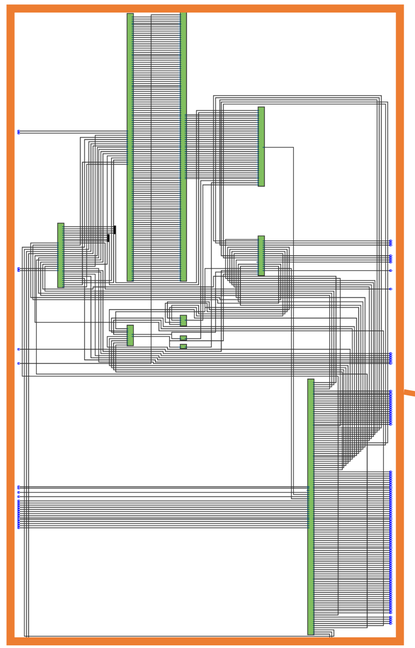


*Netlist View of recovered circuitry (quartus)*

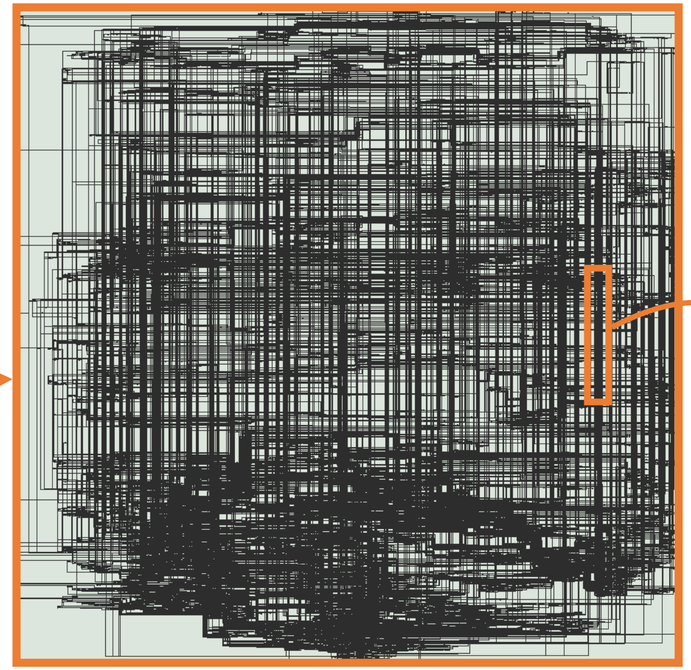
# Netlist Reconstruction

## Toward Hierarchical Netlist

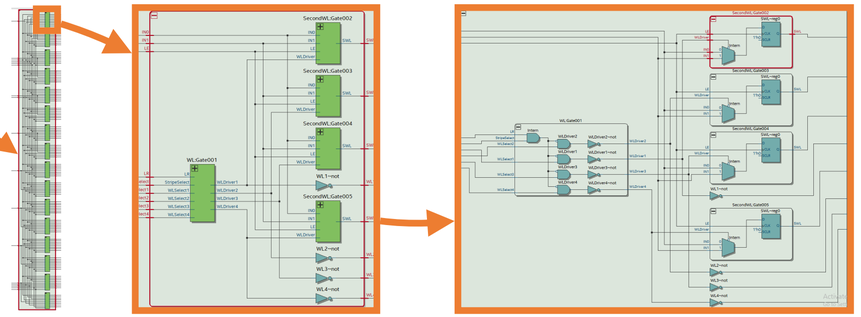
- Being able to extract a netlist of any IC is just a start. On top of cross-referencing IC pictures to IC schematic, netlist hierarchization is (optional - application dependent) the next analysis phase.
- This makes it possible to quickly find the function of interest and to perform the given study (from risk assessment to backdoor research and IP theft, etc).
- Those hierarchical information can be re-used on different targets.



