ISTFA™ 2017: Proceedings from the
43rd International Symposium for Testing and Failure Analysis
November 5–9, 2017, Pasadena, California, USA

Steps Toward Automated Deprocessing of Integrated Circuits

E.L. Principe[1], Navid Asadizanjani[2], Domenic Forte[2], Mark Tehranipoor[2], Robert Chivas[3], Michael DiBattista[3], Scott Silverman[3], Mike Marsh[4], Nicolas Piche[4], John Mastovich[5]

[1]Synchrotron Research, Incorporated, Melbourne Beach, FL,
[2]Florida Institute for Cybersecurity, University of Florida, Gainesville, FL, USA
[3]Varioscale Incorporated, San Marcos, CA, USA
[4]Object Research Systems, Montreal, Canada
[5]Bruker, AXS Inc., Madison, WI, USA

Abstract

Deprocessing of ICs historically employs a variety of mechanical and chemical process tools in combination with one or more imaging modalities to reconstruct the IC architecture. In this work, we explore the development of an extensible programmatic workflow which can take advantage of evolving technologies in 2D/3D imaging, distributed instrument control, image processing, as well as automated mechanical/chemical deprocessing technology. Initial studies involve automated backside mechanical ultra-thinning of 65nm node 3.0 cm^2 Opteron IC processor chips in combination with automated montage SEM imaging and lab-based x-ray tomography and microanalysis. Areas as large as 800umX800um were deprocessed using gas-assisted plasma FIB delayering. Ultra-thinning the silicon substrate in the packaged device within 1-2um of the IC device significantly reduces the amount of time required for deprocessing. The computer aided backside ultra-thinning approach not only improves the success rate, as compared to manual techniques, it also allows the dense lower layers with smallest feature size to be imaged via high resolution SEM first, while the sample layers are the most uniform. Backside deprocessing has the additional advantage that it can be possible to access the device while keeping it "alive" for in-situ electrical testing. Ongoing work involves enhancing the deprocessing workflow with "intelligent automation" by bridging FIB-SEM instrument control and near real-time data analysis to establish a computationally guided microscopy suite. As described in the text, a common python scripting API architecture between the FIB-SEM platform and the image processing and microanalysis platforms permit rapid development of customized programmatic instrument control with data process integration and feedback. Current studies use smartcards as an archetype to develop automated workflows. Smartcards represent a good architecture to discuss and develop these methods because they are as much as sixteen times smaller area than a $1cm^2$ processor and typically containing far few layers. Yet these small form factor embedded integrated circuits have rapidly become a widespread element of modern society and their security architecture represents an important problem. We demonstrate for the first time; tomographic reconstruction based upon automated back-side ultra-thinning coupled to automated gas-assisted plasma FIB delayering.

Keywords: Deprocessing, Integrated Circuits, Computationally Guided Microscopy, tomography, plasma FIB, delayering

Introduction

The typical deprocessing task extends from the centimeter to sub nanometer scale – over seven orders of magnitude in length scale. This panoscopic workflow requires the integration of a variety of repeated mechanical and/or chemical

processes interleaved with a variety of data modalities which contribute layout data, structural data, chemical data and functional device data. A depiction of the traditional deprocessing workflow is illustrated in F1. A single monolithic tool which can accomplish the complete task of automatic deprocessing of an IC still does not exist, and practically may never be the most effective approach. Depending upon the technology and the objective of the analysis, a varying degree of mechanical deprocessing is required in addition to chemical processing which could involve reactive ion etching and/or wet chemical processing along with the image data.

Common tool suites for deprocessing in a modern facility may combine x-ray tomography tools, mechanical delayering tools, chemical delayering tools, reactive ion etch tools, laser ablation systems, focused ion beam systems, IR imaging systems, electron beam based imaging systems and tools to determine elemental and chemical composition (i.e., EDS, ToF-SIMS).

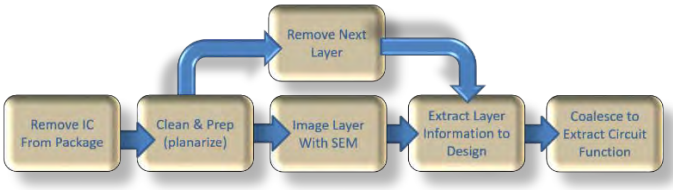

Figure 1. Traditional deprocessing workflow based upon SEM imaging. Graphic adapted from David Weaver, et al., "Fast Mask Data Recovery to Provide Missing/Incomplete Technical Data Packages (TDP) for Obsolete ICs and Validating Trust Within ICs", GoMACTech 2011.

The overall process can be considered as an integration of sub-processes and subsystems. As technology has evolved advances have been made in SEM imaging, particularly in terms of low voltage high resolution imaging.

More recently, with the advent of high current plasma FIB-SEM platforms with advanced Gas-Assisted Etch (GAE) chemistry; it has become more practical to perform large area delayering in-situ. This integration removes one iterative ex-situ step requiring mechanical planarization and cleaning. An open API architecture based upon Python scripting, further allows rapid and customized automation of the FIB-SEM operations, including montage imaging and GAE delayering. This capability provides the end-user with a versatile programmatic functionality which reduces dependence upon vendor-specific software functions.

Likewise, the development of adaptive 5-axis CNC precision multi-tool grinding and polishing ushers a new level of capability and automation to IC deprocessing. The end result is an ability to perform automated backside deprocessing within 1-2um of the active area across a 25 mm x 25 mm die. To appreciate the importance of this technology, one must consider that neither a virgin packaged or extracted die is flat, but undergoes stresses and relaxation with an individual manufacturing and assembly history. As the silicon substrate is removed from the die during thinning steps, the stresses due to packaging and thick copper redistribution layers (RDL) result in bending. Thus, this automated precision milling technology must actively measure both shape and thickness and dynamically adapt to the evolving surface profile while reaching a nominal 3nm RMS roughness.

A representation of this process is shown in Figure 2. The initial thickness of the device in package is 775um with a curvature that results in a measured sag of 180 um. When the process reaches its desires substrate thickness of 25um, the device has relaxed and the overall curvature of the device has reduced by nearly 55um to a measured sag of 125um.

