Electronic Packaging and Interconnect Tool Box for Secured Smart Systems Packaging

Bernard Candaele
Thales
Gennevilliers, France

Abstract
Security has become a vital part of electronic products as they handle sensitive data in uncontrolled environments and as they face more and more content protection issues. The paper will introduce the security challenges for smart systems and describe a new security tool box and smart packaging which can be obtained by introducing 3D Nano-materials printed envelope (several meters electrical performance with spacing capability of 50µm), 3D embedded devices into electronic modules (active die in PCB) and multi-die WLP System in Package, with active anti-tamper sensors as well as the combination of all, focusing on both the security performance assessment as well as the manufacturing process.

Introduction
Any type of electronic interconnected systems is now vulnerable, not only the IT ones. We could take the example of an automotive system. It is built with a complex interconnect system, or even several of them dealing with Powertrain, Chassis, Body Comfort and Infotainment. Questions arise now about possible remote attacks (both long distance and nearby) with malicious applications at a large scale of cars, malicious contents, eavesdropping of remote connection or malicious authentications. We need to mention also local attacks, such cloned keys, malicious firmware updates, malicious device connection – as today you get access to some part of your car system with your smart phone – and identity usurpation. The attacker will use known and unknown vulnerabilities in the system. This also applies to the numerous interconnected systems in many application fields from health to automotive, smart energy, Industry 4.0, governmental, security or financial solutions, to name a few.

Security shall be provided at the different layers, available at the several levels of the system: the application, trust management, connectivity, software stacks, operating environment and OS, and hereby hardware solutions. When a lot of protection technologies have been developed at the IC chip level with secure microcontrollers and others, the paper addresses the protection and detection technologies to be made available by the Electronic Packaging and Interconnect community and its supply chain and to get more tamper-resistant electronic system boxes and packages. We are concerned by the hardware attacks from the threat actors with a history of intent and capabilities to persistently target your system, such highly capable groups of individuals (i.e. industrial spy hackers, ethical and elite hackers), organized crime or some intelligence services. The hardware attacks are about opening the box such as by mechanical means, lasers or chemical means, about visual inspection such as X-ray 3D tomography, endoscopes, electronic or optical microscopes, about electromagnetic probes, about power consumption static or differential monitoring (e.g to guess a RSA private key), acoustics, electromagnetic emission readings and many others. Once the attacker gets access to the hardware system and some of its data, they are then able to access to other sensitive parts of the full value chain of the system.

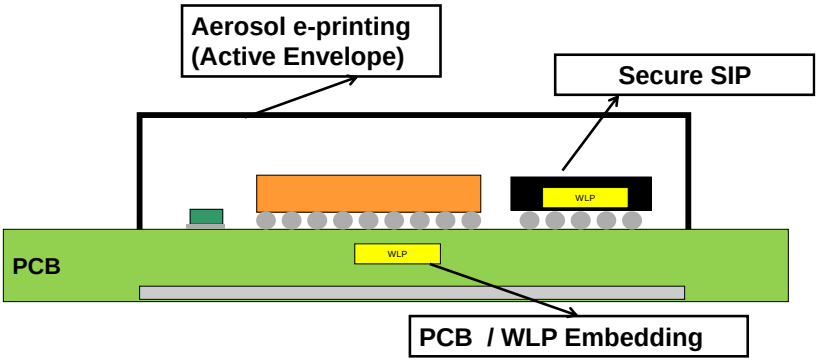


Figure 1 : Schematic view – EP&I Tool boxes to provide anti tamper protection

A smart electronic module is considered for the security studies, in order to evaluate the security level reached by the different security improvements, as shown in Figure 1 including:

- A cap on top of the PCB, connected to a security monitor and able to detect intrusion,
- Die embedded in the PCB, with a secure loop to detect security attacks.
- A secure SiP, protected plain text data from snitching,

The smart system architecture is representative of targeted secure architectures, with an applicative processor, other electronic functions and a security micro-controller. Sensors underneath the envelope are active sensors such as temperature and voltage ones, but also pressure sensor, chemical ones, gyroscope and accelerometer, etc.

Enabling Electronic Packaging and Interconnect technologies

Three main innovative technologies are introduced and reported in the paper:

- Nanomaterial aerosol jet printing to build a resistive sensor mesh in a protective cap;
- Die embedded in the Printed Circuit Board and its shield;
- Wafer-level SiP to integrate a multitude of chips and passive components into a single eWLB package, using molded reconstituted wafer and Re-Distribution Layers (RDL) as connectivity elements plus safety meshes and anti-tampering features.

3D nano-ink printed cap

Aerosol Jet Printing (AJP) is a non-contact direct (without mask) deposition system which is capable of producing high resolution conductive or non-conductive features onto 2D and 3D surfaces. The technology is based on atomizing inks (containing suspended nanoparticles) by the flow of a gas (nitrogen). The stream of aerosols thus generated, can then be further densified and guided to a nozzle system where it is aerodynamically focused and deposited onto the substrate. Figure 2 depicts a schematic diagram of the process. Once the deposition is finished a straightforward post processing (thermal sintering) is employed to cure the material and produce the final structures.

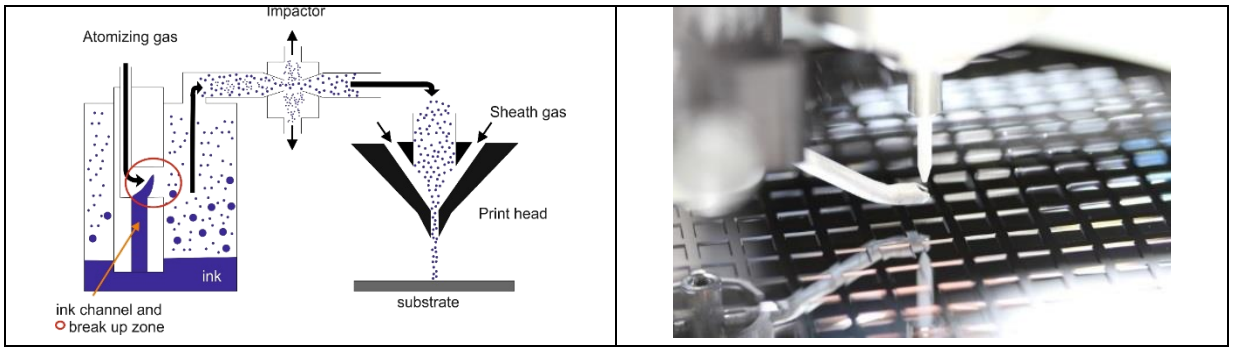


Figure 2 : Schematic process flow Aerosol Jet Printing technology (left) and picture showing the printhead, shutter and substrate [1]

The ability of printing conformal electronics on non-planar substrates has been opening up new opportunities for the development of highly integrated electronic components. Among many established or development applications of AJP technology are: printed antennas, 3D interconnects, die attach, printed transistors, sensors, fuel cells, solar cells and displays. Moreover, the technology is scalable and AJP systems are available in multi nozzle versions, suitable for large volume production.

AJP is one of the technologies for the rapidly growing field of printed electronics. The primary advantage of printed electronics is the very low cost of manufacturing in high volume and no tooling which is competitive for prototypes or low volume. This has encouraged many activities in research and development to replace, partially or fully, the conventionally manufactured electronics by printed electronics. The considered applications are photovoltaics, OLED display and lighting, new transistor structures, e-paper displays and displays.

As a solution [7] we propose to use nanoparticle based aerosol-jet-printing AJP technique to create very thin mesh like circuits inside a 3D cap or a System in Package (SiP). Several metal particle inks for aerosol jet are available on the market for different applications and have been tested to define suitable materials for an active envelope sensor structure. Due to the good process-ability and resistance stability, Ag nanoparticle inks are promising materials and the most mature conductor material

In the proposed method a polymer thin film is used as an insulation layer between the conductive multilayers and the interconnect vias are opened by a fine-tuned laser ablation process. The entire process for conductive multilayer fabrication and via filling is performed by the AJP technique.

The development of the active envelope includes several and successive steps including:

- AJP enables fine line deposition (<20µm) of metal particle inks on flat surfaces whereas the fabrication process and technical results are strongly depending on the selected ink and substrate materials and surface roughness as well as on the applied pretreatment technologies. With this work we explored the deposition of a commercial available silver nanoparticle ink on thin dielectric coating. Therefore the printing process for Ag Nanoparticle Ink was set up; it required the adjustment of AJP techniques to fabricate relevant electrical circuits, and the development of interconnection techniques between the printed electrical conductive mesh layers. Both flat and 3D curved sides printing are needed;
- The identification of suitable substrates and then the selection of suppliers for substrate fabrication (Flat and 3D parts). The dielectric is deposited using a CVD process in a vacuum chamber close to room temperature. Thermal cycling tests are performed, to check long term stability, as well as that no delamination appears. Several meters long meander structures have shown technology feasibility of the AJP process. Pull and shear tests have been performed to achieve a base to compare the adhesion of Ag ink on different substrates and dielectric layer. Long term heat treatment (125°C, 1000h) has demonstrated good resistance stability;
- A laser via drilling process has been established, with plasma treatment. Such fabricated vias are about 50x200µm. Related interfaces have been pictured and additional thermal cycling tests have been done to check their manufacturability and their reliability. Opening the via in the dielectric is performed by laser ablation without damaging underneath layers.