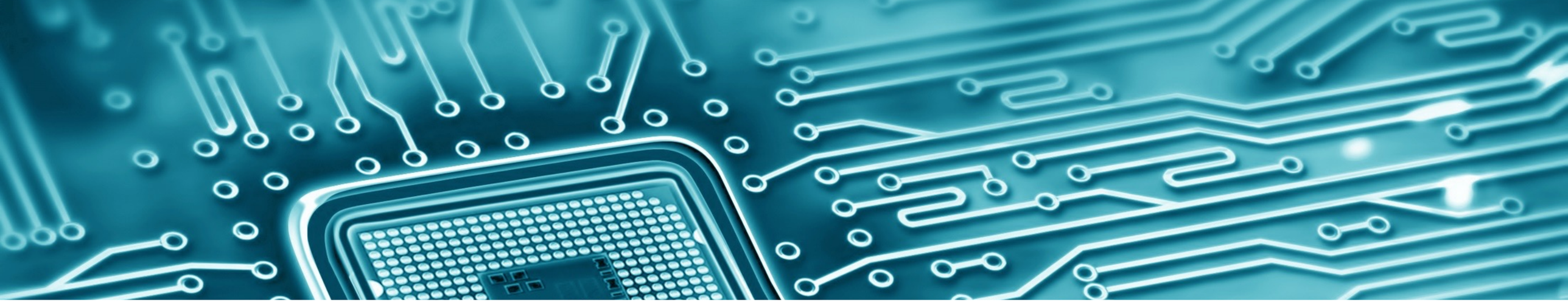
*Chip Bloc View*



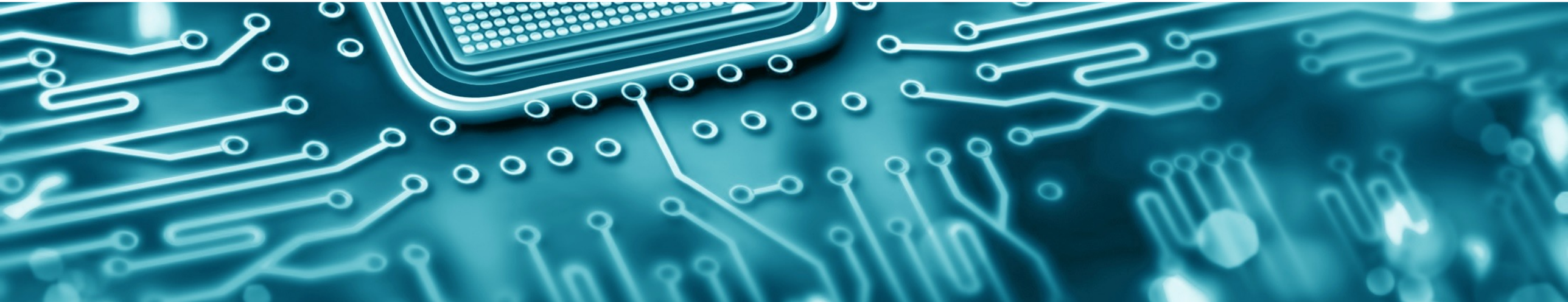
*State Machine Netlist Graph*

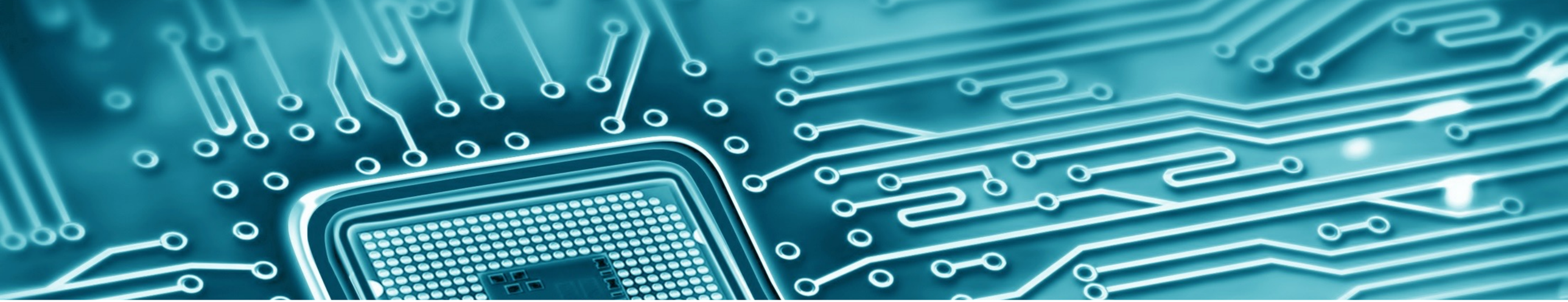


*Addressing logic (3 levels of details)*

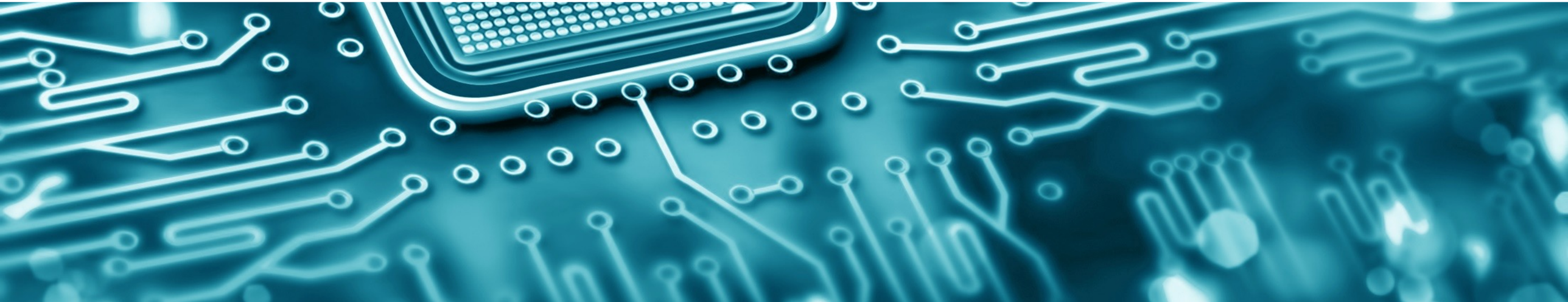


# WORKING WITH THE MODEL





# NETLIST NAVIGATION

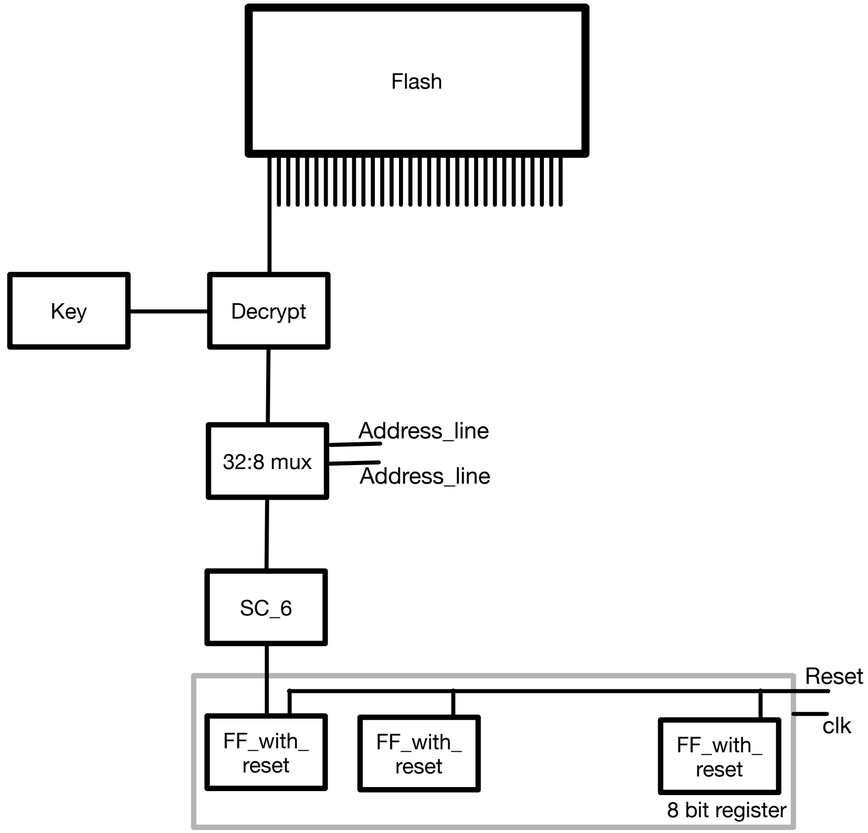


# Netlist navigation

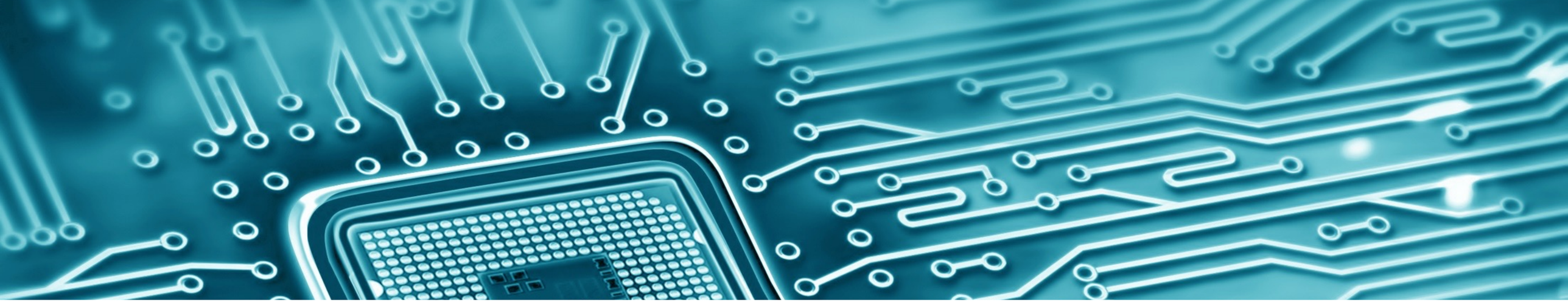
## Invasive Attack Usage

- Tracing signals inside a schematic
- Functional bloc discovery and hierarchization

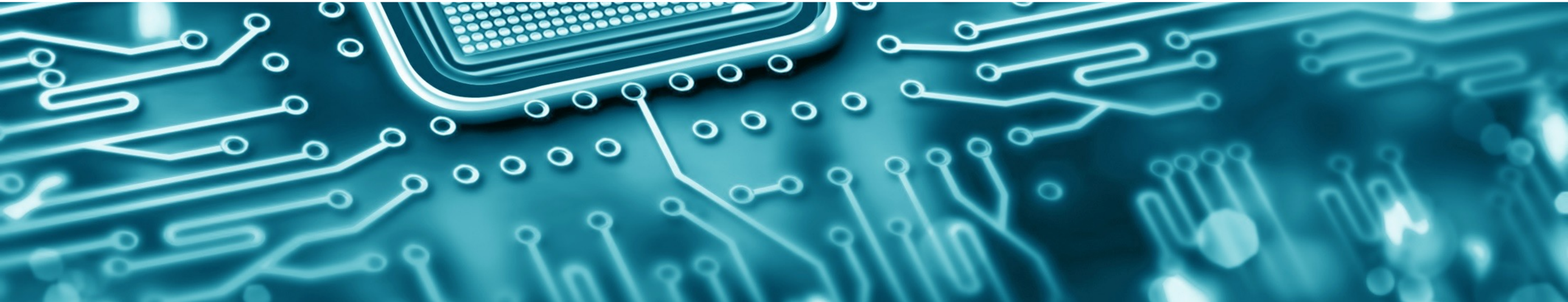
TRACING DEMO




*Flash bus schematic*



# SIMULATING FUNCTIONAL BLOCS

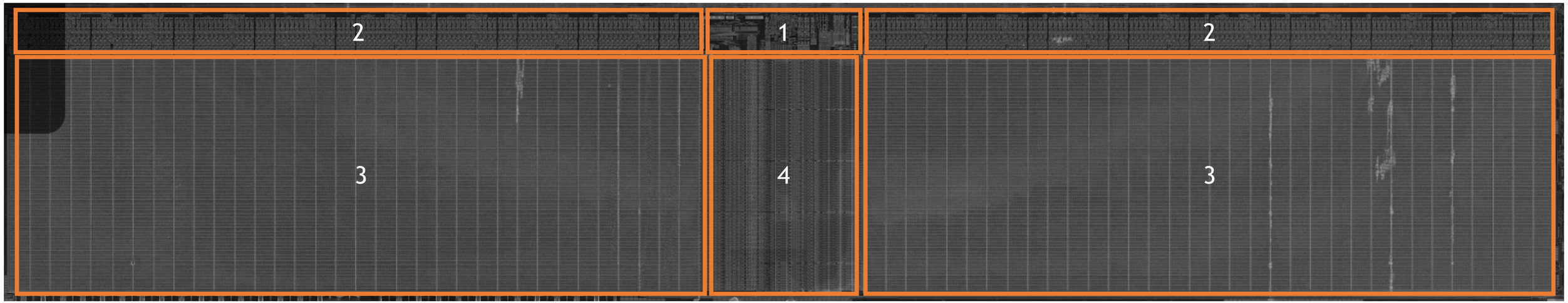


# Simulating Functional Blocs

## Scrambled & Encrypted NVMs

- Encrypted ROMs
- Scrambled Word Lines
- Scrambled Bit Lines

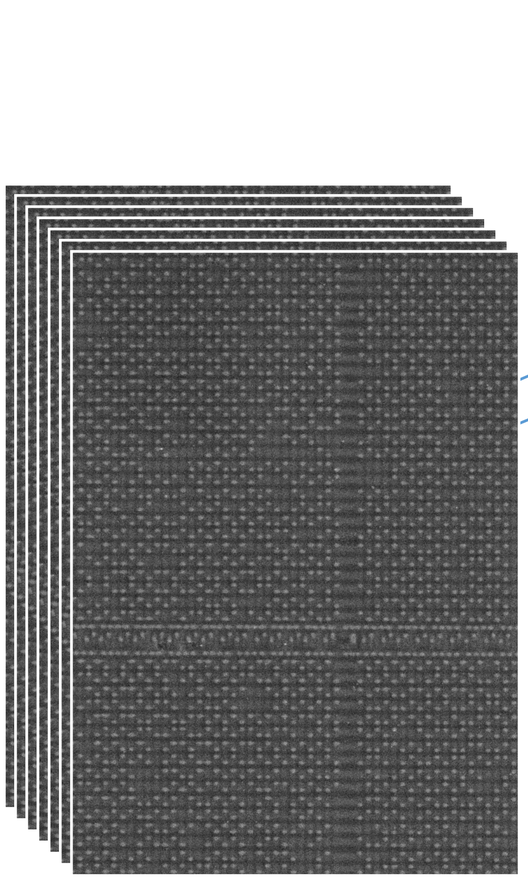
- 1. Control Logic
- 2. Output Buffers
- 3. Bit arrays
- 4. Address Decoder