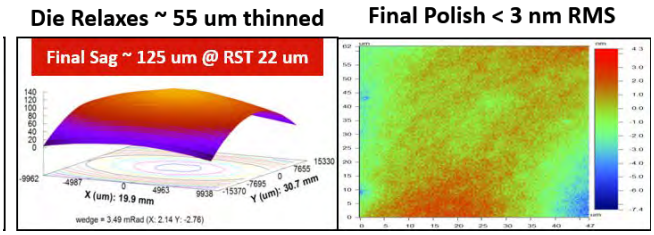

Figure 2. The initial die is not flat (panel 1); relaxes during thinning (panel 2-3); polishing head adaptively tracks the surface thorugh final polish (panel 4).

The necessary key statistical data from grind and polish process steps from these advanced sample preparation tools can be fed forward to the API driving the automated plasma FIB-SEM. Such values include the remaining silicon thickness (RST) and optical measurements of die warpage at each physical location on the die. This data and the corresponding model of the substrate shape and residual silicon thickness provide guidance during delayering. Combining the evolution of automated plasma FIB-SEM platforms and automated backside milling technology enables a revision of the traditional delayering workflow, represented in Figure 3.

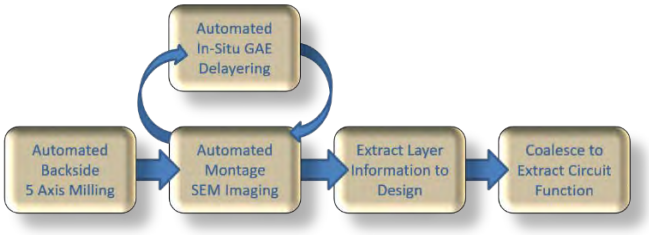

Figure 3. A revised deprocessing workflow based upon the combination of automated backside ultra-thinning and automated plasma FIB-SEM delayering. Ultra-thinning may be performed with the chip without depackaging and frontside mechanical planarization.

The ability to perform ultra-thin automated backside preparation significantly reduces the effort as compared to frontside preparation and eliminates the typical requirement for mechanical polishing down to ~M5, prior to FIB-SEM delayering. Moreover, the sample is prepared for delayering at the most dense layer, where high resolution SEM imaging is most critical. The coupling of these two automated subsystems, involving ultra-thinning and large area plasma FIB-SEM delayering represents a step forward in the automation of IC deprocessing. Following presentation of data from the deprocessing of a 65nm node AMD Opteron chip, we will discuss the potential for further automation of IC deprocessing.

1. Case Study: 65nm node Opteron IC delayering

An example of a 17mm x 18 mm die previously backside ultra-thinned by automated adaptive 5 axis CNC processing using a Varioscale VarioMill™ and inserted in a Tescan FERA plasma FIB, prior to in-situ large area delayering, is shown in Figure 4.

Initial backscatter electron (BSE) imaging at 30kV, prior to any delayering already reveals IC structure. Note the entire die while still in the package can be accommodated. In this case, no coating or other preparation was employed. The delayering process involves the use of a proprietary gas chemistry in conjunction with 15kV plasma FIB and a current density ranging from ~0.5-2.0pA/um^2. Typical GAE exposure times between imaging were 7-10 minutes per layer.

In Figure 5, a set of images are shown following removal of the first layer of residual silicon. The BSE image on the left is 5kV while the BSE image on the right, showing more detail of features at greater depth was acquired at 30kV. Both images represent a montage, each consisting of 49 images of 4096X4096 pixels.

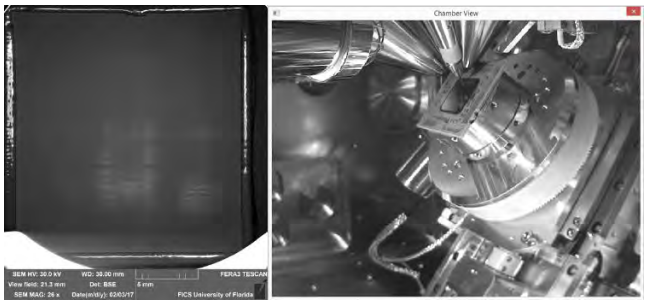

Figure 4. At left is shown a SEM image of the entire die inside the plasma FIB. Note the IC structure is already visible in the lower right corner in the BSE image prior to any pFIB delayering. The panel at right shows the entire die and package mounted in the plasma FIB-SEM at the delayering position.

Each montage was acquired in either 26 minutes or 43 minutes, depending upon the programmer's choice of field of view (FOV) and pixel density.

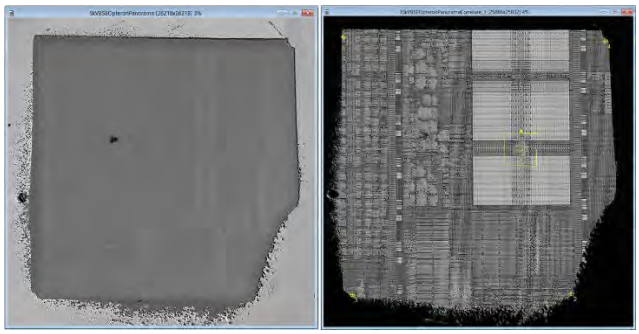

Figure 5. Initial backside delayering to remove silicon.

The BSE image at left was acquired at 5kV while the BSE image on the right was acquired at 30kV. The delayered area is approximately 800x800um. Each each shown is a montage consisting of 49 indivual images of 4096x4096 pixels each, acquired programmatically.

5kV BSE imaging following the initial removal of the residual silicon layer illustrates doping contrast, as shown in Figure 6. The panel at left shows the original montage, followed by two zoomed in regions and an inset panel in the upper right representing a cumulative horizontal profile trace defined by the region outlined in the first panel. The brighter and larger areas are the P-doped regions while the smaller and dimmer areas are the N-doped regions. This information is easily acquired from the thin silicon backside and enables the identification and placement of the NMOS and PMOS transistors during the circuit extraction function. This information has not been shown to be possible when the device is deprocessed from the frontside.

The process of sequential GAE delayering continues progressively moving through each layer, followed by automated imaging. There is full choice of the image conditions (voltage, detector, pixel density, field of view) for the montage operation. Typically, preset conditions are defined, saved and recalled programmatically by the operator. The choice of preset is based upon the optimal condition and virtually all relevant aspect of the electron column condition and other microscope parameters related to the presets are able to be saved and easily recalled through python scripting, on in the microscope GUI. Another set of 5kV/30kV images is shown in Figure 7, illustrating the gates highlighted at 5kV and looking into M1 at 30kV.