All scientific details about the related AJP process will be published in the coming months in an industry journal.

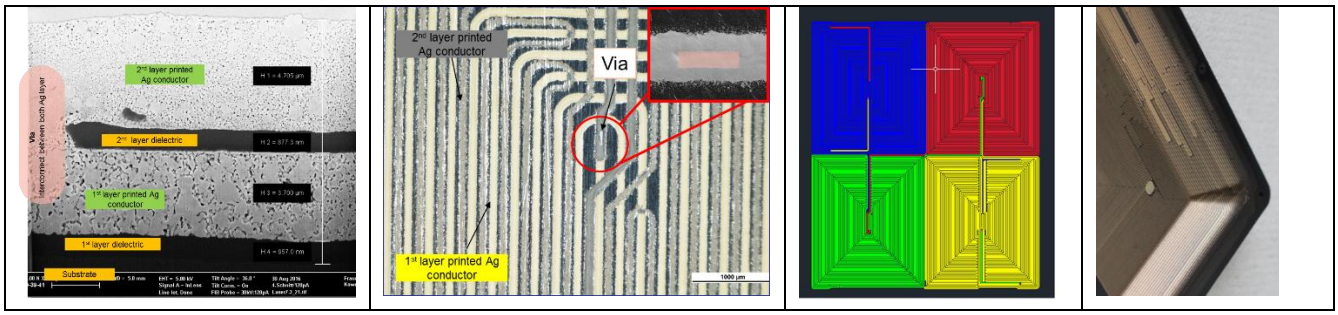


Figure 3 : 2 layers interfaces, Double-layer mesh fabrication, Mesh design and Testing 3D corners

Figure 3 above shows the several building blocks of a nano-inked based meshed 3D cap,

- The 2 conductive interconnected layers and both their underlying and intermediate dielectric layers
- A bottom plus middle layer mesh, with via interconnect
- The design of the interleaved meshes in the cap
- Investigating printing in the corners of a full cap

Table 1: Some characteristics of the realized 3D cap test vehicles

Mesh length	several meters
Mesh wire width / space	150 / 250 µm
Via size	opening inside the conductor
Resistance value	+/- 5% change from cap to cap

Some of the achieved characteristics with the Cap test vehicle are reported in Table 1. Several meshes have been laid out in the envelope. The realized 3D Cap is then assembled to the PCB.

Limits have been observed with today's available printing equipment. First to speed up the manufacturing time multiple heads would be useful. Second to print angle and slopes, it would be useful to move the table with good accuracy. However the nano-ink Aerosol Jet Printing is a promising solution to build the smart, flexible and anti-tamper protection cap.

Embedded die in PCB

Embedding a bare die and passives into a printed circuit board allows a very dense interconnection, and it has opened the way for 3D integration [2]. A single layer of embedded chips already provides room for passives or other SMD components on top, a multi-level embedding of components creates real 3D packages which are a must for the next big wave of Internet of Things (IoT). The technology is going to System in Package and the question today is how far you can go in miniaturization and how much of complexity and density you can handle.

An embedded component technology from the PCB partner has introduced a powerful solution for heterogeneous integration (combining silicon devices made with different technologies or other semiconductor technologies, with standard components on one substrate). Embedded PCB [3] gets a lot of advantages such as high density interconnect,

excellent high frequency behaviour, good thermal properties, etc. The technology is based on top end HDI technology that will be further developed to a technology level required by the interconnect density of the complex embedded chips. An advanced semi-additive technology and a novel embedding technology are the main topics of this development. Therefore embedded packaging requires Cu depositions on passive chips and post processing of bare dice: wafer must be tinned and receive RDL with copper finish.

An innovative solution is being proposed and developed by combining two major packaging technologies [6] in order to achieve a higher level of miniaturization and to find a cost effective solution for its implementation. The embedded component packaging technology from the industry company and the Fan Out wafer-level packaging (FOWLP) technology from another industry company are the candidates which are evaluated and further developed to show a system in package (SiP) concept which can handle different components and interconnect complexity in one module [5]. The FOWLP technology provides component in fan out solutions and provides the capability to combine two or more dies in one package to handle ultra-high density interconnection. The embedded component technology is able to package passive, active and FOWLP components in a module construction, which can be used, for this case, in security modules as shown in Figure 4 below.

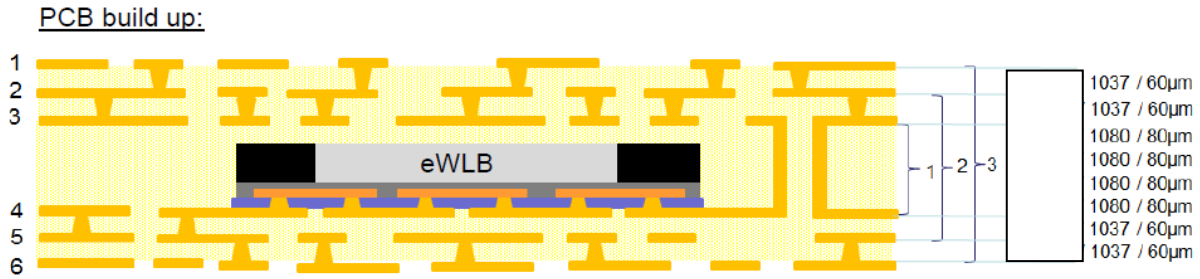


Figure 4 : Building WLB embedded in PCB (compliant with embedded passive chips)

The embedded component packaging technology production starts with the printing of an adhesive material partially on the surface of a copper foil. Components are assembled with the face side down (via redistribution layer of the component: the RDL) into the printed adhesive. A curing step after the assembly hardens the adhesive and fixes the components to the copper foil.

The integration of the component into the PCB –the embedding Core - is completed by a following pressing step. For isolation prepreg material is surrounding the components. An ultra-low transmission loss multi-layer circuit board material has been the main PCB material used to build these test vehicles. It is a halogen-free material with a Tg of 170°C and CTE in the X/Y direction between 14 and 16 ppm/°C.

Figure 5 : Realized SoM (System on Module) module and related PCB stacked layer

The interconnection between component pads and PCB is made by a laser drilling process followed by copper plating and structuring. For embedded component technology mass production different laser parameters have been evaluated [4] and qualified for several component sizes/adhesive thicknesses. To finish the complete PCB build-up 4 additional pressing steps are performed. At the end of production, the finished test vehicle is a 10 layer PCB with five pressing steps in total as shown in above Figure 5. This build up has been chosen and defined to simulate the final product of a security project which is also produced in five pressing steps (16 layer PCB) and the same FR-4 material.

As a secure application we first imagine a secure microcontroller (MCU) to be embedded inside the embedded PCB package. The MCU will monitor the different sensors in the secure box as well as manage the several resistive meshes that surround the closure for protection. The additional stacked µvia PCB layers are used to build protecting meshes to be connected and to be mapped in the back side of the PCB. This step requires a very good yield HDI manufacturing line, to

be able to process the unbalanced copper PCB and very dense meshes. Then we imagine a SMT BGA or SiP device mounted on the top PCB.

Today restrictions are the size of the embedded die – 5 x 5 mm2. Actions are going on to develop improved embedded component packaging for larger dies. The program is now engaged in reliability assessment and improvements. Also one of the next actions is to better specify test vehicles for new generation embedded as part of IPC 7092.

Multi-die SiP

A short outlook of the considered System in Package is proposed as this is less a topic for IPC APEX up to now. We address embedded Wafer Level Ball Grid Array (eWLB) a packaging technology for IC (integrated circuits). The package interconnects are applied on a temporary/artificial wafer made of silicon chips and a casting compound.