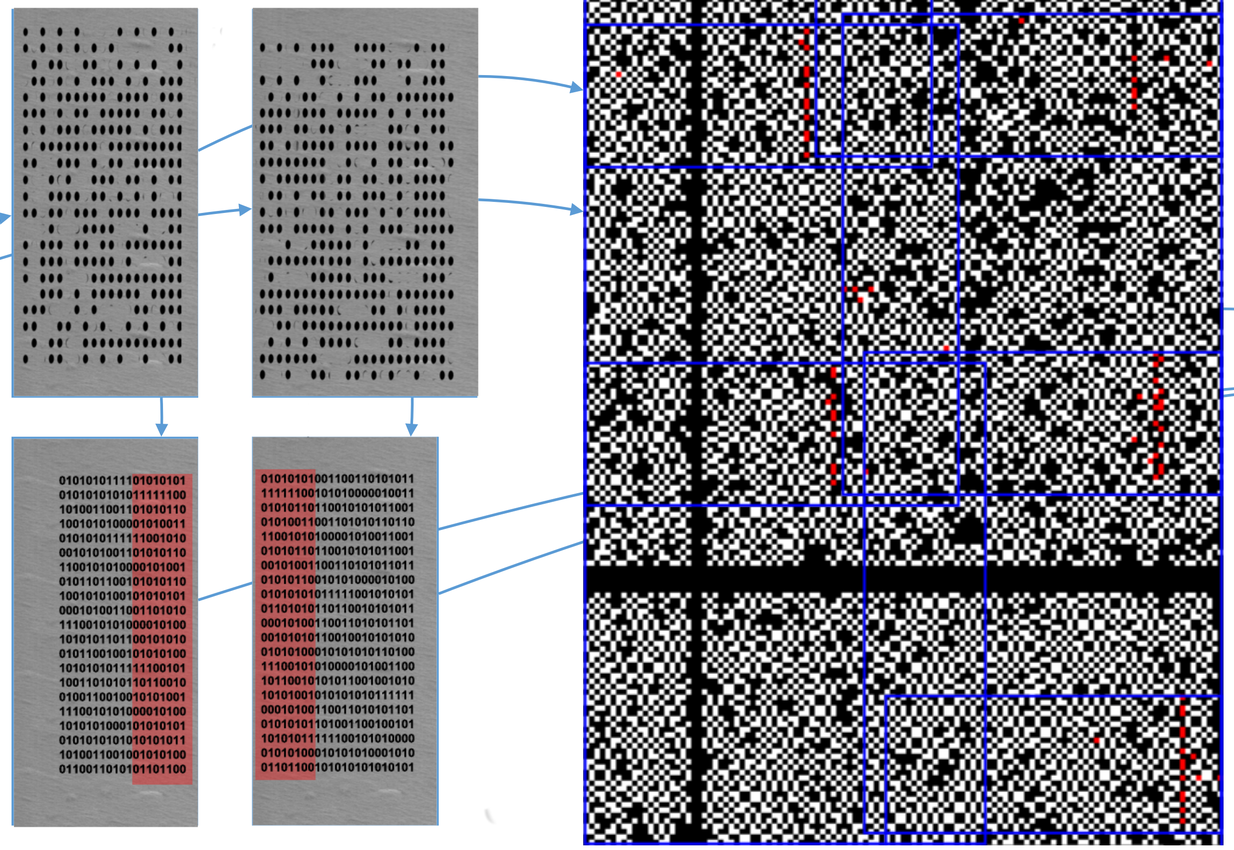

*ROM SEM Overview*

# Simulating Functional Blocs

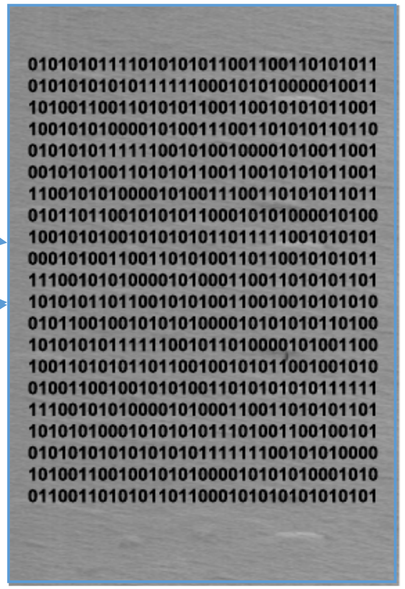
## Scrambled & Encrypted NVMs



*40nm ROM SEM Scan*



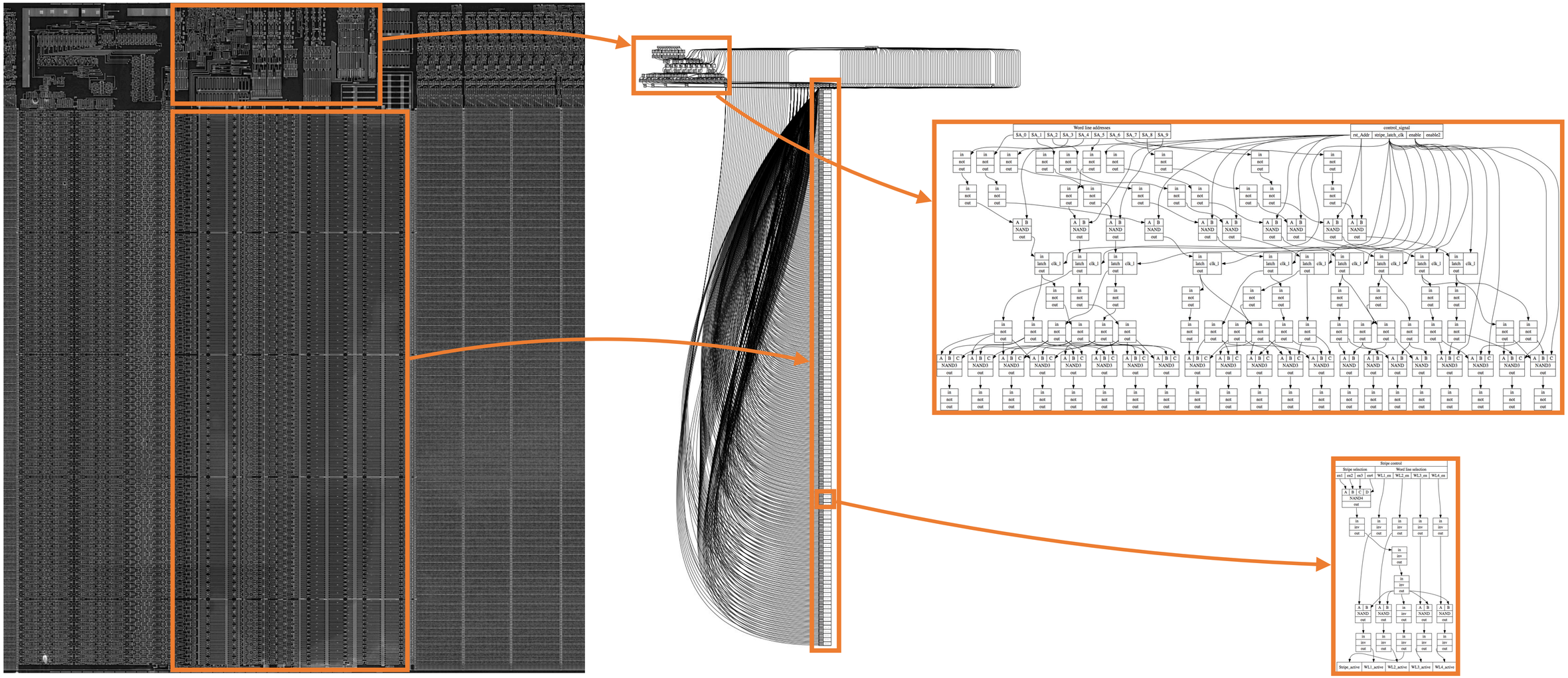
*Extracting every single images for ROM reconstruction*