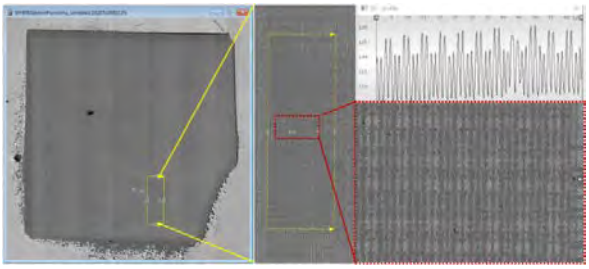

Figure 6. 5kV BSE imaging of ~800x800um delayered area showing P and N doping contrast. Shown is a 49 image montage, each image consisting of 4096x4096 pixels.

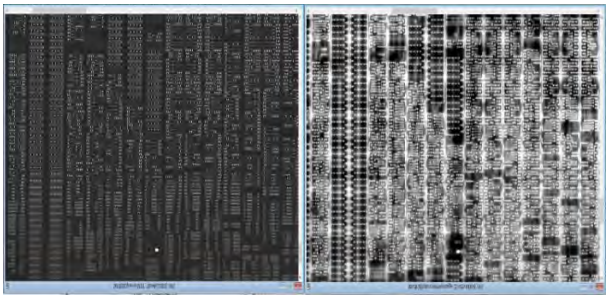

Figure 7. Gate structures highlight at 5kV BSE, shown on the left and looking into M1 in the 30kV BSE image at right. Both images are a montage of 49 images @ 4096x4096 pixels each.

A final image pair from the Opteron case study is a montage acquired from the M1/M2 layer, shown in Figure 8. The 5kV BSE image data highlights the M1 metal layer while the 30kV BSE image montage is peaking through M2 and into M3.

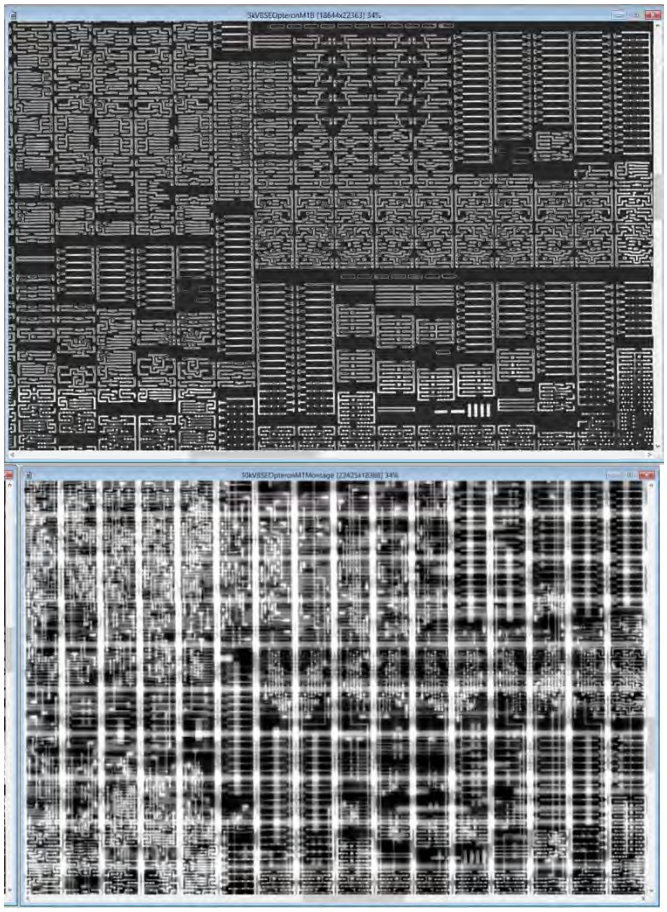

Figure 8. Contact layer is prominent in the 5kV BSE montage image at top while the 30kV BSE image montage is looking into M2/M3 (bottom). Both images are a montage of 49 images @ 4096x4096 pixels each.

2. X-ray Tomography and Microanalysis from Opteron Sample

X-ray tomography is often an initial characterization method in an advanced deprocessing workflow and is a non-destructive process used to visualize the internal structure of an object. X-ray microanalysis is also a non-destructive technique providing spectroscopic data that contributes vital elemental composition information on the sub-micron scale required to correlate structure and device function. Modern x-ray systems incorporate advanced pulse processing and atmospheric thin window technology combined with large active area silicon drift detectors to enable low voltage operation, generating analytical elemental information extracted from volumes on the order of 100nm^3. Integration with FIB-SEM platforms via API control allows x-ray spectral data acquisition to be automated and extended into 3D volumes acquired in concert with delayering and imaging processes. The X-ray microanalysis resolution is limited to the electron beam voltage while the imaging resolution is limited to the X-ray beam spot size, which is nominally a few hundred nanometers in a commercial lab-based X-ray tomography system

The principle of 3D tomography and microanalysis is based on acquiring a stack of 2D images and then using mathematical algorithms to reconstruct the 3D image. Once the 3D image is reconstructed, one can apply advanced image processing algorithms on the raw images to reduce the noise virtually and segment features of the interest. Details of this work can be found elsewhere [1-4].

A Bruker Skyscan 2211system was used for x-ray tomography experiments, which is equipped with an open X-ray source with a high range of power for imaging low and high Z material. All the tomography parameters are optimized through a non-trivial process involving multiple scans. The process enables high X-ray transmission rate and minimum noise in raw images. Figure 9 represents 3D image of a 65nm processor on the left and a 2D virtual slice from the top layer of the processor's PCB on the right.

Synchrotron-based x-ray tomography has also been successfully applied to extract interconnect and trace data corresponding to 14nm node technology [17]. Even in the case of synchrotron based x-ray imaging techniques, the current state-of-art does not match the current and future

technology nodes. In addition, the present synchrotron-based system design accommodates small volumes relative to a typical 1cmx1cm processor. Finally, for academic or commercial investigators, access, scheduling and beam time allotments may limit the pace of the study.