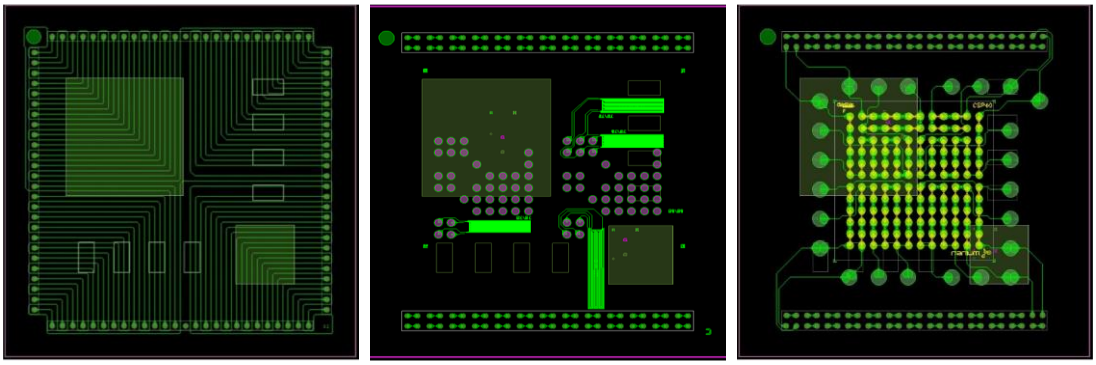


Figure 6 : Multi die SiP with PoP to secure

SiP (System in Package) is the next integrated generation for SoM (System on Modules) or COM (Computer on Modules). The need is to increase the integration of Fanout eWLB with 2 layers as PoP (Package on Package). In the multi-dies test vehicle, Figure 7, we assess several variants in the RDL Redistribution layer. One is with a mesh plus a thin film shielding. A second examines high density down to 10/10µm. A third provides land pads for PoP and asymmetric 3D construction.

Test vehicles have been prototyped and are both under functional and reliability testing. The next action on the agenda is also to define advanced anti-tamper structures.

Considered Use cases and EP&I protection tool box roadmap

The proposed technologies will get different implementations depending of the final product form factors. We identify three or four categories of equipment or products:

1. Data server or gateways. It is about the protection of the (de) ciphering equipment part. They get to process very high data bandwidth, with strong power dissipation constraints and a large domain surface to protect. Generally, the equipment is in controlled facilities or offices, they may require low or medium anti-tamper protection
2. IoT nodes, wire or wireless radio portable modules or even smart phones. The surface to protect is small; anyway the products get very strong small physical size constraints, also to introduce anti-tamper protection. As the node is remote, there are more and more high anti-tamper demands. The full products may get as well strong mechanical drop/shock stresses, as well as low power autonomy requirements. A lot of embedded products are today introducing SoM (System on Module) or COM (Computer on Module) as a small daughter board on a large carrier board. COM offers in a dense module a computing system for embedded applications. It includes the CPU processor or microcontroller chip, the companion chips for power management and clocks, main I/O controllers plus the memory chips and RF connectivity interface
3. Above IoT nodes made with SiP System in Package. SiP is a more compact version of above COM or SOM modules. Leading microcontroller component providers are now introducing such SiP. The SiP integrates several bare dies such as the processor itself, companion chips, embedded passives in the interposer. Flash memories may be added as PoP (Package on Package). SiP reduces the complexity of the underlying PCB. Anyway in several applications SiP may require anti-tamper protection.
4. This category deals with key generation modules or key firmware transfer devices for applications not using remote download. These products get to protect data to store them securely, anyway they are remote. Generally, the protected area is with a small surface.

One of the factors conditioning the attacks performed against devices with security envelopes is the size and form factor of the product. Depending on the scale of the device, the attack could be different, and the difficulty may increase or decrease depending on such a scale.

The anti-tamper physical protection has to guard the application payload such as key storage, key fill resources, crypto algorithms if not public ones, or sensitive application code programs and FPGA bit-stream storage in some cases.

The anti-tamper platform or secure box, which applies to the four above use case categories, gets common embedded resources to guard. It is about inside intrusion/opening sensors, temperature and voltage range sensors as available as well in secure microcontroller IC, Tamper detection and zeroise action control, backup energy source and sensitive anti-tamper program code (secure boot, auto-test, etc).

The anti-tamper physical protection has to be active. Upon intrusion or opening or environmental threat detection it activates a zeroise signal and generates a security event log. It detects environmental conditions outside the normal operating range for temperature and voltage. The zeroise feature should erase keys, passwords, sensitive data flow or sensitive parameters.

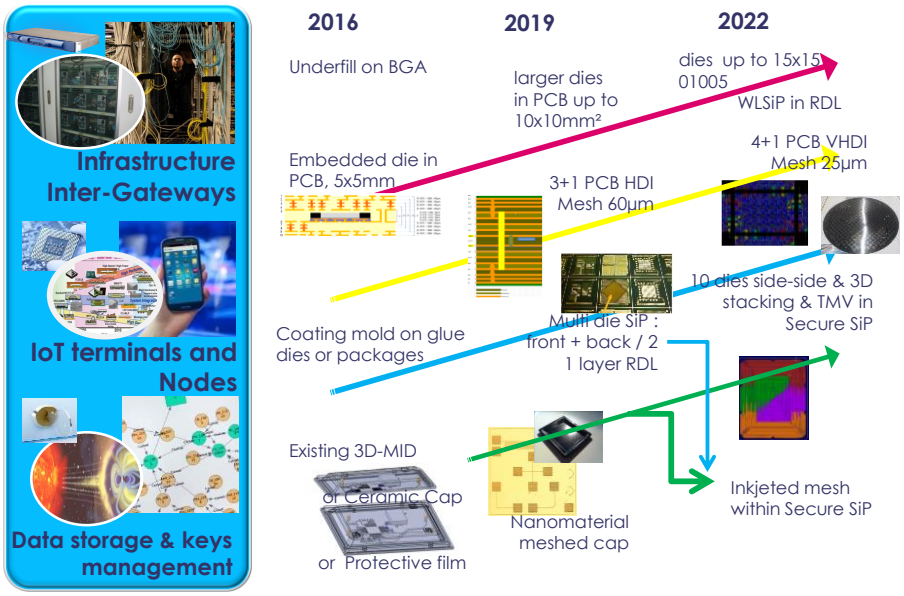


Figure 7 : Considered use case categories and enabling EP&I protection technologies roadmap

As it is a long history of competition and never ending race between hackers and resistance with new countermeasures, the set of technologies that we consider, will require further improvements. Each of the considered technologies in this paper presents opportunities to improve, to further integrate and miniaturize. The related roadmap is shown in the Figure 7.

As a next step a Protection Profile (PP) is proposed for secure boxes and secure electronic modules [8]: it shall be used as part of a certification process according to Common Criteria for Information Technology Security Evaluation and EAL4 + (Evaluation Assurance Level). We refer to the technical requirements in use by the European market as regulated by the SOGIS for "Hardware Devices with Security Boxes" a Technical Domain related to products from a series of discrete parts on one or more printed circuit boards whereby significant proportions of the required security functionality depend upon a hardware physical envelope with counter-measures against direct physical attacks. The PP defines the security properties of an envelope encapsulating an electronic module (also denoted as “payload”). For The Target of Evaluation (ToE) consists of both the envelope and the electronic device protected by the anti-tamper envelope or package. All hardware, embedded software, firmware, and data components within the TOE get to be protected. During the operation of the TOE, unauthorized attempts at physical access, use, or modification shall be detected leaving “visible” signs and appropriate actions will be taken to protect the TOE assets, including critical security parameters of the anti-tamper mechanisms.

Summary and Conclusions

New products in the IoT and connected world will require secure box and anti-tamper protection beyond the solutions available within secure microcontroller IC or in modern secured processors and FPGA. Several alternative and complementary technologies were presented in this paper, tested and need to be further developed by our IPC communities. The actions are to select and customize the related security box with the appropriated form factor and protection mechanisms depending on the considered IoT products: data servers and gateways, IoT nodes and terminals or security resources devices. Three enabling technologies are:

- A new fabrication process for additive manufacturing of the active Cap envelope. It is based upon nanomaterial aerosol jet printing to build a resistive sensor mesh in the protective cap. This requires fine pitch with good

electrical conductive paths on relevant surface materials with good adhesion within controlled and reproducible parameters;

- Die embedded in the Printed Circuit Board and PCB network based shield;
- Wafer-level SiP to integrate a multitude of chips and passive components into a single eWLB package, using molded reconstituted wafer and Re-Distribution Layers (RDL) as connectivity elements plus safety meshes and anti-tampering features.

Test vehicles have been built both as technology vehicles and as shown in the Figure 1 system test vehicle. The test vehicles have undergone reliability testing that showed that the enabling technologies can be manufactured provided there are some improvements. The vehicles are still in the hands of the security evaluation lab and first results should be introduced shortly.