*ROM Binary*

# Simulating Functional Blocs

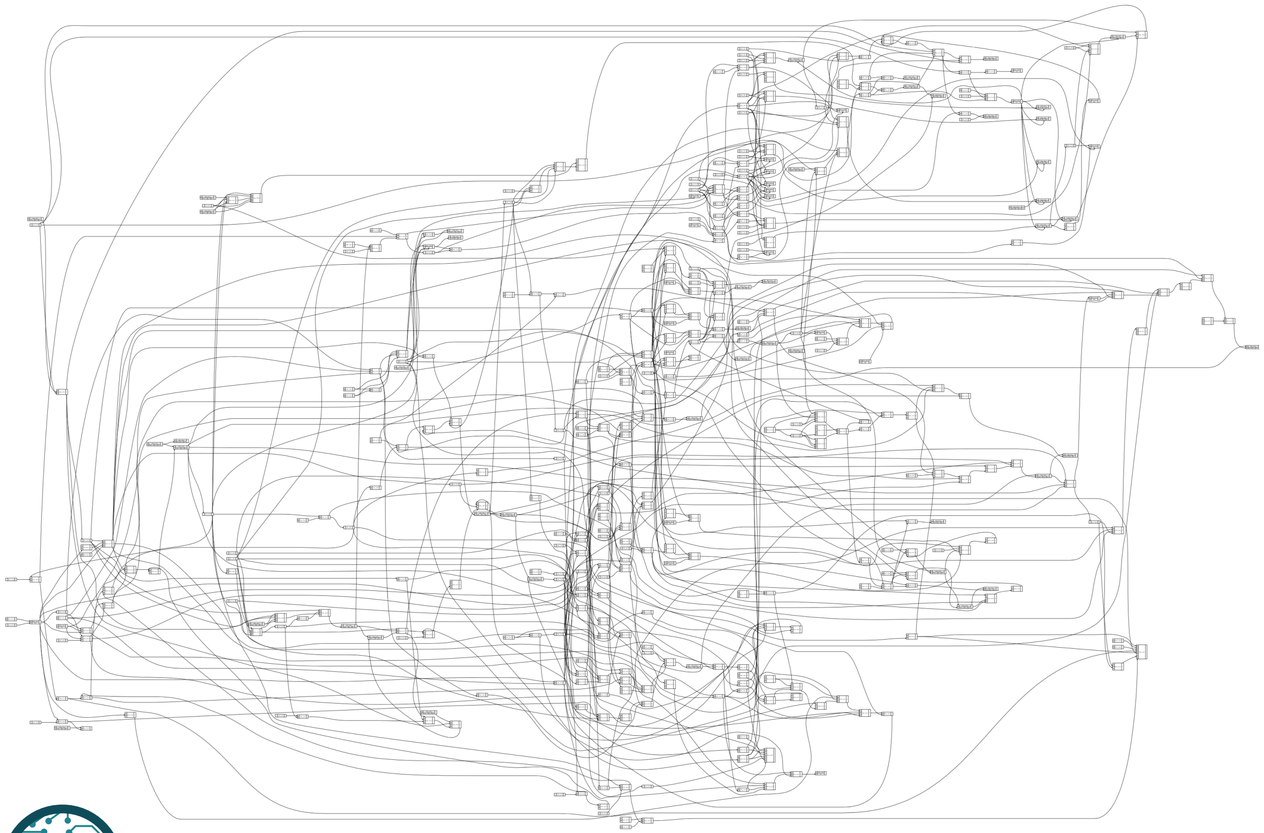
## Scrambled & Encrypted NVMs

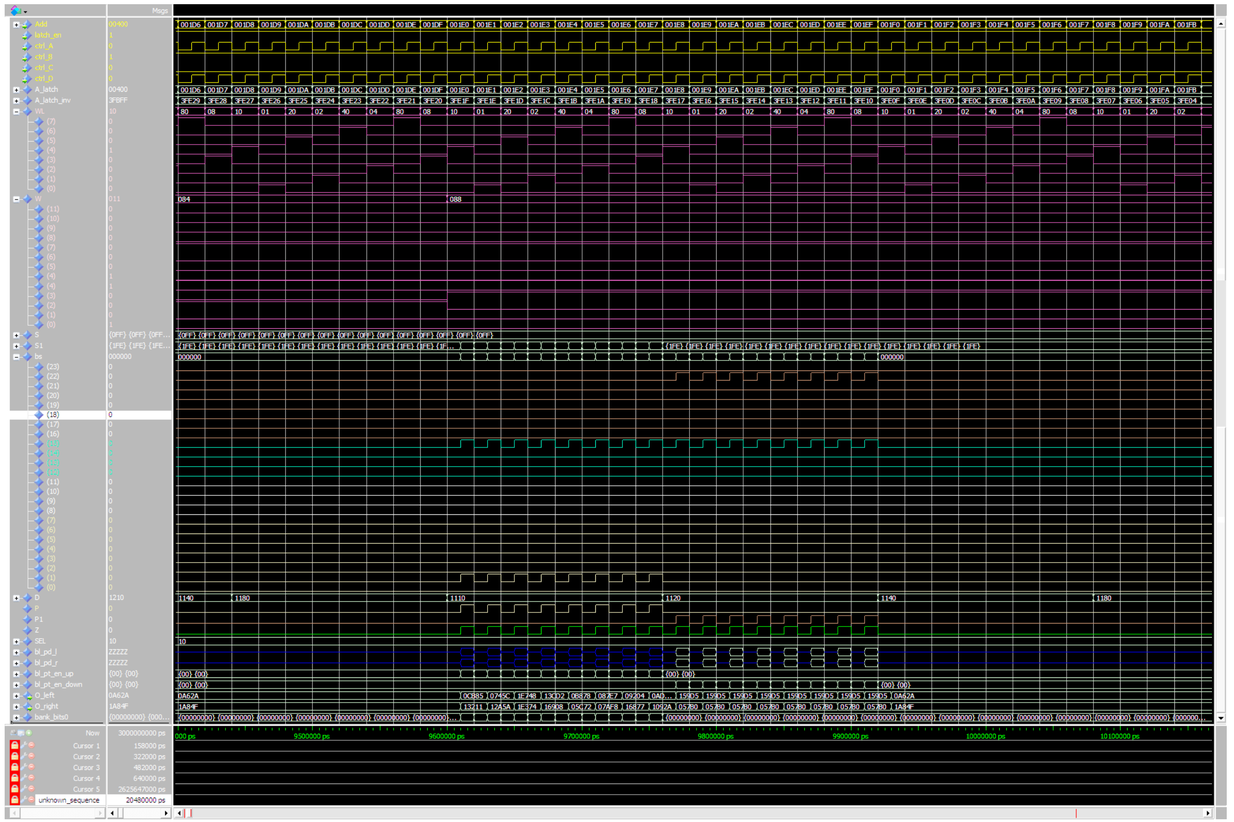


# Simulating Functional Blocs

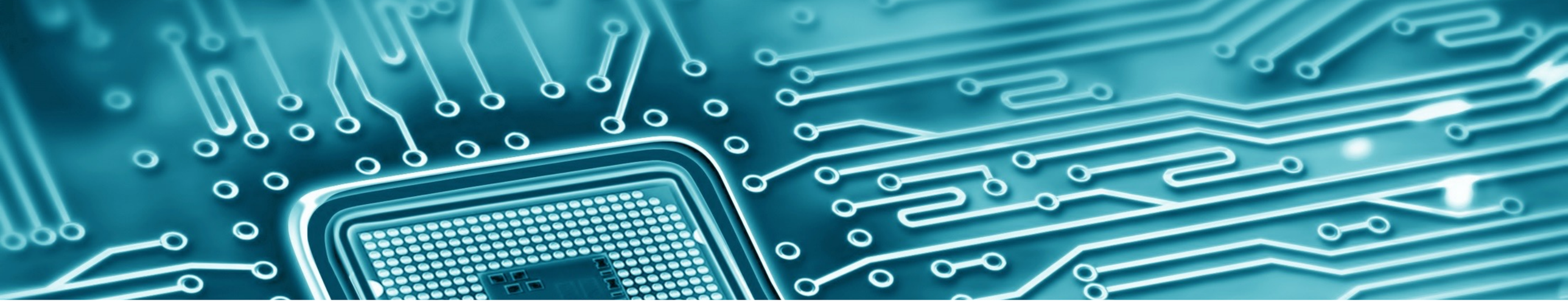
## Scrambled & Encrypted ROM

- Extracting the decryption circuitry and simulating it with the rest of the model makes it possible to extract the NVM - no FIB needed.

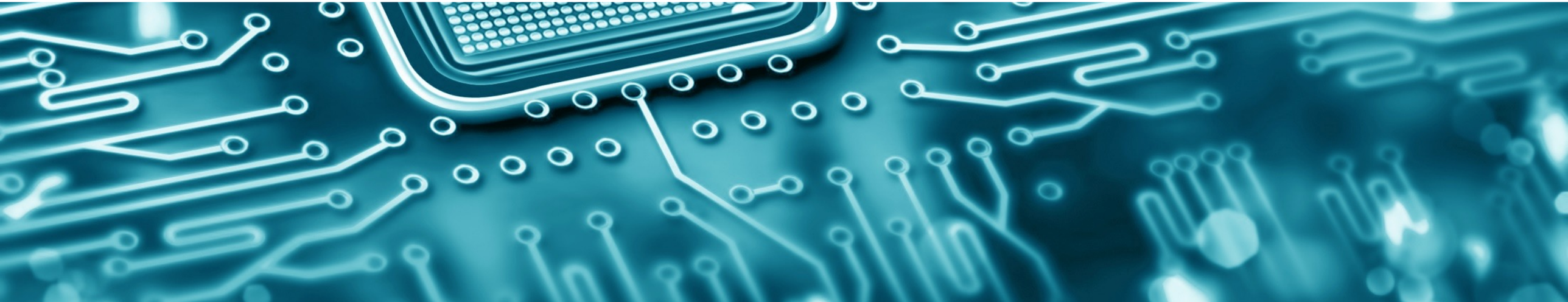


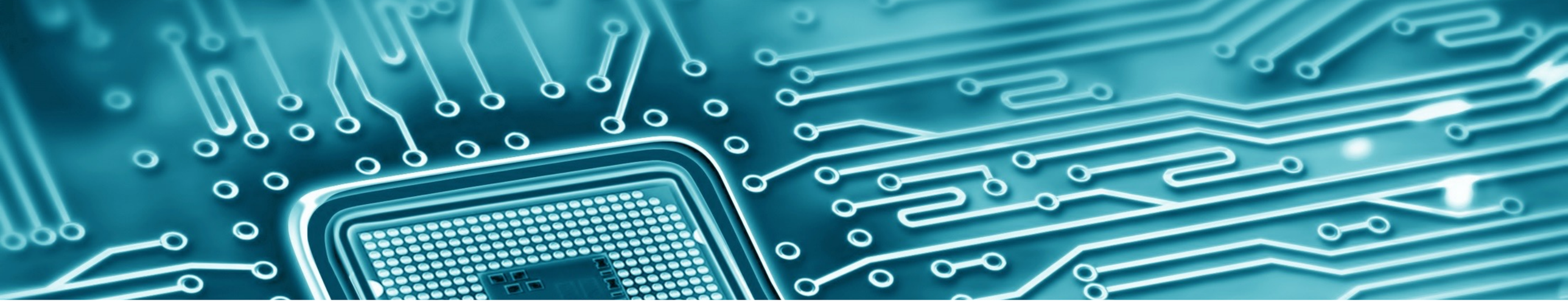


*Extracted Decryption Circuit and Its Simulation Data*

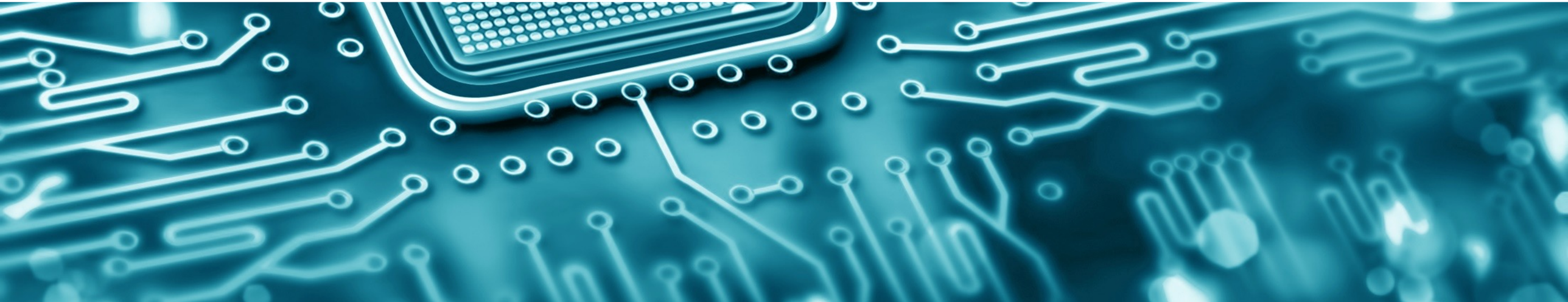


# REVERSE-ENGINEERING BASED ATTACKS





# CLK GLITCH FROM THE INSIDE



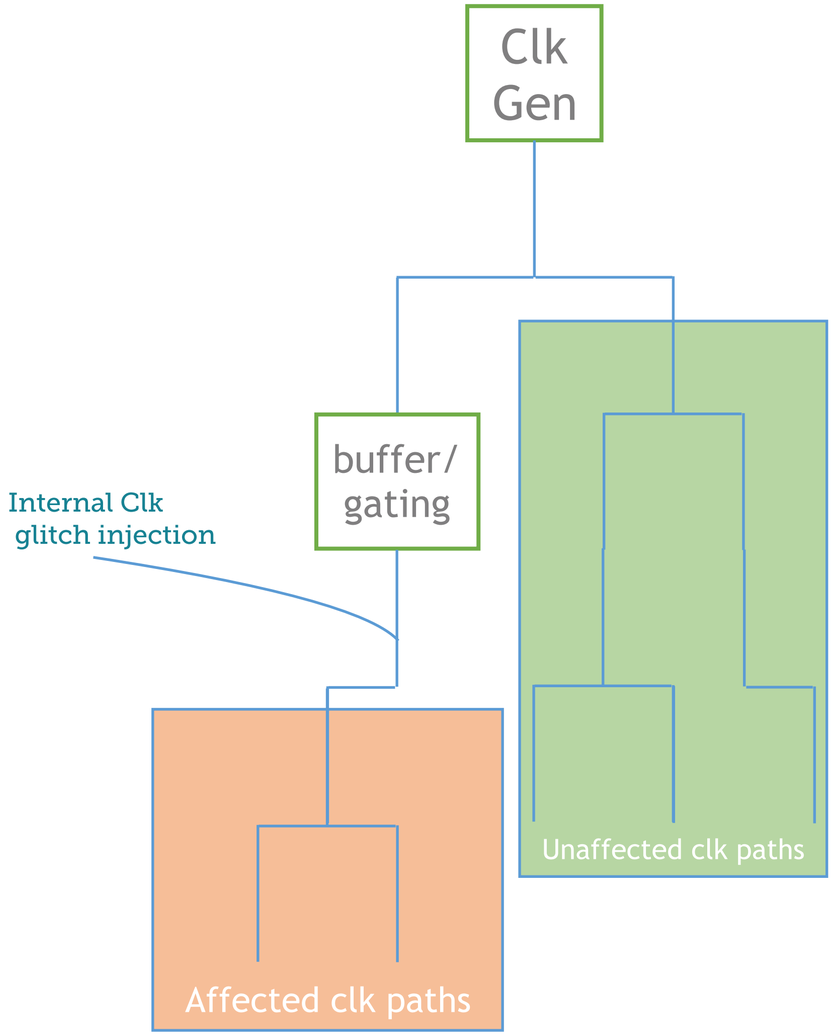
## Invasive VCC/clk Glitching

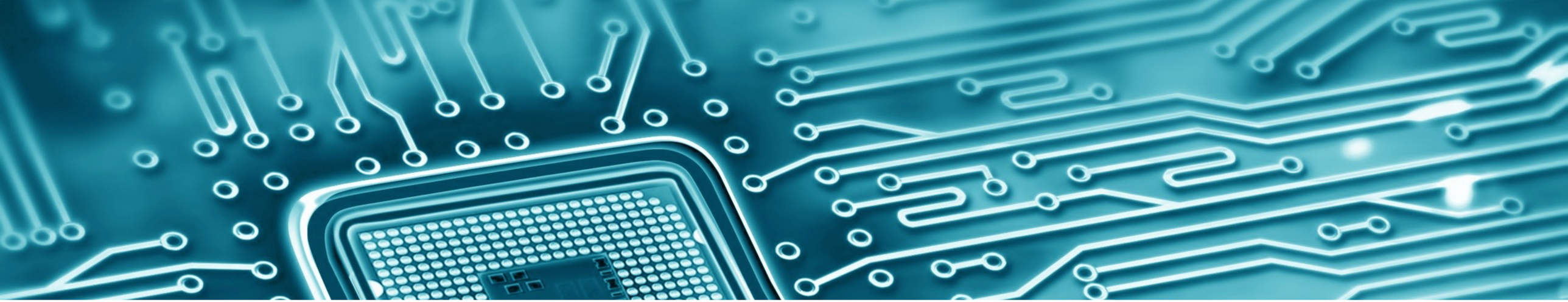
From non invasive global fault injection to invasive targeted fault injection :

- Silicon vendors have (almost) solved issues such as non invasive attacks for example.