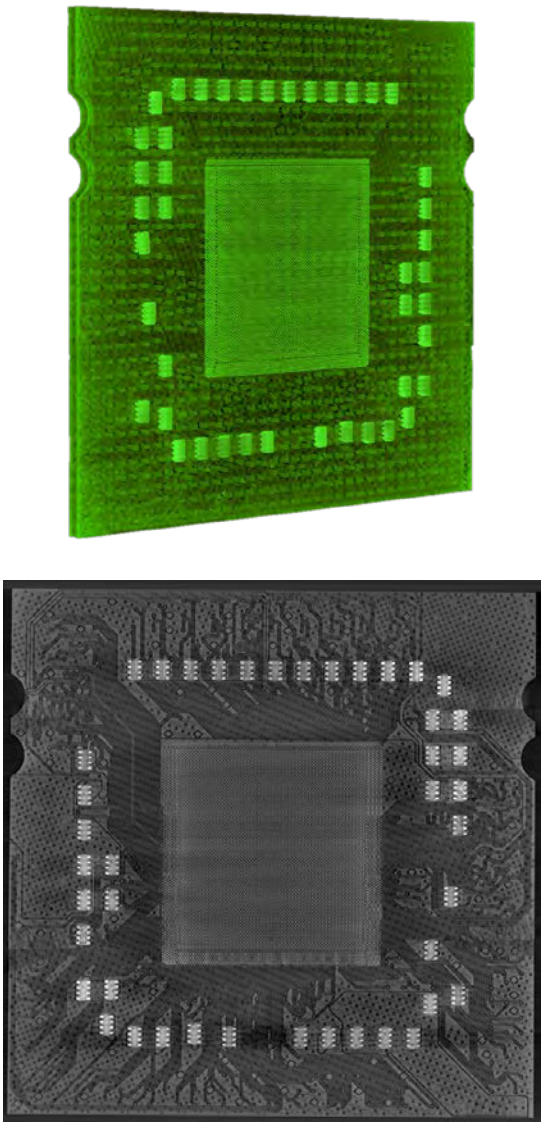

Figure 9. X-ray image of a 65nm processor before FIB-SEM delayering. Image pixel size is 14um.

Despite the short comings of synchrotron-based x-ray 3D imaging, this method has played an important role in the evolution of x-ray based techniques to "non-destructively" analyzed integrated circuits and extract circuit architecture [18-19]. There are efforts underway to develop automated laboratory-based x-ray imaging systems in combination with electron imaging which may point into the future direction for advanced IC deprocessing [20]. If successful, the optimal approach may employ advanced x-ray imaging to acquire upper layer information and SEM-based imaging to extract lower layer data.

3. Case study: Smartcards

Future studies to evolve the steps toward automated IC deprocessing will involve interrogation of smartcards. A smart card (a.k.a., chip card) is any pocket-sized plastic card that contains embedded integrated circuits (ICs) for storing and transacting data. The ICs embedded in the card chip typically include a microprocessor, a crypto coprocessor, memory units, and I/O control units. Simple serial communication protocols, such as ISO7816, are typically used for data communication between card chip and terminal (or reader) [5]. The terminal is usually part of a computing system. Smart cards can be either contact or contactless. Smart cards can provide personal identification, authentication, data storage, and application processing. Systems that are enhanced with smart cards are in use today throughout several key applications, including healthcare, banking, entertainment, and transportation. All applications can benefit from the added features and security that smart cards provide [13-16]. For example, they may provide strong security authentication for single sign-on (SSO) [6] within large organizations.

By far, the most serious problem for smart cards is the attacks that exploit vulnerabilities caused by poor design or implementation of a card or system. For hackers, gaining physical access to the embedded microchip on a smart card is a comparatively straightforward process. Physical tampering [7] is an invasive technique that begins with removing the chip from the surface of the plastic card. It's a simple enough matter of cutting away the plastic behind the chip module with a sharp knife, until the epoxy resin binding it to the card becomes visible. Figure 10 shows the package and assembly of the smart die before

removal of the die. The wire bonds can be seen in the optical image and assist in locating the die in the package.

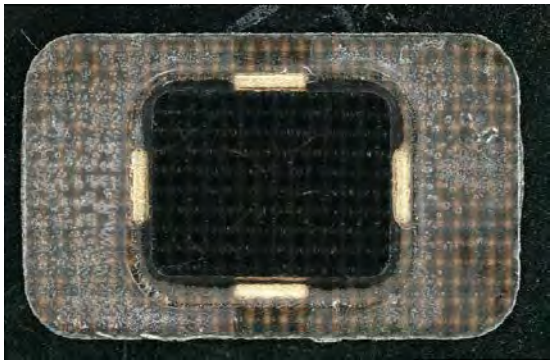

Figure 10. The package and die of a smart card before exposure and extraction of the silicon die.

This resin can then be dissolved with a few drops of fuming nitric acid, shaking the card in acetone until the resin and acid are washed away. The attacker may then use an optical microscope with camera attachment to take a series of high-resolution shots of the microchip surface. Analysis of these photos can reveal the patterns of metal lines tracing the card's data and memory bus pathways. Their goal will be to identify those lines that need to be reproduced in order to gain access to the memory values controlling the specific data sets they are looking for. In general, smartcards are considered as "secure" processors because they employ advanced tamper detection and protection mechanisms. For instance, firmware, passwords, and other important data on a smart card (including the secret encryption key) are generally encrypted and stored in a non-volatile memory. Nevertheless, all these items must be decrypted at some point in order for the smart card to perform transactions. If an attacker can identify the buses that handle decrypted data, then they are vulnerable to probing attacks. Micro-probing can be accomplished with an optical microscope or scanning electron microscope fitted with a sharpened tungsten filament arm that establishes electrical contact with the bus lines on a smart card chip without causing damage to them. Probing may allow dynamic manipulation of CPU instructions as they are being fetched and executed, processor commands to be overwritten,, and reveal valuable information like the clock, power, reset, and input/output signals required to remotely manipulate the processor. Applying out-of-spec voltages or clock signals can also create glitches that allow attackers to access privileged data or states.