Acknowledgements

The author would like to express its thanks to its partners in this research and development program:

T.Schwartz and H.Stahr AT&S. Loeben, Austria for their contribution on embedded die PCB
F.Roscher and N. Saeidi, Fraunhofer ENAS Germany for the nano ink multilayer Mesh
A.Cardoso and E.Fernandes, Nanium SA, Vila do Conde, Portugal for the multi die WLP SiP
Ch. Hannauer and C.Marron Thales Communications & Security, Gennevilliers, France, for anti-tamper hardware architectures
M.Brizoux and A. Lecavelier des Etangs-Levallois, Thales Global Services, Velizy, France for manufacturability and reliability analysis

The program is performed in the framework of FP7-SEC UNSETH (Grant Agreement No. FP7-SECU-312701).

References

[1] Optomec Inc

[2] http://cordis.europa.eu/project/rcn/111493_de.html

[3] http://www.ats.net/wp-content/uploads/2013/07/ AT_S_Hermes_Newsletter_2009.pdf A.Kriechbaum, H.Stahr, M.Biribauer, N.Haslebner, M.Morianz, M.Beesley: “Embedded Component Packaging Technology”, AT&S Semicon Europa October 2011 Conference Paper

[4] J. Perraud, A. Lecavelier des Etangs-Levallois, A.Grivon, M. Brizoux: SAM and IR microscopy to characterize die embedded in PCB“, SSI March 2016 Conference presentation

[5] Steffen Kröhnert & Gerhard Schmid , Leading, Edge Embedding Technologies Combined, Semicon Europa October 2014

[6] Timo Schwarz, Hannes Stahr , Andre Cardoso, Elisabete Fernandes, Aurélien Lecavelier des Etangs-Levallois, Michel Brizoux , Merging of packaging technologies for highly integrated embedded modules, ESTC September 2016, Grenoble

[7] Frank Roscher, Nooshin Saeidi, Tom Enderlein, Franz Selbmann, Maik Wiemer and Thomas Gessner, A new approach for 3D Integration based on printed multilayers and through polymer vias, SSI March 2016, Munich.

[8] http://www.epoche.es/16iccc/unseth.html Miguel Bañón , "The challenge of methodically opening smart tamper envelope technologies. The UNSETH project", 22 September 2016, International Common Criteria Conference 2015, Windsor, United Kingdom.

Electronic Packaging and Interconnect Tool Box for Secured Smart Systems Packaging

Bernard Candaele

THALES

bernard.candaele@thalesgroup.com

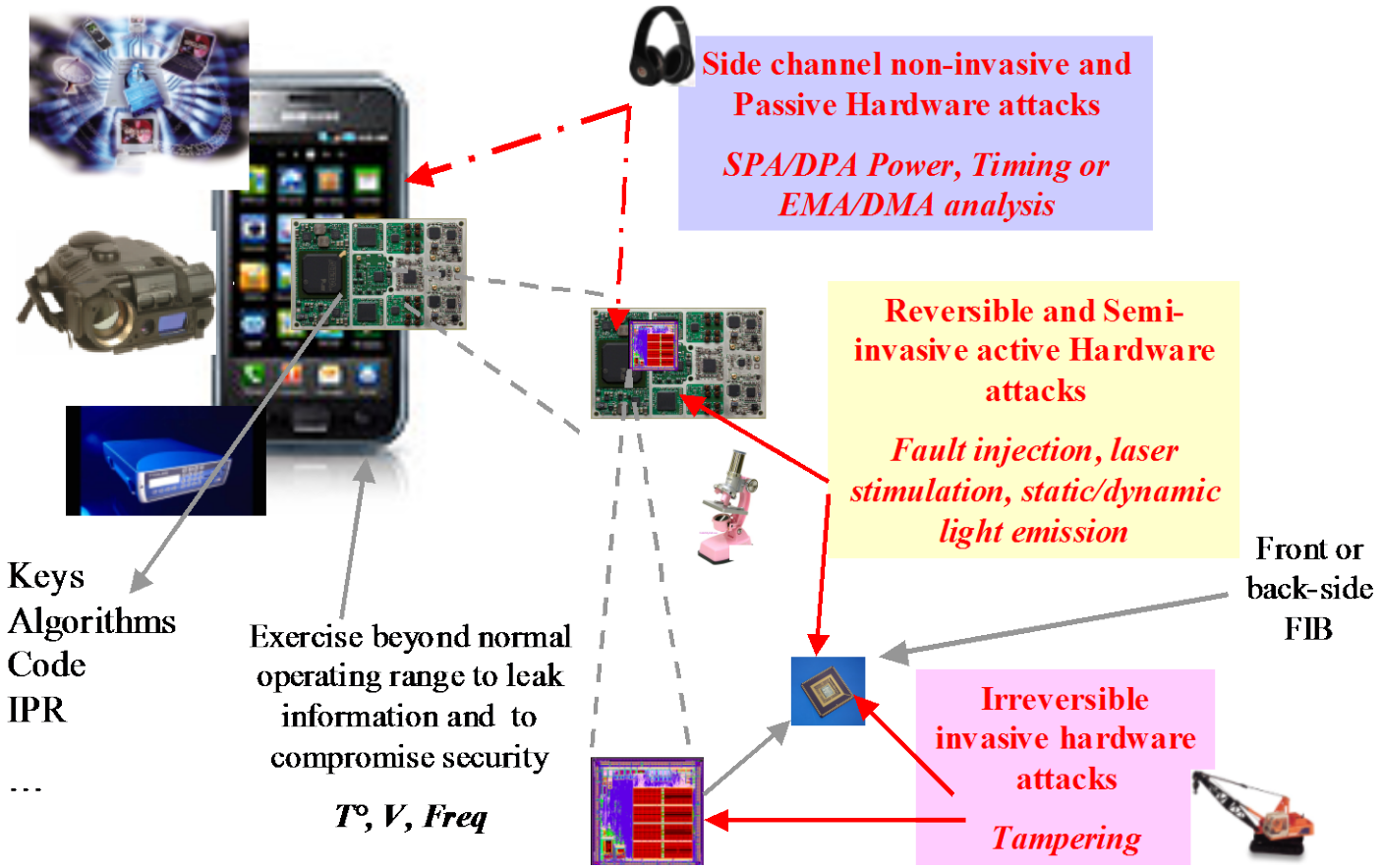
Outline

- Security tool boxes – new added value of Electronic Packaging and Interconnect
- 3D Additive nano-ink e-printing
- Embedded die in PCB and its shield
- System on Modules (SoM) towards SiP
- DoE vehicles results
- Use cases and roadmap
- Some Expectations and Conclusions

Security attacks

- A long competition between hackers and resistance with new counter-measures
- Brings Out of range parameters

Hardware Attacks on embedded systems!