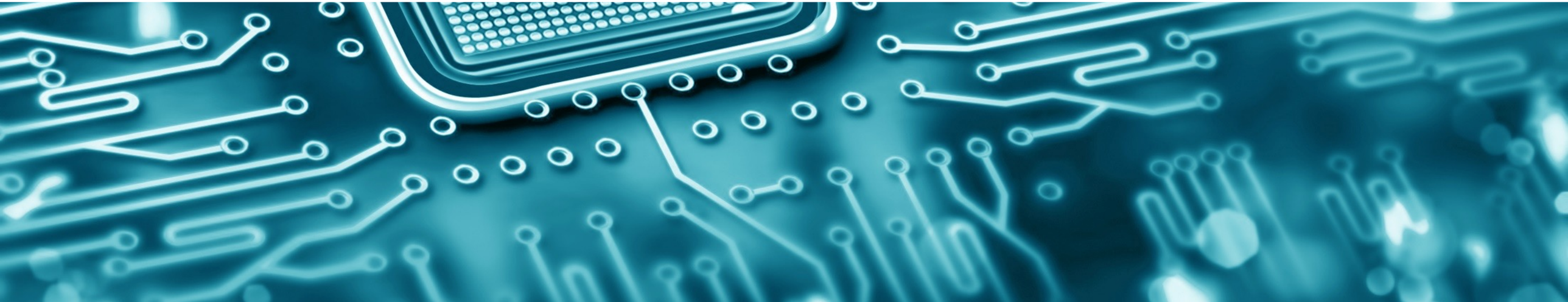
- Having the ability to study the netlist of an IC means that :
  - its clock tree can be fully analyzed. This means that not only a clock glitch could be performed from the inside of the chip but that it could be performed on a specific branch of the tree, avoiding the creation of a global disturbance which would be hard to understand and therefore harder to exploit.

    - The same reasoning can be potentially true (device dependent) for VCC glitch.



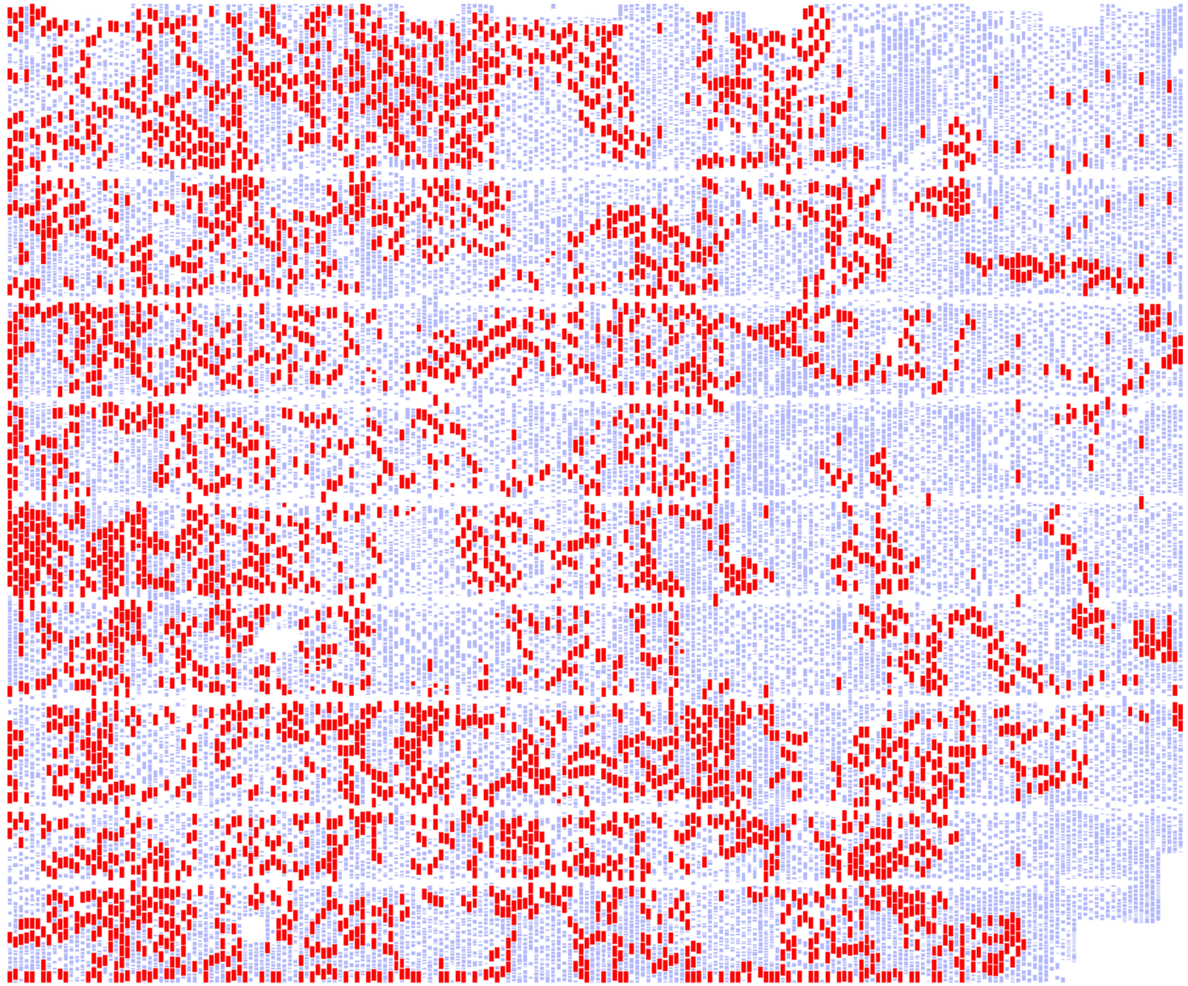


# IMPACT ON SEMI-INVASIVE ATTACKS



## Smart Gun

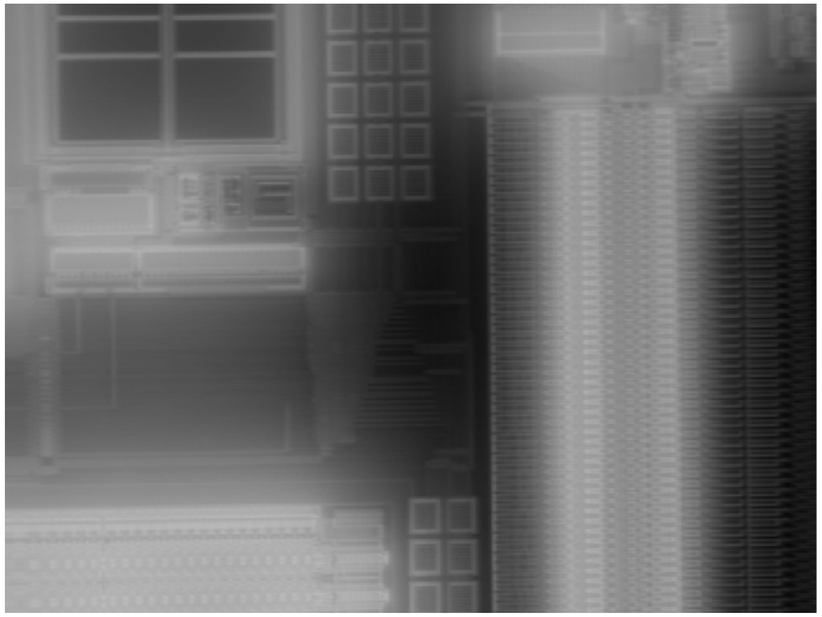
- Standard Cells can be filtered out to see only specific functions or cell types.
- This makes the GDSII ready to drive a fault injection / side channel station from the filtered data.
- When it comes to Laser Fault Injection,
  - firing on combinatorial standard cells might have an effect that can disappear before it is registered.
  - firing on sequential logic is a good way to increase the chance the fault is actually being registered.
  - only firing at the later can bring a huge decrease (>75%) of the duration of the evaluation while making the result more detailed.
- We call that technique « SMART GUN ».
  - It can be extended to a number of semi-invasive attacks.
- This also applies for other techniques such as EMA and photo-emission.



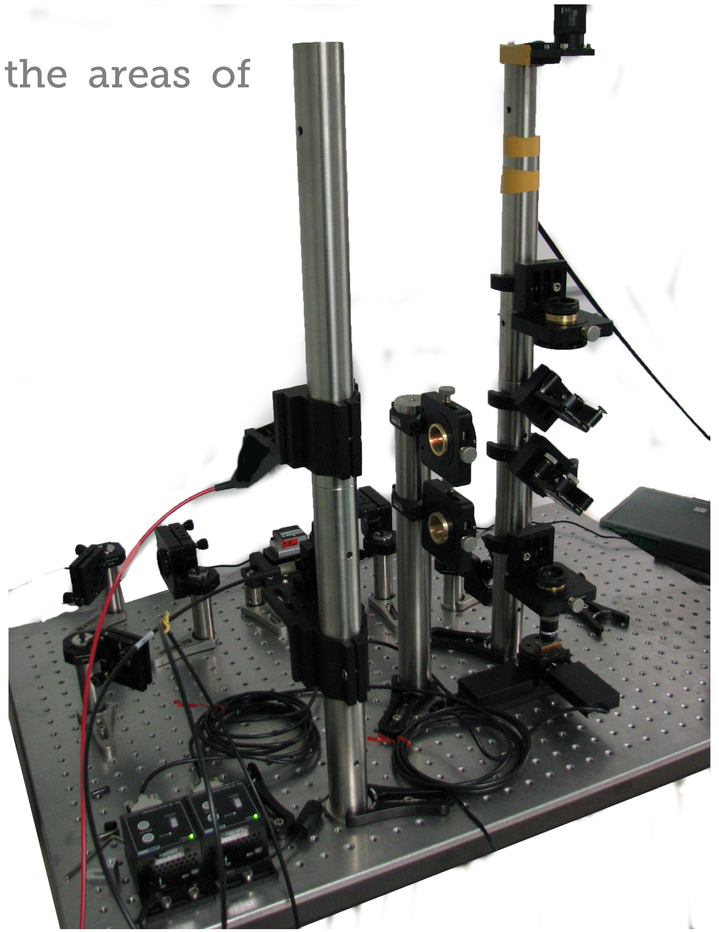
*Standard Cells Map (Sequential Cells in red)*

## Upgrading a DIY Semi-Invasive Station

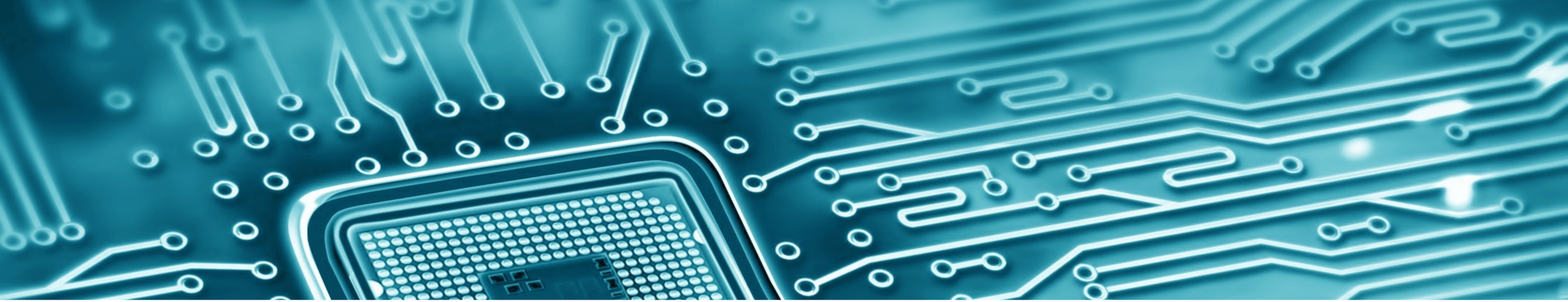
- Building a Laser Fault Injection station can be achieved for few K$.
- By adding stages or by using scanning mirrors, OBIC (Optical Beam Induced Current) measurement can be automated to create pictures of the device under test for navigation purpose.
- By being able to use the scanning capabilities of the station for creating picture of the areas of interest, placement of the laser for the actual fault injection can become very precise.
- By writing the appropriate software, the station will become Smart Gun ready.