Figure 11 shows optical microscope images of separate smart card die that have been extracted from the assembly. The left side image is of the top interconnect layer and wire bond locations. This provides the basic insight into the chip architecture. The right side optical image is a dark field optical microscope image of a smart card die after it has been thinned to 1-3 um of silicon substrate remaining. Using a standard microscope with off axis light, functional blocks of the circuitry are clearly visible. This image can also be integrated into the automated FIB-SEM routine to allow precise navigation to specific circuits of interest.

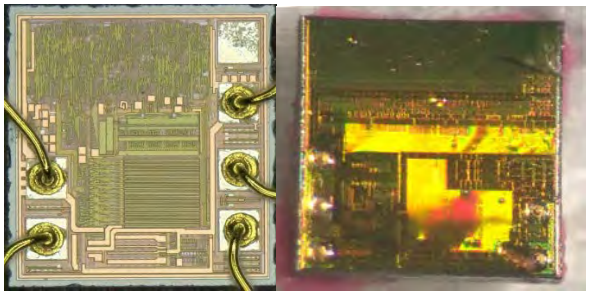

Figure 11. Optical microscope images of the front side of a CDMA sim card die (left) and a dark field image of a separate thinned smart card die.

Aside from the aforementioned physical invasion of the card's electronics, non-invasive attacks that exploit weaknesses in the card's software or hardware can also be used. The typical end goal is to expose private encryption keys and then read and manipulate secure data such as funds. Once an attacker develops a non-invasive attack for a particular smart card model, he or she is typically able to perform the attack on other cards of that model in seconds, often using equipment that can be disguised as a normal smart card reader. While manufacturers may develop new card models with

additional security, it may be costly or inconvenient for users to upgrade vulnerable systems. Tamper-evident and audit features in a smart card system help manage the risks of compromised cards.

Side-channel attack can be used to figure out the key used by the crypto in the smart card chip. For example, differential Power Analysis (DPA) [8] uses statistical analysis of the power used by a smart card during cryptographic functions to determine the secret keys stored on the card. A timing attack [9] precisely times private key operations on a smart card and analyzes this information to determine important cryptographic information.

By examining and taking apart the smart card chip, reverse engineering [10] can be exploited to figure out the internal structure and working principle, and further disclose sensitive information. In future work, we will use the proposed flow to fully RE different types of smart cards in order to understand the security primitives that maybe a candidate to be bypassed by an attacker to extract critical information. Once we know all the vulnerabilities we will look for possible solutions.

Automated Plasma FIB Delayering. The first Smartcard type selected for the automated delayering testing is a microprocessor chip card from Almex Ltd. based upon Basic Card OS with 2k EEPROM and 3DES encryption [25]. The chip was depackaged by removing from the chip and mounting it on a metal backing with epoxy adhesive prior to the automated ultra-thinning process. Future work will explore the CNC adaptive milling directly through the gold contact layer and mesh backing. An image of the chip following depackaging and ultra-thinning is shown in Fig 15. The 2kV secondary electron image depicts the as-received surface condition. A practical concern evident from the image is the presence of various particles randomly strewn on the surface. Obviously, a careful automated delayering process is compromised by the presence of particles and other forms of contamination covering regions of interest and this reality will need to be managed in the future. For this first test, the depackaging and mechanical ultra-thinning process also produced some chipping and cracking on some portions of the microchip. But the vast majority of the chip was undamaged.

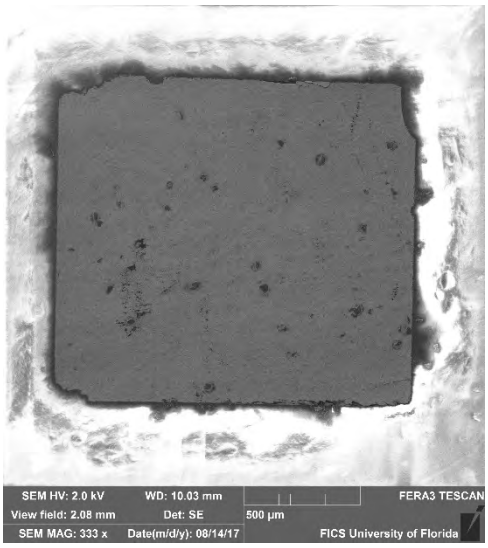

Figure 12. Initial 2kV secondary electron image showing surface condition of as-received die following mechanical backside ultra-thinning.

In Fig 13 we show an overview image of the entire die acquired at 30kV and using BSE detection. Under these conditions the overall structure of the processor is evident. The approximately 400um X 400um in the lower right is the region of the die selected for initial testing of the automated plasma FIB delayering. The increased brightness is due to the initial manual thinning of the backside silicon to establish the starting point for the automated processing. The single crystal silicon typically mills very uniformly and progress can easily be monitored directly in the FIB image to determine when the device structure is exposed. In future, combining the API visualization engine, this process could also be fully automated to define the starting point for GAE plasma FIB automated delayering.

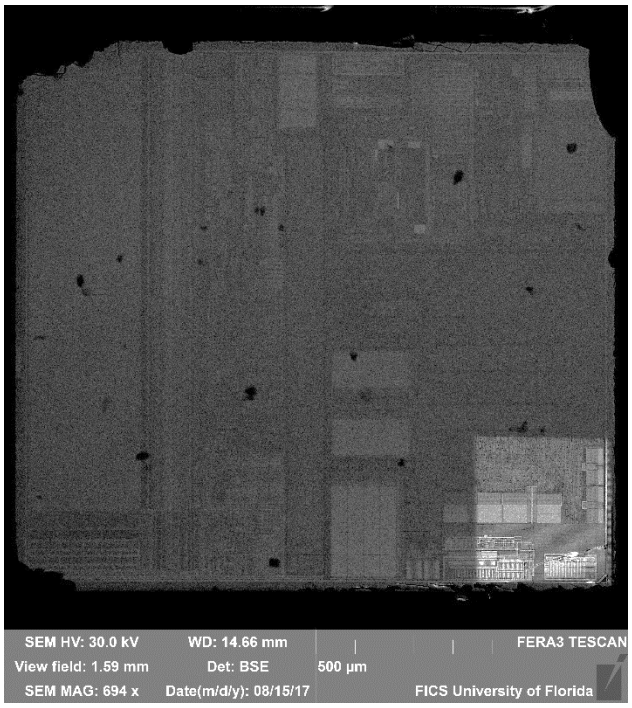

Figure 13. 30kV BSE image depicting the entire Smartcard die structure following manual plasma FIB thinning in the lower right corner in preparation for automated plasma FIB delayering.