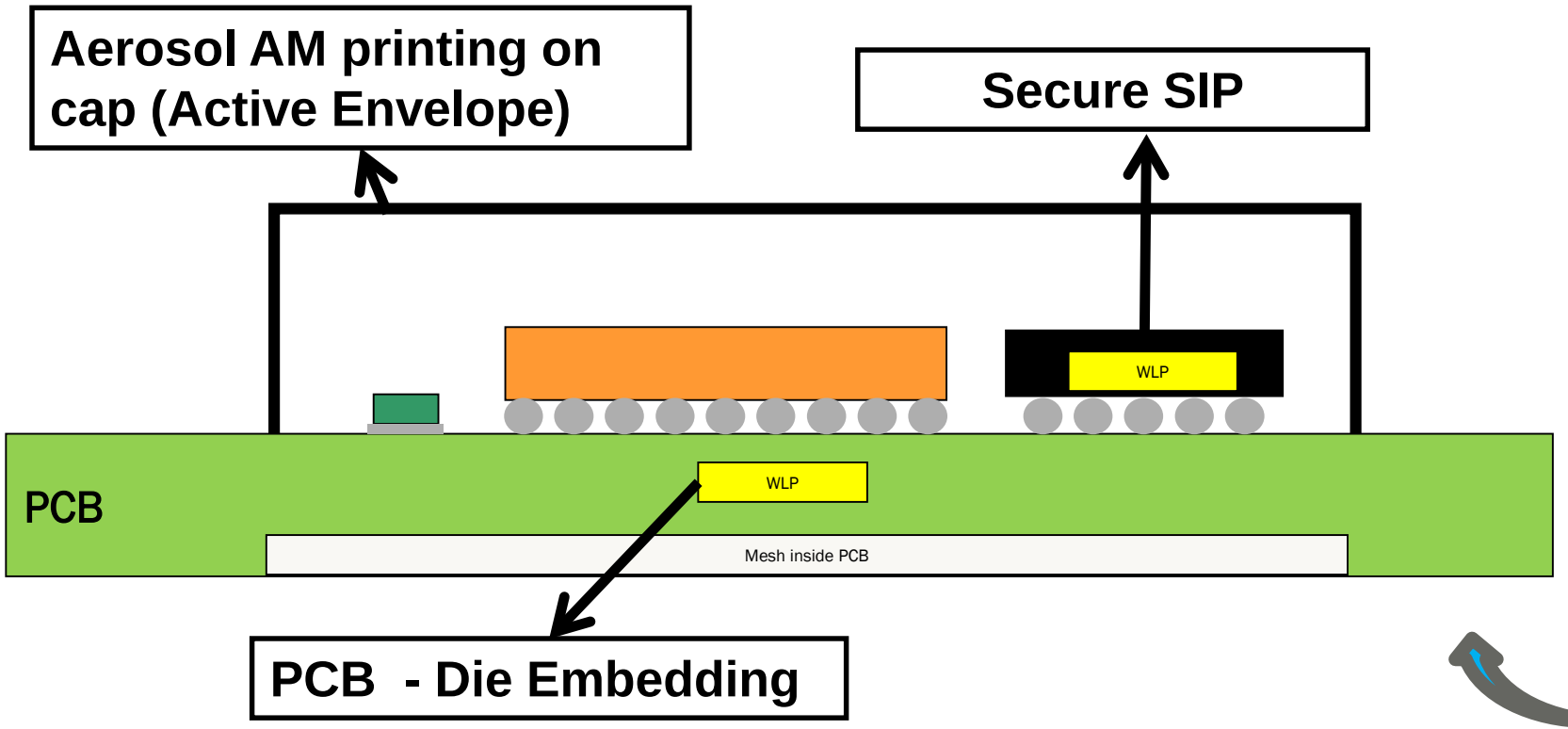


SecureTool box is with

- True Random Generator (keys),
- Cryptographic engines,
- Secure processor,
- Trusted Firmware and Operating Envt,
- Non Volatile memory Flash/Eeprom

Secure Tool box is to be completed with anti-tamper active packaging against side-channel attacks.

Secure Tool box architecture for augmented security



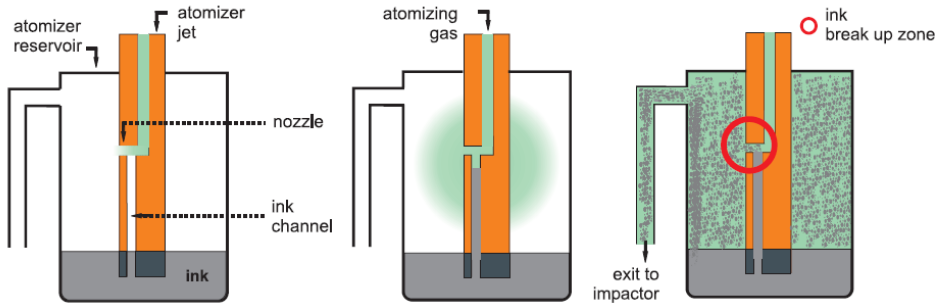
Security at the different layers / levels of the service

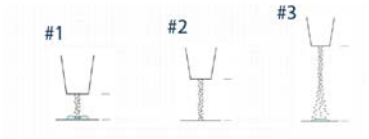
- Application, Trust management and end to end connectivity, software stacks and OS, and hereby:
- Hardware solutions

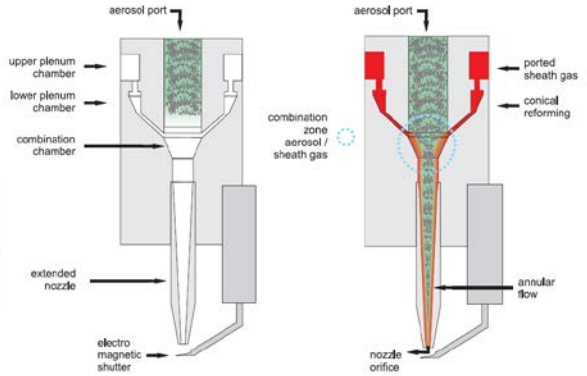
The secure perimeter or box to integrate as well a lot of embedded sensors such t°, voltage, UV, … against well know side channel attacks.
It is an active sensor.

3D Active envelope with Aerosol-Jet Deposition

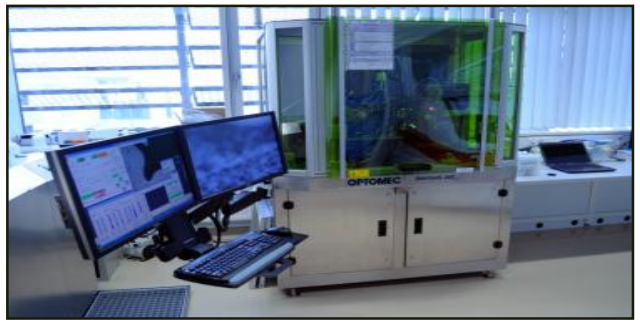
- Enables fine line features as low as < 20µm Line width up to 200µm
- Maximum size of substrate: 300 x 300 mm^2
- Pneumatic Atomizer principles
- Speed 200 mm/sec (current lab equipment)
- Precision +/- 6µm
- Partly 3D capability due to focused material beam

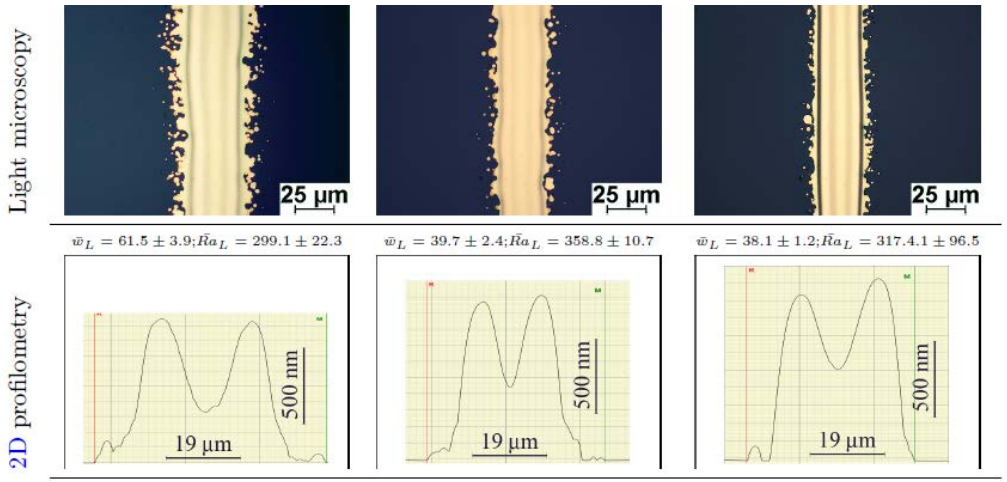


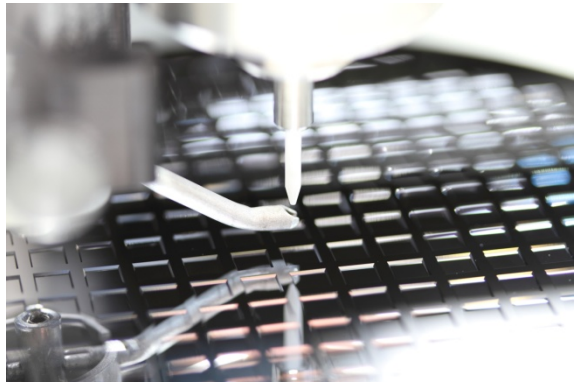




Equipment in lab



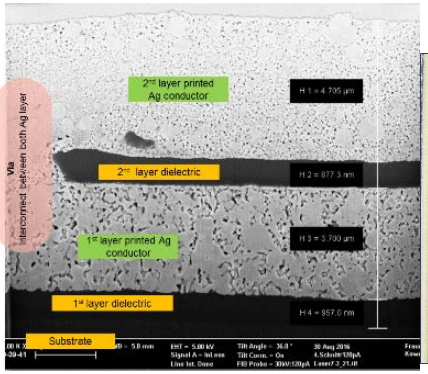




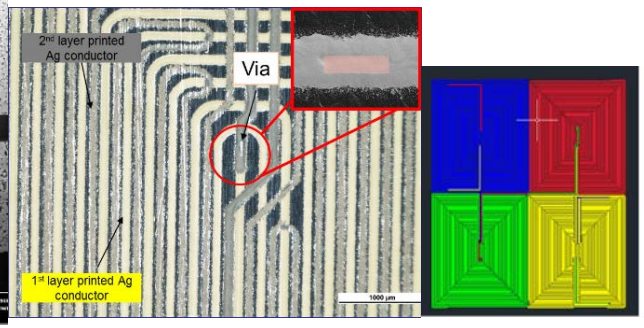
Characteristics of the realized 3D cap test vehicles