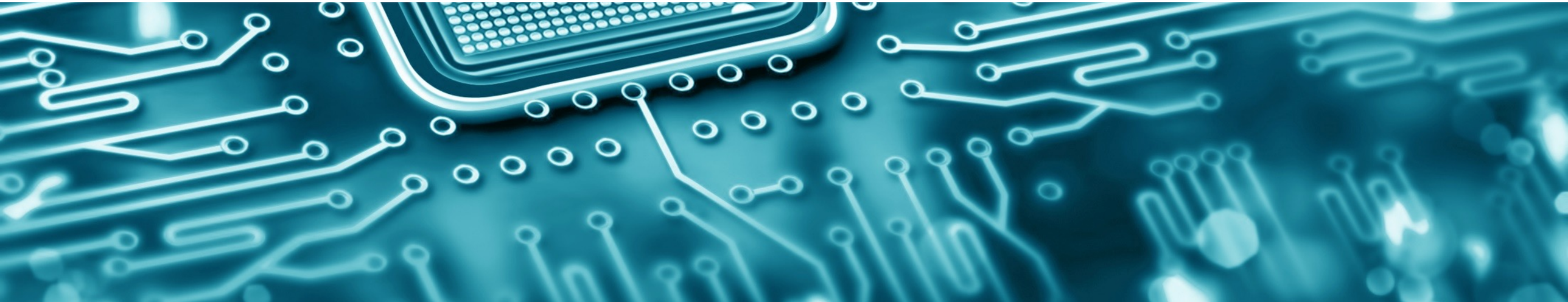
*Example of OBIC picture made with a DIY LFI Station*



*DIY LFI Station*



# INTEGRATED CIRCUIT SECURITY EVALUATION



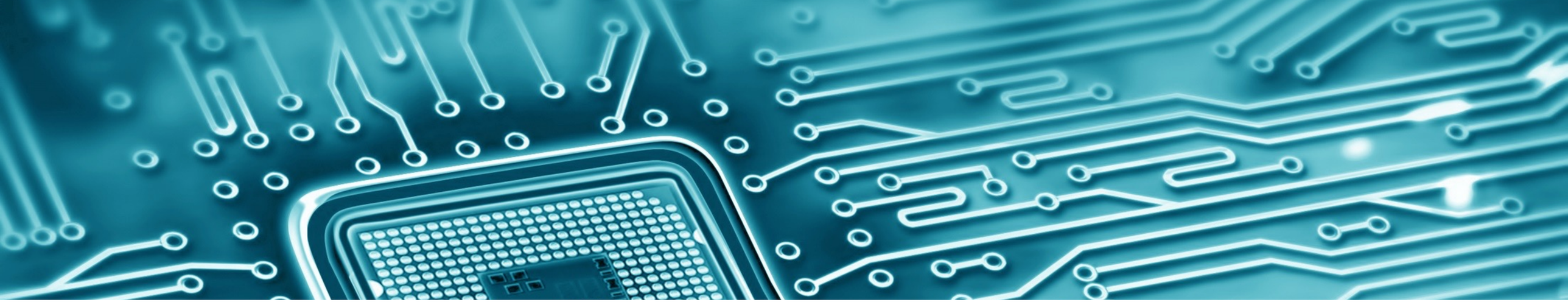
## Common Criteria Example

- Security evaluations cover non- and semi-invasive attacks.
- Invasive attacks are also in the list of items to be evaluated but:
  - An attack that would fall inside the invasive category will be considered de-facto as a residual threat:
    - timing evaluation does not makes sense in the invasive context
    - extracting the netlist brings a penalty as it is considered as having prior-knowledge
    - Equipments is considered not common and expensive
    - Expertise of the attacker is considered the highest

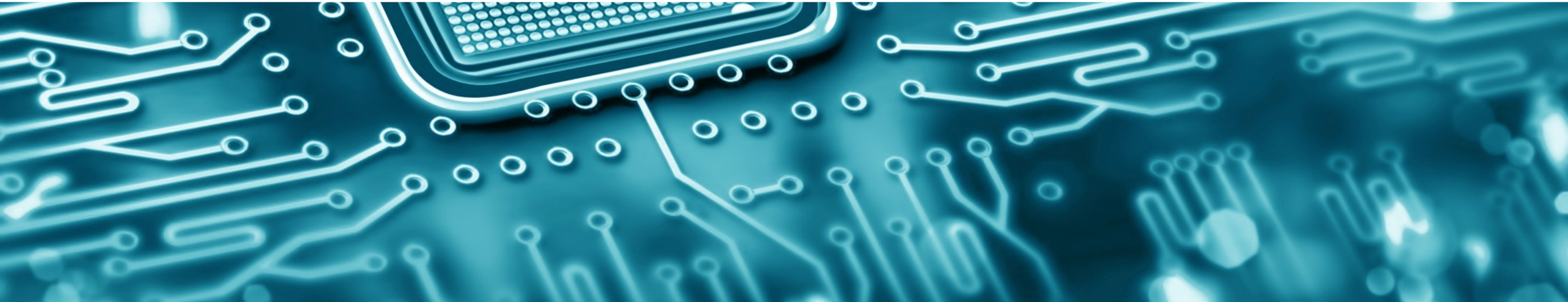
- In these condition, an invasive attack always reaches the 31 points mark, making it a residual threat before it is even evaluated.

| Range of Values | TOE resistant to attackers with attack potential of: |
|---|---|
| 21-24 | Enhanced-Basic |
| 25-30 | Moderate |
| 31 and above | High |

*Common Criteria Overall TOE Security Level*



# INTEGRATED CIRCUIT REVERSE-ENGINEERING APPLICATIONS



# Integrated Circuit Reverse Engineering Applications

Texplained

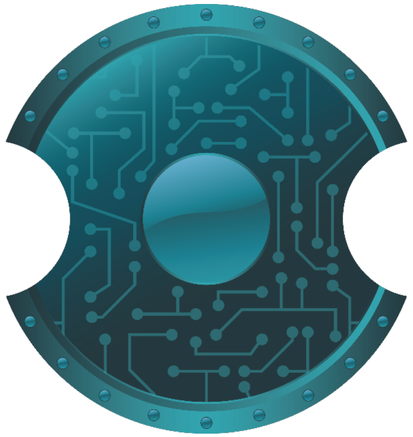
## Overview

### Custom Hardware Analyses

Realization of in-depth explorations: specific -> global

### Patent Infringement / IP Theft

Documented technical report that can be a basis for litigation against an infringing party, based on gds2 / netlist re-construction of the suspect device



### Pirate Devices Analysis

Analysis of Pirate Devices & accompaniment in the implementation of countermeasures

### Obsolescence Management

Recovery and replacement of the obsolete IC with an alternative solution

### Backdoor Research

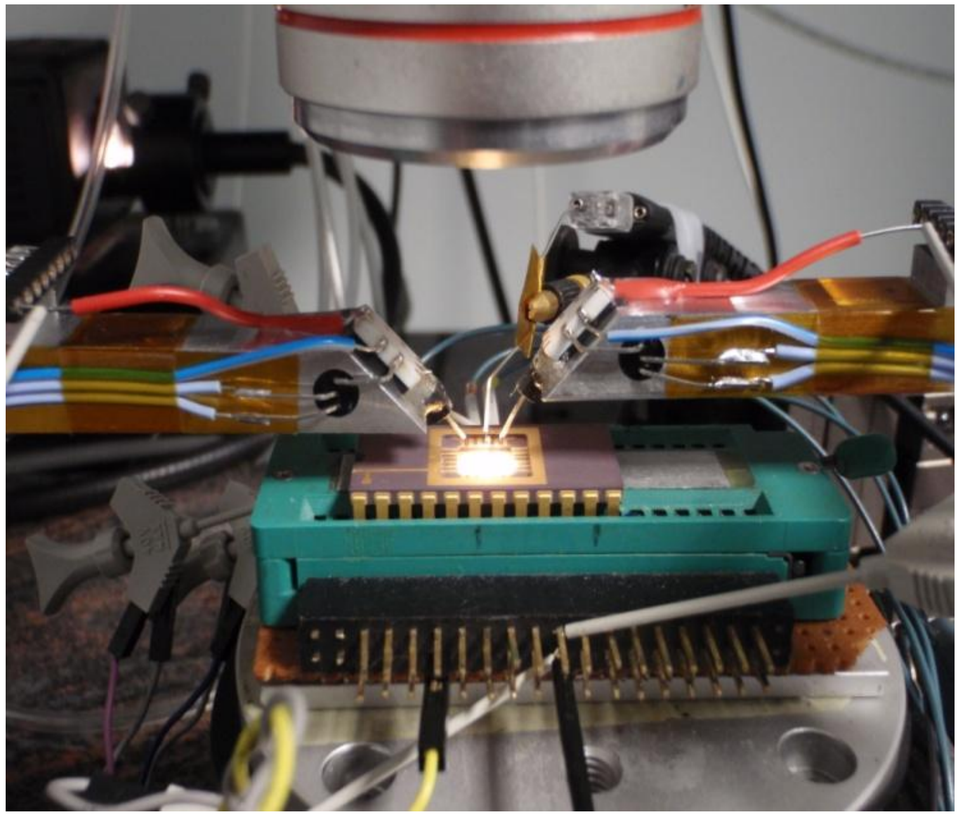
Detection of hardware backdoors

### Design Review

Providing support for development and test of innovative security mechanism

## Risk-Assessment / Benchmark

- Security Evaluation for Chip Vendors / OEMs / Integrators
- Benchmark : the best security / price ratio
- Integrators can also « hack » in the pirate devices to find out about the pirate implementation of their products and therefore create targeted counter-measures.