The 400um X 400um region was then automatically delayered using GAE delayering chemistry in conjunction with the plasma FIB and automated montage imaging. The instrument and acquisition conditions used in for this result was 300nA@30kV and 400um FOV for the plasma FIB. The delayering cycle is programmatically set to seven minutes. The montage imaging conditions following each delayering cycle was 5kV with BSE detection using a retractable below the lens detector. The FOV for each montage tile was 100um at 4096 x 4096 pixels to generate a 5x5 image matrix. The dwell time per pixel was 1.5us. Following the acquisition of the 5kV montage, the process automatically collects a second montage using the similar image parameters, but at 30kV.

An API script guides the user through the setup process using input prompts and both audio and onscreen printed instructions. A future version of the module will employ a compact GUI driven from the computational visualization engine. The overview of the automated process setup workflow is shown in Figure 14.

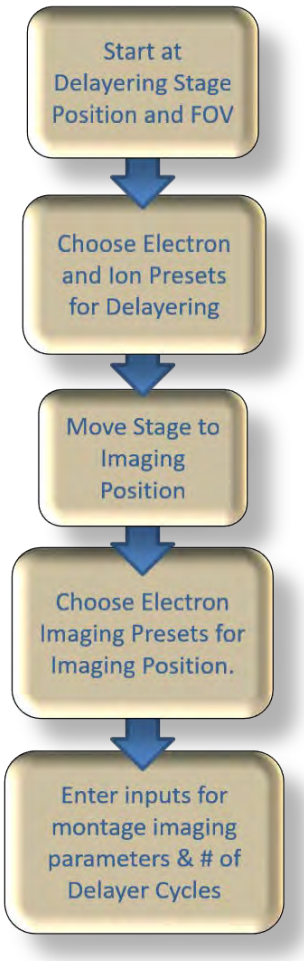

Figure 14. Automated Plasma FIB Delayering Workflow.

The user begins at the coincident point defined by the system, which in this case corresponds to a stage tilt of 55° and nominal 9mm working distance. The user is prompted to verify they are at the coincidence point and safe operation of the gas injection system (GIS) insertion. These are standard operating procedures for any qualified FIB operator. The user chooses the ion conditions for delayering, which is most conveniently defined through user presets which may be saved, updated and programmatically recalled from the API during each delayering cycle.

Next the stage is moved to the imaging condition following each delayer cycle. These conditions

are completely up to the user. Imaging can be completed at the coincidence point and at tilt using In-lens detection. Or the user can move the stage to a zero tilt condition for montage imaging. The latter was done in the results shown here. The stage is automatically moved to zero tilt and 14mm working distance after each delayering cycle. Following confirmation of the imaging stage position the retractable BSE detector is insert and once that operation is complete, the electron imaging begins.

The electron imaging conditions are defined by user preset and programmatically recalled through the API. The stage automatically increments in a serpentine fashion through the matrix using a pre-defined overlap (i.e., 10%) and a matrix size which depends upon the user selected FOV for the delayering area (i.e., 400um). Once all delayering and imaging cycles are complete, the system powers down the electron and ion columns.

A total of 25 automated delayering and image cycles were acquired from the die corner depicted in Fig 13 in the manner described above. An image pair from the beginning of the cycle is shown in Figure 15. The automated process initiated just beyond the transistor contact level. Similar to the previous series, the low kV image provides image data restricted to one layer in depth while the 30kV image data is convolved over ~3 layers. It required approximately 40 minutes to acquire both the 5kV and 30kV image matrices, a total of 50 images.

An image pair taken from the end of the data set cycle is shown in Figure 16. Finally, in Figure 17, we show what is believed to be the first tomographic data reconstruction based upon GAE plasma FIB delayering. The reconstruction is based upon the 25-layer data set taken at 5kV. But the reconstruction is just from a single montage tile, corresponding to row and column 1,2 in the 5x5 matrix. Work to complete a larger reconstruction from the complete montage is in progress. At this point, the process was concluded and another site was selected for study.

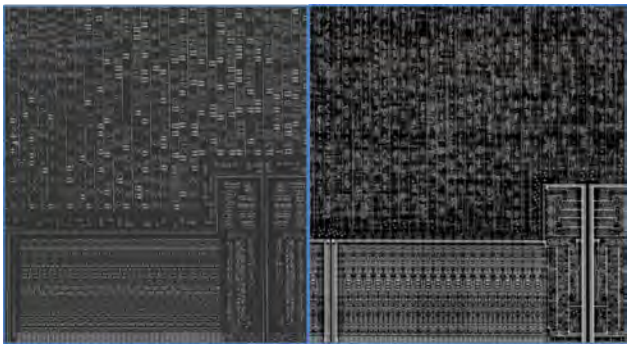

Figure 15. Image pair from Layer 1 from a 25-layer auto delayer data set. The image at left is a 5kV BSE image and the image at right from the same nominal area is a 30kV BSE image. These images represent one tile in a 25-tile image matrix. Each image is 4096x4096 pixels and 1.5us dwell time.

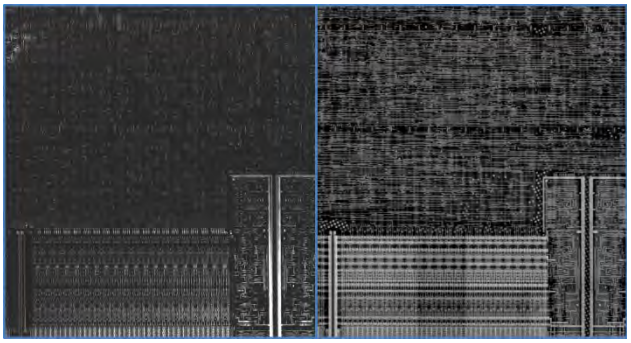

Figure 16. A 5kV/30kV BSE image pair from Layer 25 from a 25-layer auto delayer data set. The same imaging conditions were used as described in Figure 15.