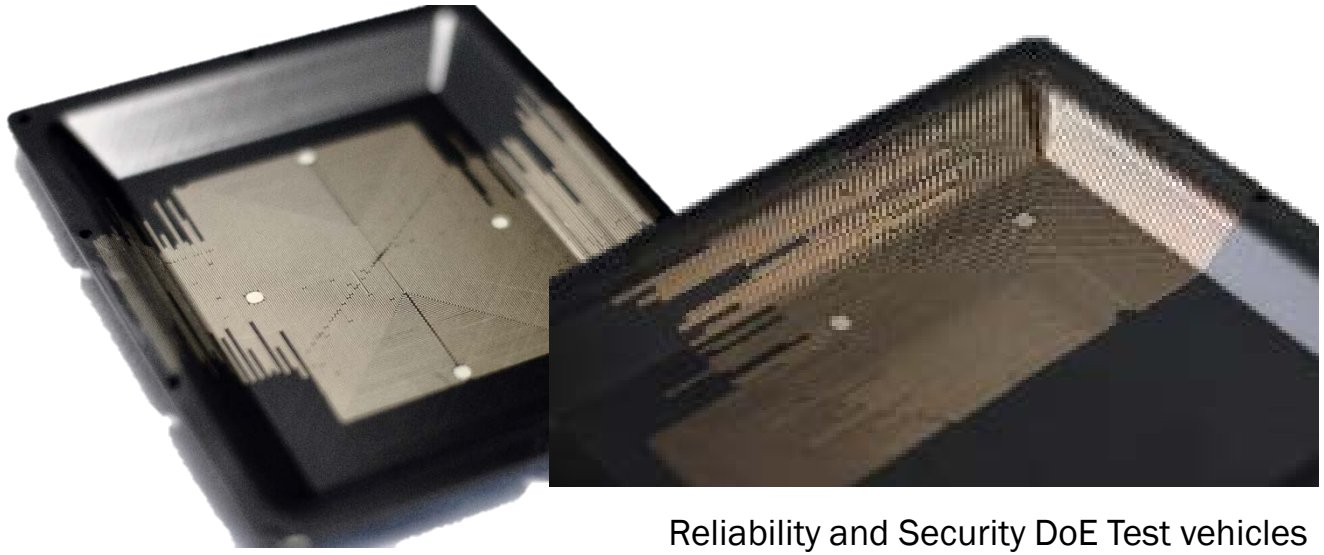
- Polymer cap
- Internal complex 3D meshes by Silver ink aerosol jet printing
- Sintering
- Laser drilling for vias with plasma treatments

Mesh length	Several meters
Mesh wire width / space	150 / 250 µm
Via size	Opening inside the conductor
Resistance value	+/- 5% change from cap to cap



Via size 50x200µm





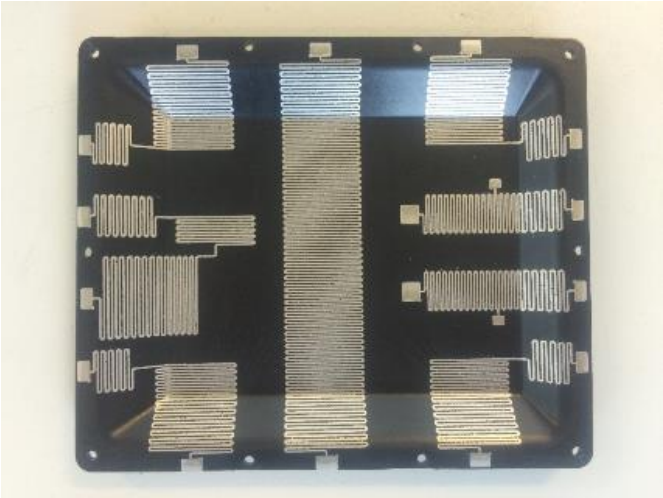
Reliability and Security DoE Test vehicles

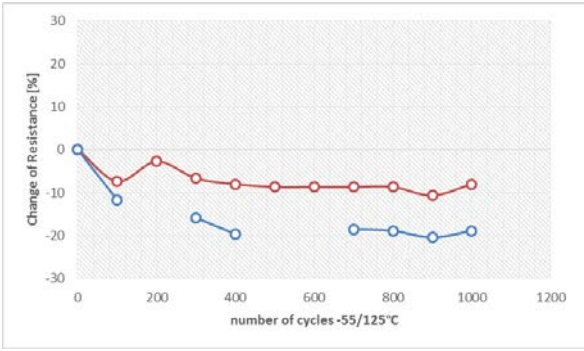
What we could expect from 3D additive nano printing equipment and related processes

- Multiple heads to speed up manufacturing time
- Steerable table with good accuracy to printing angles and slopes
- Full process for multi-layer resistive mesh built-up.
- Design rules to eliminate potential delamination between layers and to get approved tamper-resistant solution

Inkjet is one of promising technologies for Printed electronics

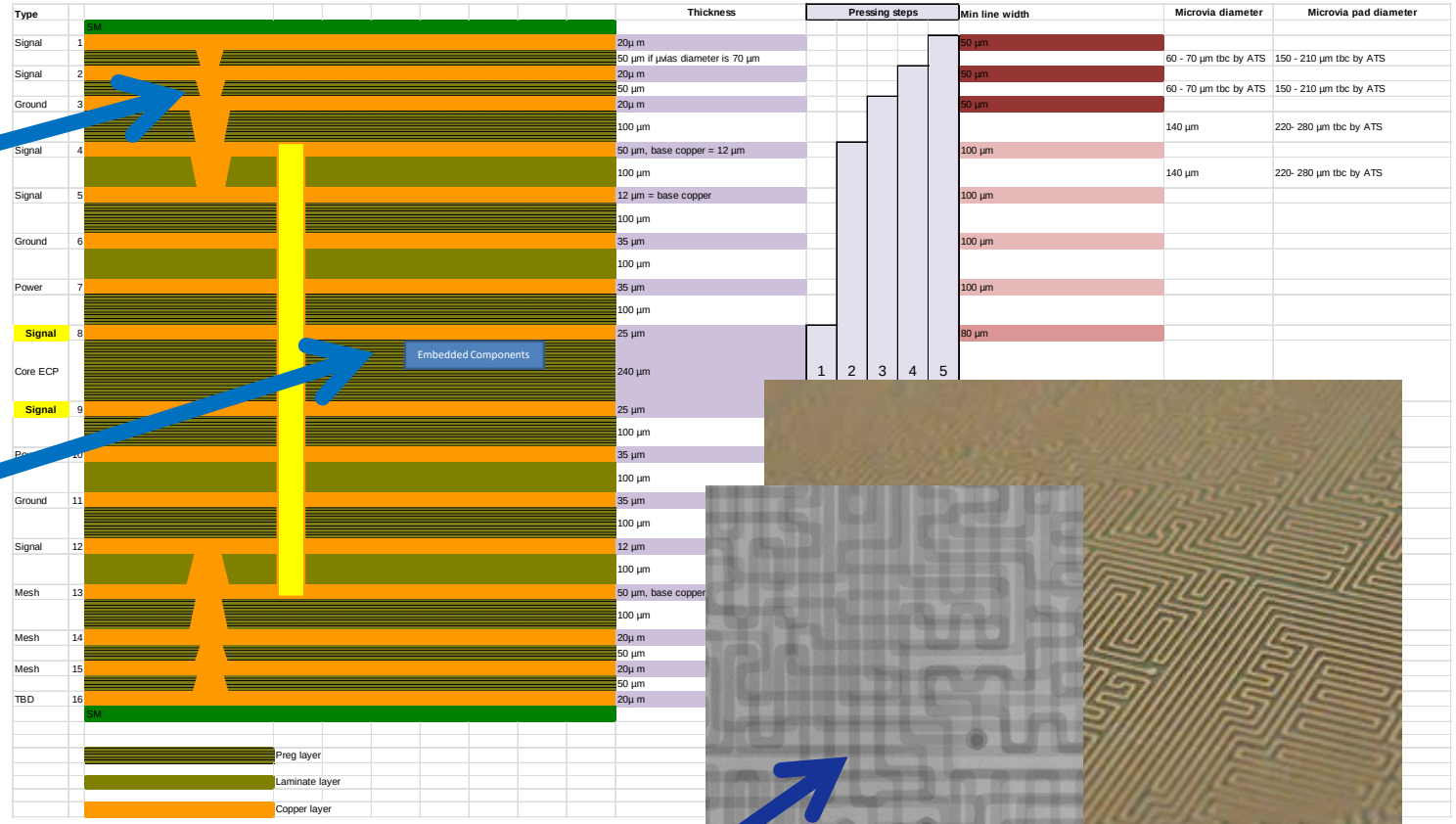
- *3D Interconnect*
- *Stable Resistive values for several lots of test vehicle*