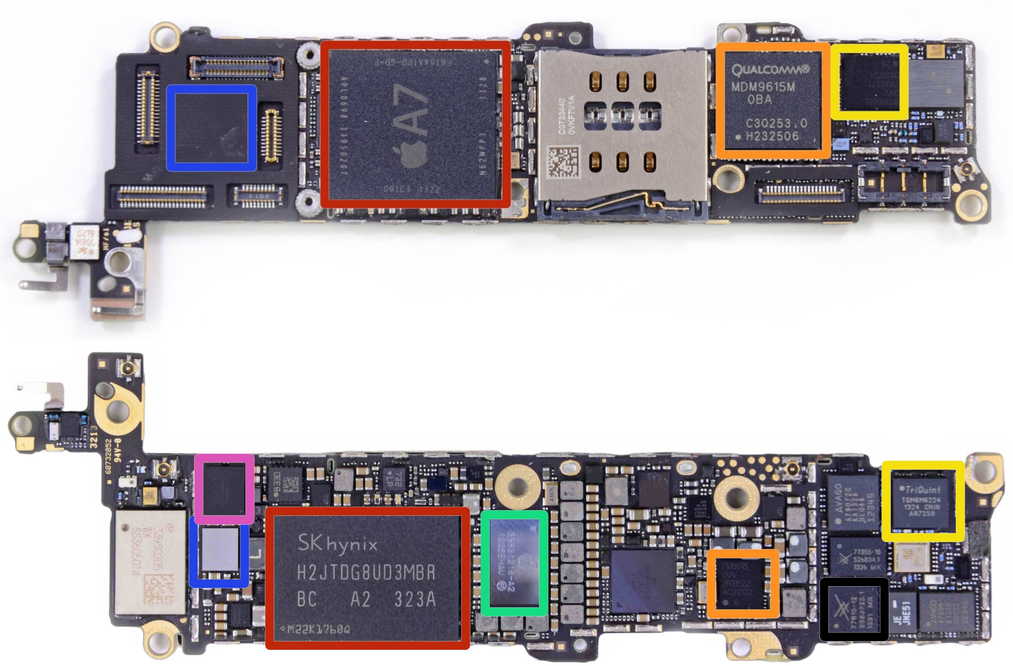


*Probing Setup With 3 Needles.*

## Forensics

- Personal data protection is key in our connected world.
- But when it comes to crime issues such as terrorism, child pornography, etc, there is a need to be able to access data.

- Forensics on modern, heavily encrypted devices requires to bypass a number of security measures and cryptographic challenges.
- Doing this in a black box scenario with known techniques can be tricky and time consuming.
- Starting with Reverse-Engineering data can help a lot in that context.



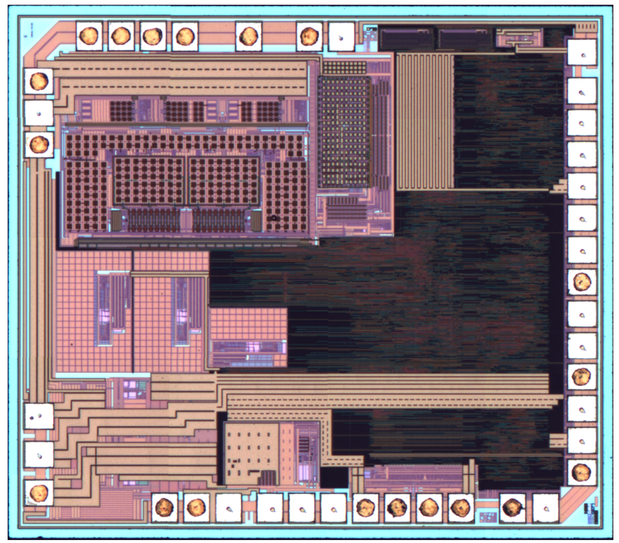

- https://www.ifixit.com/Teardown/iPhone+5s+Teardown/17383

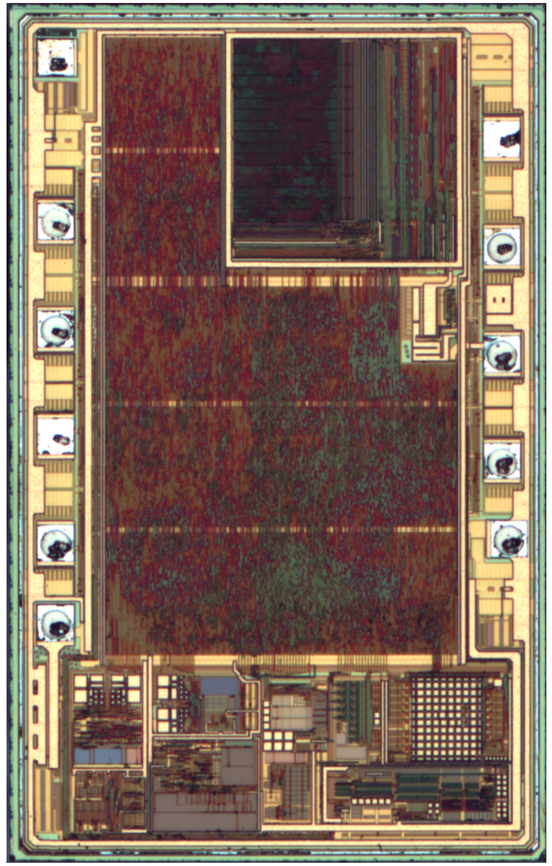
## Compatibility

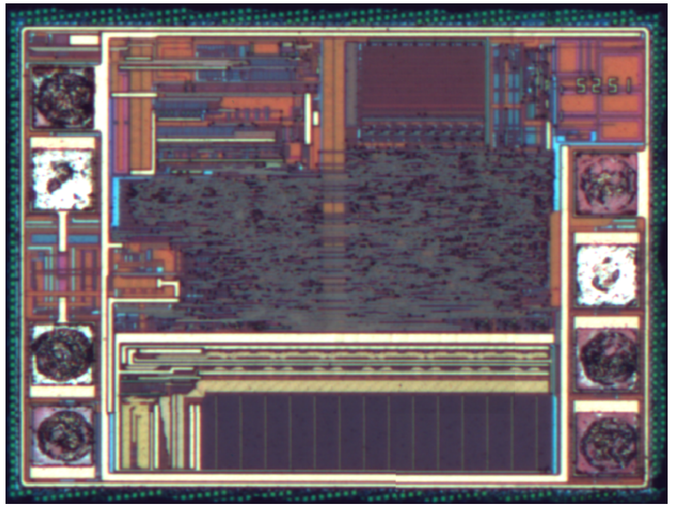
- Making compatible products is driving the IC reverse-engineering world (printer cartridges, game console controllers)
- In many area, proprietary systems makes it hard for third parties to develop their own solutions (automotive for example).

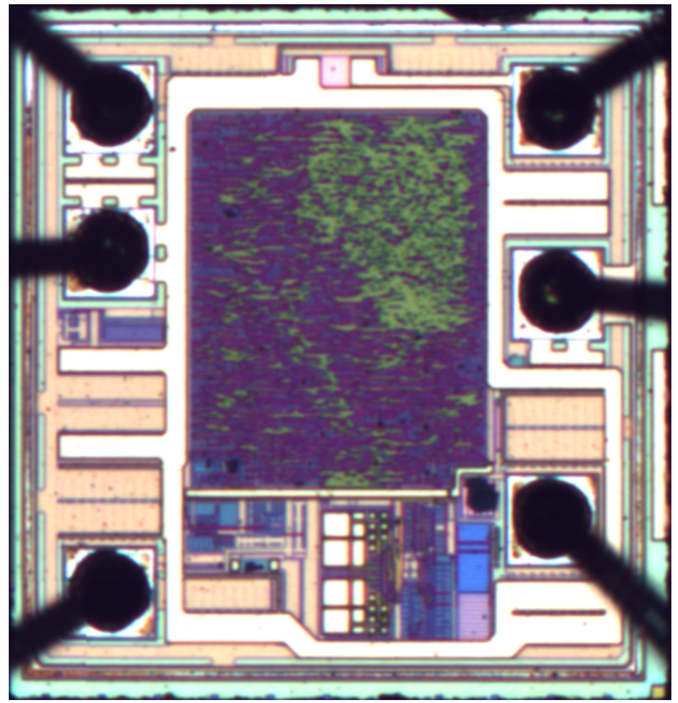

*The most attacked ICs…*

## Counterfeited Device Detection









*Several generations of lightning cable counterfeits ; from general purpose micro controllers to custom ASICs.*

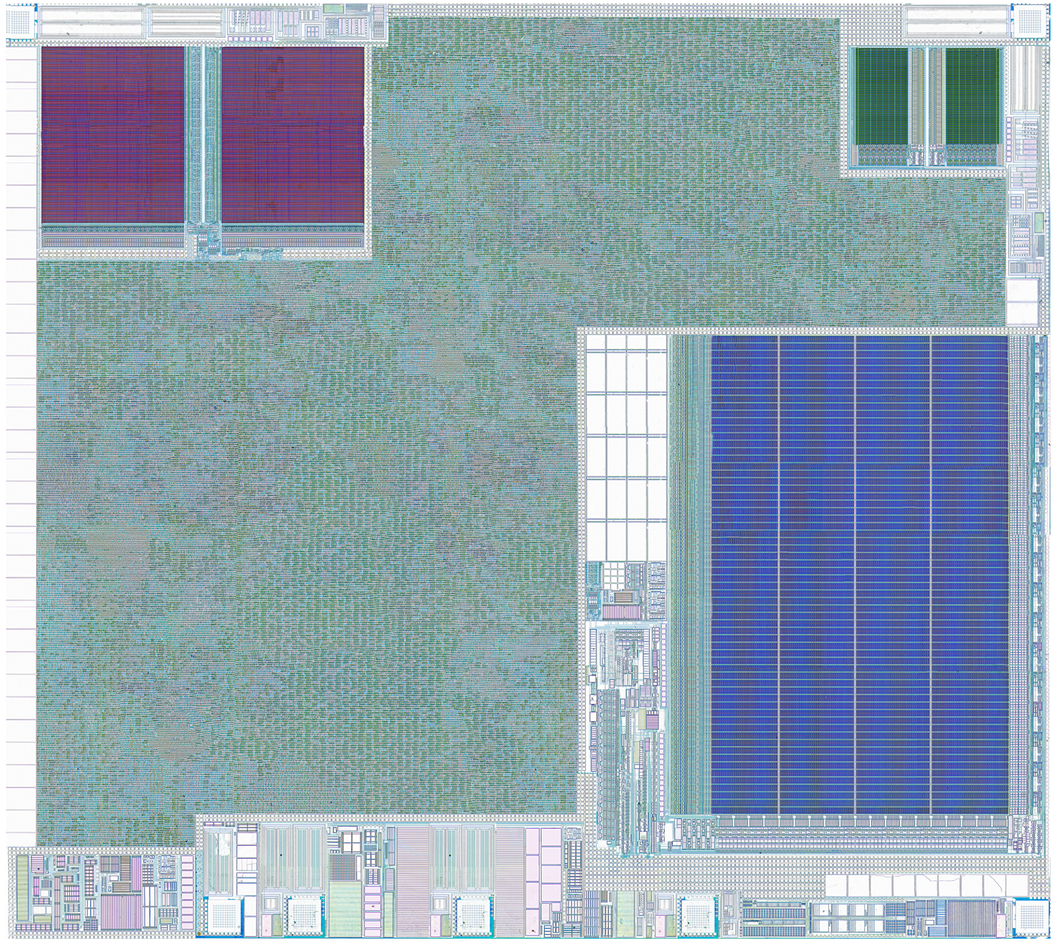
## Hardware Trojan / Backdoor

- Counterfeited ICs can be less reliable which is already a problem but…
- With the manufacturing of Integrated Circuits being most of the time outsourced, there is a need to validate the supply chain.
- A Hardware Backdoor could have been included in the final product which will then be distributed and use for critical applications:
  - networking
  - military / defense
- Checking that the device is physically the same as the golden sample is a good option to make sure the IC is genuine.
  - From pictures
  - From extracted features makes it possible to filter out any extra or missing circuitry and to get a model that can be simulated and thus characterized.