4. Future Work Toward Automation of IC Deprocessing.

We advance the processes previously developed by exploring steps toward automation of imaging and plasma FIB deprocessing through open source Python scripting for custom instrument control. We have shown the ability to automatically perform multiple delayering and imaging cycles at multiple accelerating voltages over a user selected region of interest and user-defined inputs. We have also demonstrated, for the first time, that automated delayering

performed in this controlled and repeatable manner is suitable for tomographic reconstruction. From this stage, the door opens to several extensions and possibilities to potentially automatically delayer multiple ROI in one session, stepping across a die and to incorporate improvements to enhance speed, efficiency and reliability of the process by taking advantage of the feedback loop to the computational visualization and image processing engine.

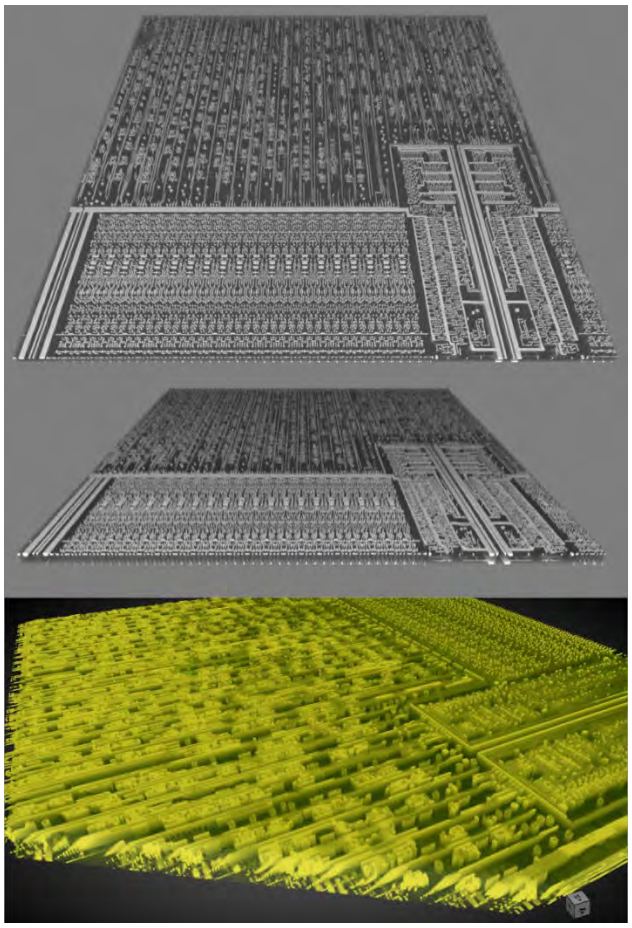

Figure 17. Tomographic reconstruction obtained from a 25-layer automated GAE plasma FIB delayering process following automated mechanical adaptive CNC ultra-thinning to demonstrate an integrated automated workflow.

The open architecture and Python-based API permit rapid custom development of advanced processes involving the plasma and liquid metal FIB-SEM platforms. This architecture permits computationally guided processes to be defined which may include optimized sample strategies such as dynamic adaptive sampling and other "intelligent" acquisition schemes. By coupling programmable deprocessing tools such as FIB-SEM platforms to computational engines via API communication protocols the versatility and opportunities are expanded dramatically. Efficacy and speed are enhanced by the ability to automate not only each individual characterization process, which includes the x-ray tomography data, the digital image data and spectroscopic microanalysis data, but also the data processing for feature extraction, segmentation, data fusion and data visualization.

The next phase of our automation effort will combine the API functionality of the FIB-SEM platform and programmatically interface with the Object Research Systems (ORS) Dragonfly and Dragonfly python API [26]. In this way, a computational image processing and visualization engine is linked with the API control of the FIB-SEM and microanalysis platform. Enormous potential is unleashed through this synergistic coupling. Using Dragonfly as the display and visualization engine, it is possible to combine the x-ray tomography and microanalysis data to define a volume envelope encompassing the package and die, where appropriate. Custom control modules and GUI control interfaces may be defined and operated directly within the ORS interface, as desired. Other image modalities may be easily added to the data structure, such as optical images or photoemission data. Collectively the data cube consisting of multiple image modalities form a local coordinate system which can be fed into and integrated with navigation in the FIB-SEM environment. Because Dragonfly is not just the programmable platform for automated routines, but also a feature-rich interactive application, user can interactively monitor incoming images that are being aligned, stitched and composited in near real-time and also intervene during the execution of data collection. Users can perform near real-time measurements and data assessments that were

not programmed a priori, and those results can be applied to direct subsequent steps in the deprocessing workflow.

Beyond collocating image and volume data, the interfacing of the APIs enables bi-directional processing and feedback, which is the most important element of this combination. The image processing engine can function as a distributed system coordinator, taking image data as it becomes available and performing any required distortion correction, segmentation, image stitching, montage display and visualization in near real-time. Image data may be validated and data acquisition schemes may be optimized based upon near real-time data analysis.

As an example of other possibilities, optical image data commonly provides a first level outline of the device which is useful to identify the location of memory arrays and other repeating block structures. Often, it is not necessary to SEM image each individual element of the array. The optical data, coordinated through the computational image processing engine (Dragonfly API) may direct the microscope to navigate to the block corners, refine the location of the block locations with the SEM imaging, and proceed to image selected cells at the required resolution, leaving the rest of the structure to be "filled in".

The processing may be carried further, by developing segmentation and extraction to GDSII within the same environment. There are existing software products which can accomplish reconstruction of the GDSII layout. Some are commercially available, such as Pix2Net [11] and others are internal non-commercial products, such as ARES [12]. One of the advantages of the schema being proposed here, is the open architecture and the utilization of pre-existing modules based upon Python scripting. This includes such modules as GDSPy (for GDSII creation) [13] and TomoPy [14]. Python is also easily extensible to multi-core processing and even adding multiple computer processing on the fly. The interface is not limited to Python scripts, but Matlab programming may also be called, which for example can be applied to implement processing of compressed sensing, giving an appropriate sampling schema [15].

This element of the deprocessing workflow utilizes an image processing platform which also incorporates an open API for Python scripting. This API empowers not just feature extraction, image filtering, and reporting, but also 3D registration of images collected from a variety of data modalities comprised of different pixel sizes and spatial resolution into one common coordinate system for co-visualization and co-analysis of the multi-layer data set. Importantly, the end user is not limited by specific vendor software.