Embedded die in PCB and its shield

- It is a complex HDI PCB
- Complex interleaved interconnects on back to build complex resistive mesh loops : 4 layers
- Embedded MCU inside PCB, to detect any change in the loops



X Ray analysis of PCB Mesh

Complex PCB meshes with stacked µvias and HDI are possible and manufacturable

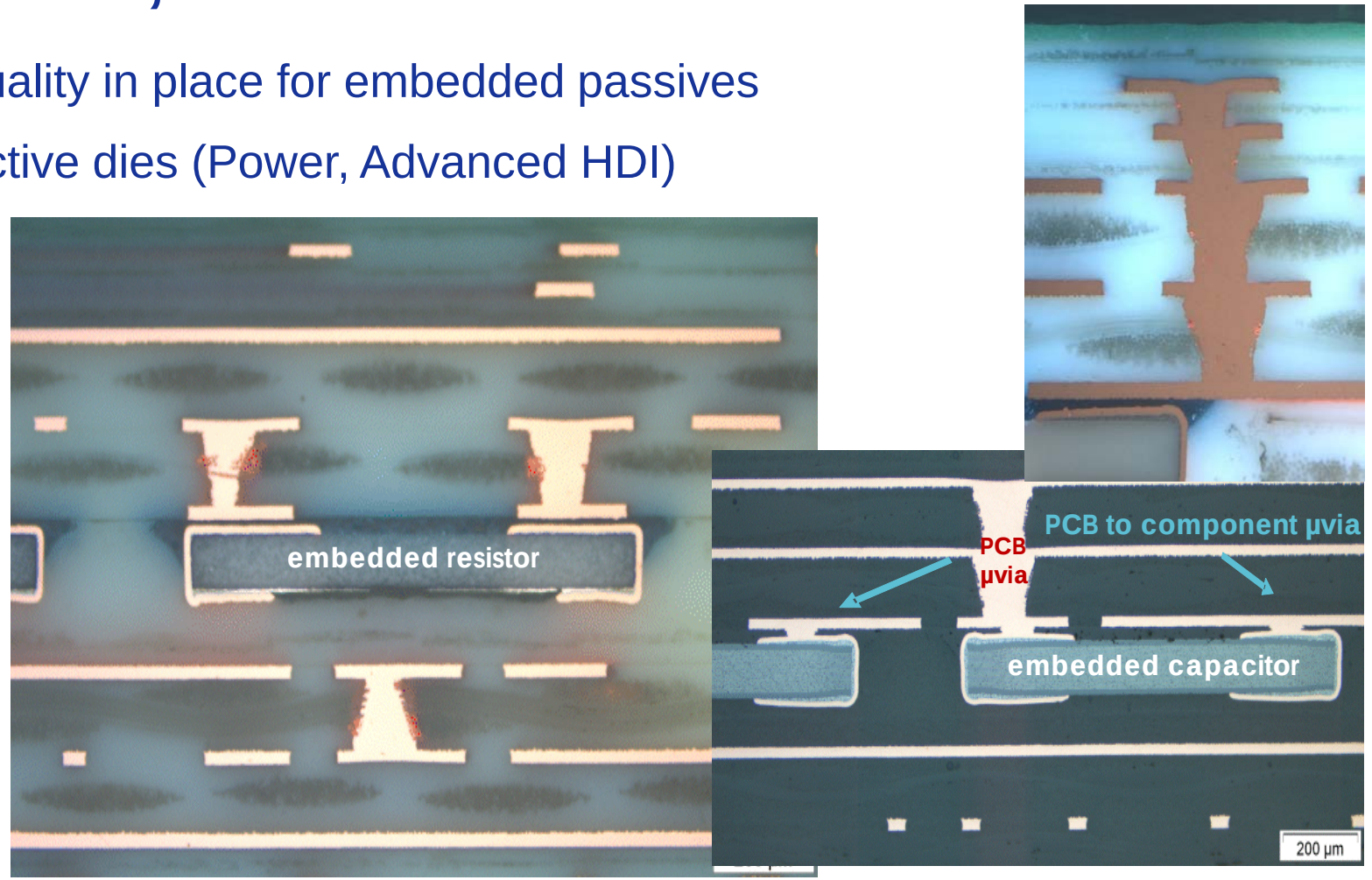
Embedding passives, dies and WLP in PCB

- Good manufacturing quality in place for embedded passives
- Current initiatives on active dies (Power, Advanced HDI)
- Solution for SoM and for Security

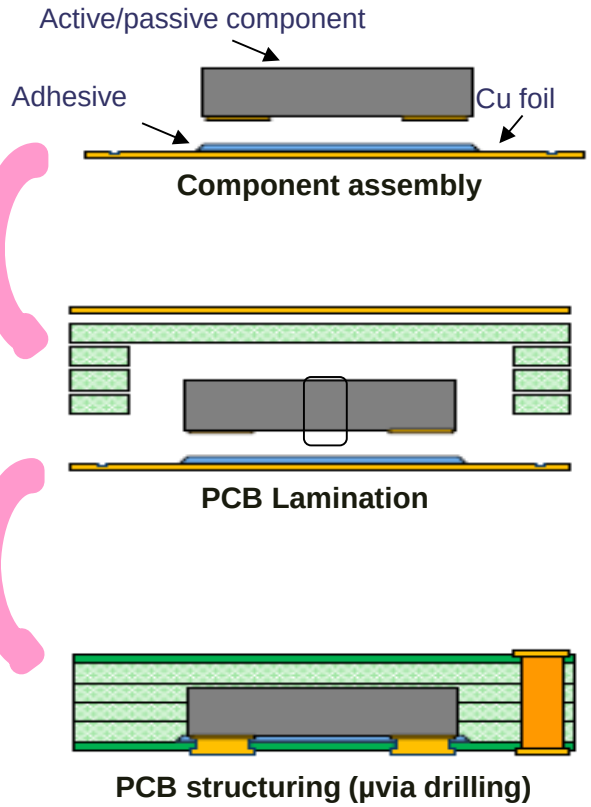
Example

10-layer PCB with 5 levels of stacked filled µvias in pad

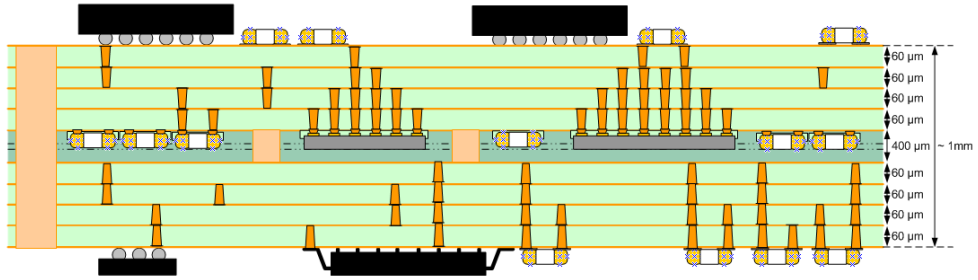
Passives components (capacitors & resistors) embedded in PCB core



Embedded die in PCB (1/2)



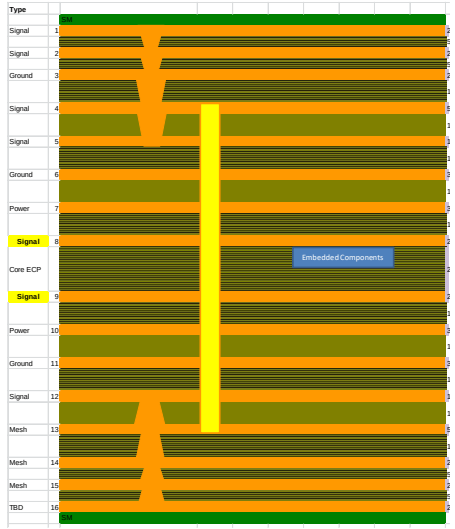
- Components with Cu finish and low thickness (*<200µm*)
- IC Post-processing to make it thinner and to create a redistribution layer to adapt it to PCB design rules
- Components are face down
- Curing step to harden the adhesive and to fix the component on the copper foil



[1]