*Hey Joe, Cool Sticker :-)*

## Patent Infringement Research

- When a chip vendor suspects its competitor to use one of its IPs without the appropriate rights, it may be hard to prove the IP theft.
- Being able to Reverse-Engineer the IC and to extract the functional blocs from the recovered netlist allows for the creation of documents that proves the infringement.
- Those data can then be used in court.



*Optical Scan of Substrate Layer*

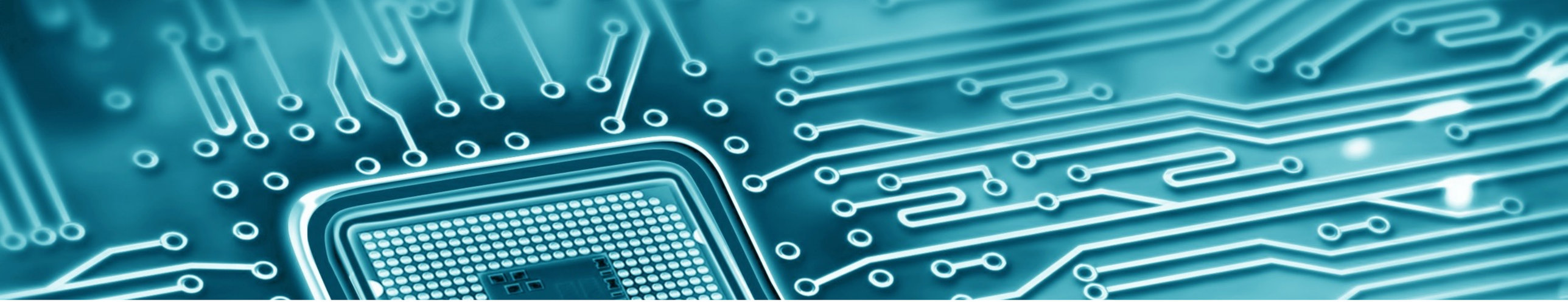
## Cost Effective Method for Obsolete IC Management

- Integrated Circuits have a limited life time.
- When ICs are discontinued, there is a risk that the knowledge about the hardware implementation and functionalities disappear.

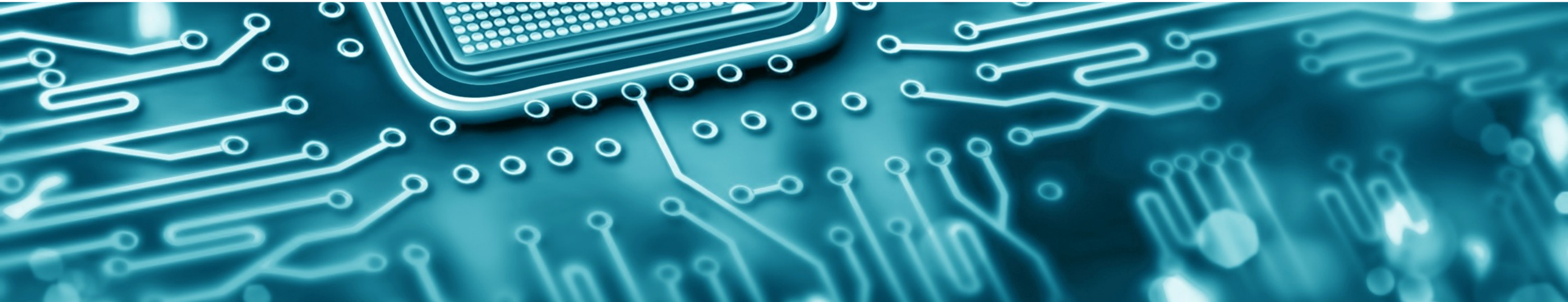
- On top of that, embedded data and firmware can also be not accessible.
- In these conditions, it might be hard for an Integrator to find a replacement for its obsolete device.

- Being able to Reverse-Engineer the digital logic can be used to recover the IC functionalities and their implementation.
- It can also be used to re-gain access to the embedded data (firmware, cryptographic keys, other stored data) which is often mandatory to design a replacement solution.

- From the recovered data, a new design can be implemented in a FPGA for example in order to replace the obsolete component without redesigning complete sub-systems.



# CONCLUSION



## Conclusion

Goal : Let's discuss the following

- IC RE and invasive attacks are often considered as a residual threat by certification schemes / Chip vendors
- In a number of applications, REing a chip and extracting its embedded data is common practice
- IC security seems to be used in an offensive context only

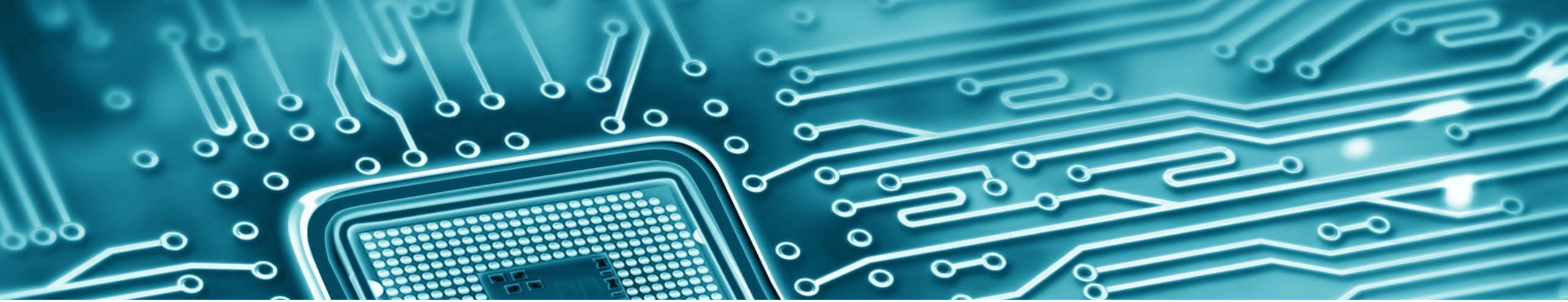
Few remarks :

- Chip vendors made a lot of progress but there is a lot to do

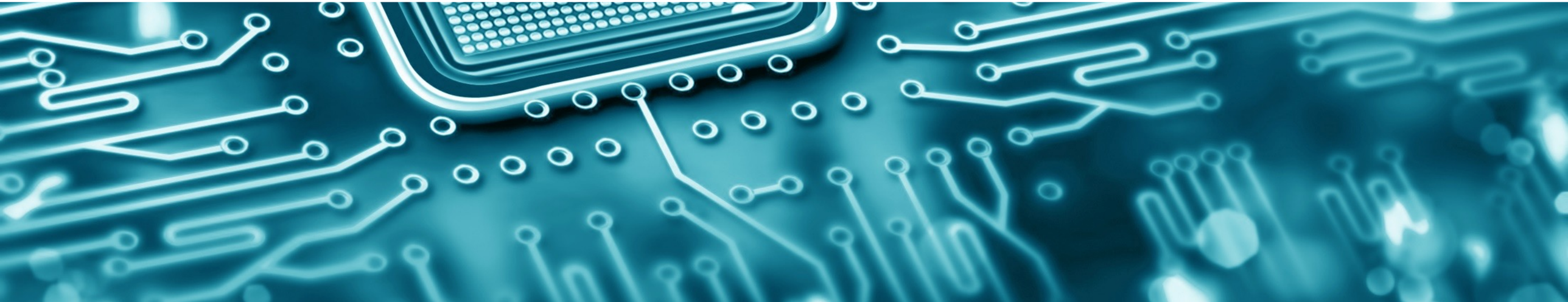
- Certification schemes are mostly considering that invasive attacks are a residual threat. What about RE based attacks.?

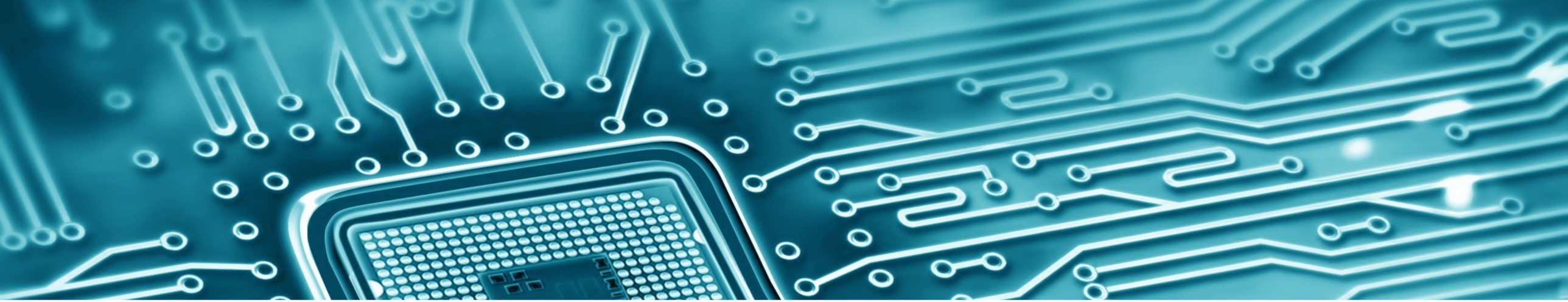
- There are a lot of applications for IC RE
  - Integrators do not want to rely on datasheet / certification only especially in the most exposed markets
  - Forensics demand is constantly growing, showing that other attack vectors are better handled
  - Supply chain verification against hardware trojan is a reality for security critical markets
  - IP infringements research and obsolescence management need RE to be performed efficiently

- Compatible products design pushed the RE technology a lot but tools and methods are proprietary and well hidden assets of the main players.



# QUESTIONS?





# CONTACT


**Olivier Thomas**
Chief Technical Officer
+33 6 64 80 06 87
olivier@texplained.com

**Clarisse Ginet**
Chief Executive Officer
+33 6 35 54 12 04
clarisse@texplained.com

www.texplained.com