Conclusions

In this work elements for an automated reverse engineering process are described. Automated CNC adaptive backside ultra-thinning is paired with automated plasma FIB gas-assisted etch (GAE) delayering with automated montage imaging to produce low kV and high kV BSE data. A tomographic reconstruction based upon automated GAE plasma FIB backside delayering is demonstrated for the first time.

Different imaging modalities including optical, X-ray tomography and microanalysis, and SEM images are contributors to the final dataset. The low mag optical images reveal the large blocks and their locations in the die, while X-ray images help to understand the internal structure down to 700 nm resolution and finally SEM images will represent all details of a die with 1 nm resolution.

The coupling of plasma FIB-SEM deprocessing of devices with automated backside sample preparation using advanced adaptive computer guided backside milling provides additional key advantages in the deprocessing workflow [15]. This process enables greater success rate on lower

metal interconnects and high-density transistor levels while accommodating non-planar device geometry on the sub-micron scale. Ultra-thinning in this manner significantly reduces the amount of time and manual expertise required while providing an excellent controlled starting surface for deprocessing [16], making it possible to access larger areas of the chip card to be de-processed with increased success rate, resolution and uniformity. Backside deprocessing also provides the potential to maintain a "live" device and conduct in-situ electrical testing.

Computationally guided microscopy, as currently being defined and developed, holds the potential as a dynamic and extensible tool to analyze image data dynamically in near real-time send interactive commands to the FIB-SEM platform to validate, as well as direct, data acquisition. Such an automated tool can be used to reverse engineer integrated circuits and reveal the information for studying the vulnerabilities and introducing new primitives based on the new information.

A common Python scripting API accessible across various tool sub-systems creates enhanced synergy and integration potential while permitting customized and rapid process development. Python-driven automated feature detection and segmentation can be executed on the image processing platform while the sample is still in the microscope, and, therefore, readily coupled to subsequent Python-driven image acquisition. This creates a closed feedback-loop for image interpretation and programmatic directed image acquisition recipes, which is a prerequisite for full automation and computational microscopy.

References

[1]. N. Asadizanjani, et. al. "Non-destructive PCB Reverse Engineering Using X-ray Micro Computed Tomography." in 41st International Symposium for Testing and Failure Analysis (November 1–5, 2015). ASM, 2015.

[2]. N. Asadizanjani, M. Tehranipoor, and D. Forte, 2017. PCB Reverse Engineering Using Nondestructive X-ray Tomography and Advanced Image Processing. IEEE Transactions on Components, Packaging and Manufacturing Technology, 7(2), pp.292-299.

[3]. N. Asadizanjani, 2014. 3D Imaging and Investigation of Failure and Deformation in Thermal Barrier Coatings Using Computed X-ray Tomography.

[4]. S.E Quadir, J. Chen, D. Forte, N. Asadizanjani, S. Shahbazmohamadi, L. Wang, J. Chandy, M. Tehranipoor, "A survey on chip to system reverse engineering" ACM journal on emerging technologies in computing systems (JETC), 2015

[5]. Hocker III, L.O., Onset Computer Corporation, 1997. UART protocol that provides predictable delay for communication between computers of disparate ability. U.S. Patent 5,682,508.

[6]. De Clercq, J., 2002. Single sign-on architectures. In Infrastructure Security (pp. 40-58). Springer Berlin Heidelberg.

[7]. Smart Card Technology and Security. http://people.cs.uchicago.edu/~dinoj/smartcard/security.html

[8]. Kocher, P., Jaffe, J. and Jun, B., 1999. Differential power analysis. In Advances in cryptology—CRYPTO'99 (pp. 789-789). Springer Berlin/Heidelberg.

[9]. Dhem, J.F., Koeune, F., Leroux, P.A., Mestré, P., Quisquater, J.J. and Willems, J.L., 1998, September. A practical implementation of the timing attack. In International Conference on Smart Card Research and Advanced Applications (pp. 167-182). Springer Berlin Heidelberg.

[10]. Kumagai, J., 2000. Chip detectives [reverse engineering]. IEEE Spectrum, 37(11), pp.43-48.

[11]. http://micronetsol.net/

[12]. https://www.blackhat.com/docs/us-15/materials/us-15-Thomas-Advanced-IC-

Reverse-Engineering-Techniques-In-Depth-Analysis-Of-A-Modern-Smart-Card-wp.pdf.
[13]. https://readthedocs.org/projects/gdspy/
[14]. https://en.wikipedia.org/wiki/TomoPy
[15]. E. L. Principe et al, "Plasma FIB Deprocessing of Integrated Circuits from the Backside", FICS Research Annual Conference on Cybersecurity, March 7-8, 2017
[16]. R. Chivas et al., "Adaptive Grinding and Polishing of Silicon Integrated Circuits to Ultrathin Remaining Thickness" ISTFA 2015
[17]. Wolfgang Rankl and Wolfgang Effing, "The Smart Card Handbook" third edition,
[18]. H. Bar-El, "Known Attacks on Smart Cards" White paper, http://www.infosecwriters.com/text_resources/pdf/Known_Attacks_Against_Smartcards.pdf
[19]. Helfmeier, C., Nedospasov, D., Tarnovsky, C., Krissler, J. S., Boit, C., & Seifert, J. P. (2013, November). Breaking and entering through the silicon. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (pp. 733-744). ACM.
[20]. M. Tehranipoor, "Physical Attacks and Tamper Resistance", ECE6095: Hardware Security & Trust University of Connecticut ECE Department
[21]. Mirko Holler, et al., "High-resolution non-destructive three-dimensional imaging of integrated circuits", N AT U R E | VO L 5 4 3 | 1 6 M ar C H 2 0 1 7
[22]. Lavely, Eugene M., Yi-San Lai, Krishna Gopalakrishnan and Rick Thompson, "3D Element-Specific Bare Die Reconstruction with X-ray Fluorescence Tomography," GOMACTech2012.
[23]. Lavely, Eugene M., Yi-San Lai and Krishna Gopalakrishnan, "Joint Inversion of Multi-Mode Data for IC Estimation," GOMACTech2013.
[24]. http://www.edn.com/design/test-and-measurement/4458370/Fake-ICs--Another-weapon-in-their-detection.
[25]. https://secure.smartcardsource.com/zc314-basic-smart-card.html
[26]. http://dev.theobjects.com/dragonfly_3_1_release/contents.html)