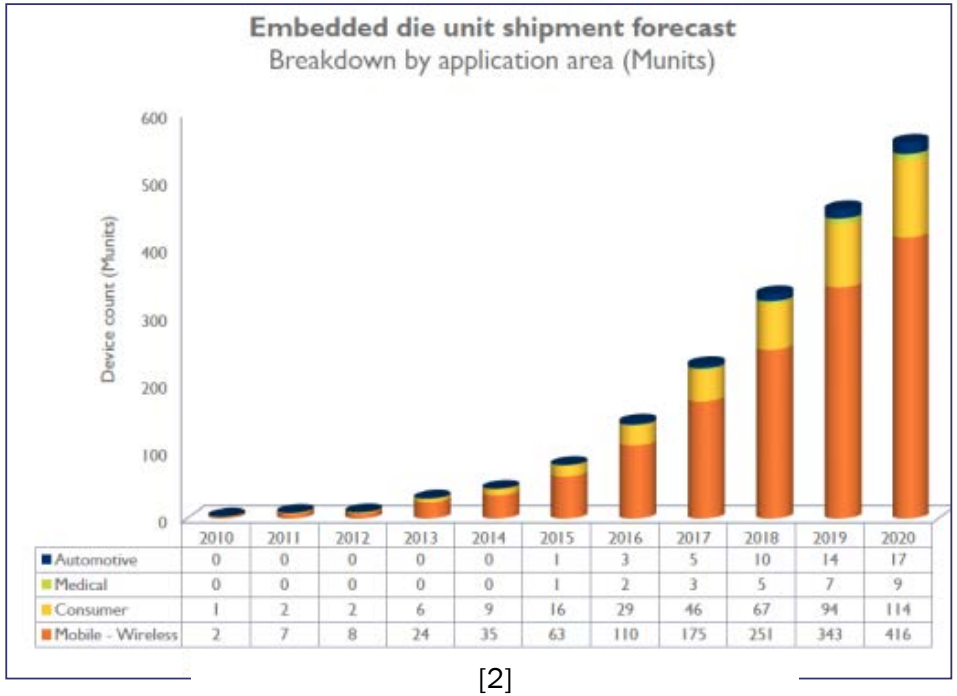
Enabling Technologies:

- Die embedding
- Several pressing steps
- Stacked µvias



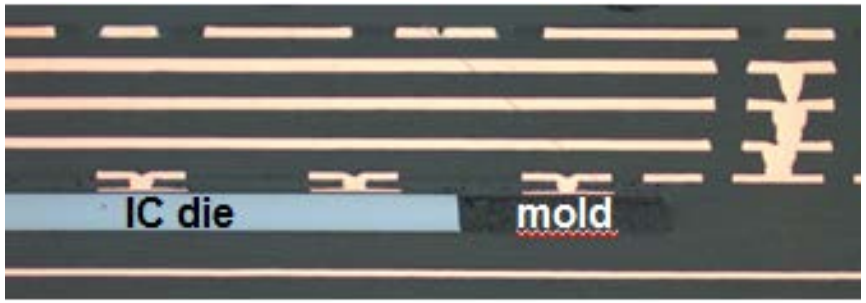
Embedded die in PCB (2/2)

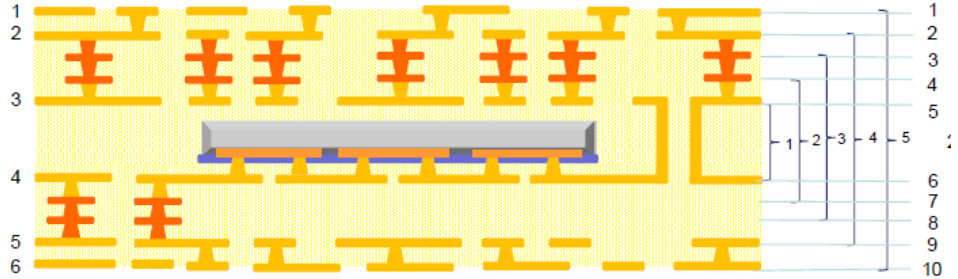
- Interconnects between component pads and PCB by laser drilling
- In total 5 pressing steps are necessary
- As part of the DoE experience, thermal cycling have been performed -



[2]

Related PCB stack layers



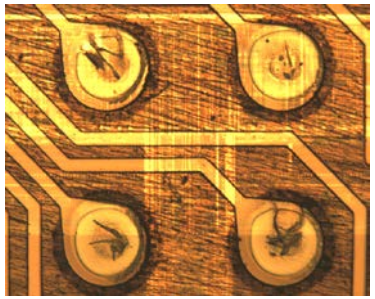


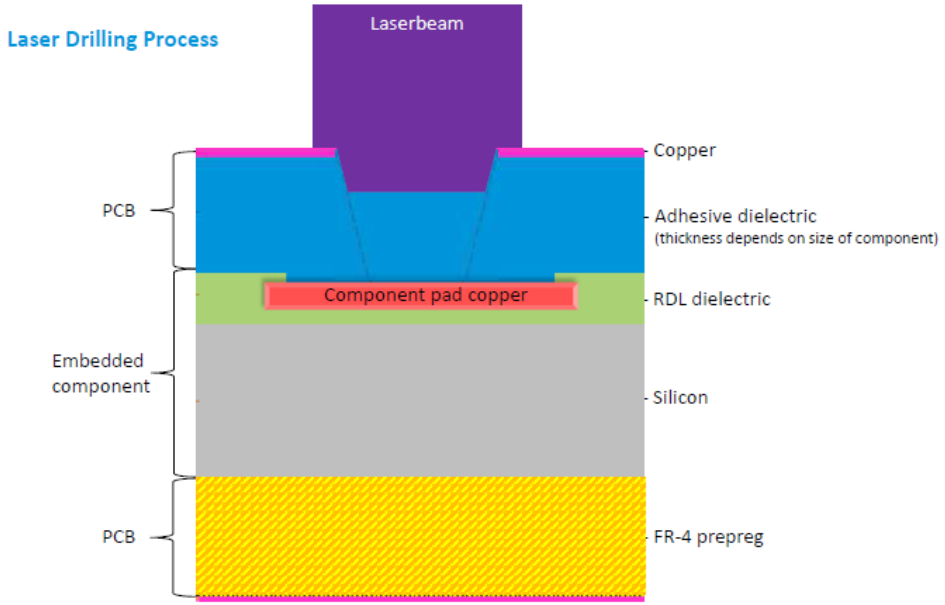
Status and what we could expect from IC embedding

- Merge of Fan Out WLP and embedded chip PCB has been demonstrated
- However interface weaknesses have been observed between Cu traces of PCB and Cu pads of the FOWL package,
- New constructions with Cu and right thickness of Cu, are successful to address both thermal shielding for the laser process and for minimization of the CTE mismatch

Embedded die in PCB is promising for secure modules

  - *However still pending security assessment*
  - *Next step is to increase die size (>5mm)*

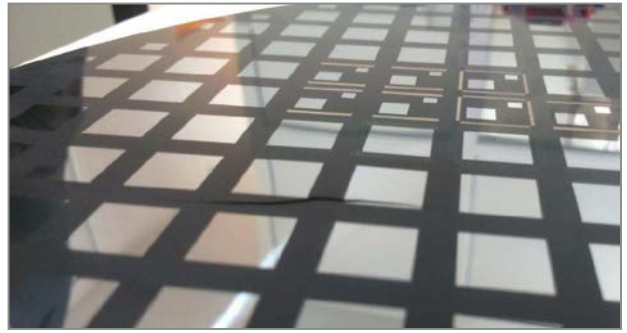


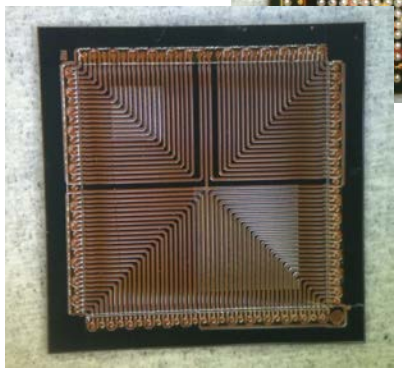


System on Module towards SiP

- Miniaturisation trends are about the integration of several dies and components in a package and its interconnects (SiP)
- One interest is to bring a secure mesh for tamper detection in secure module

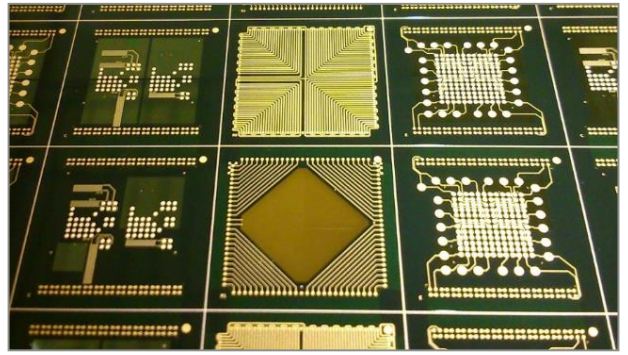
Bottom - balls



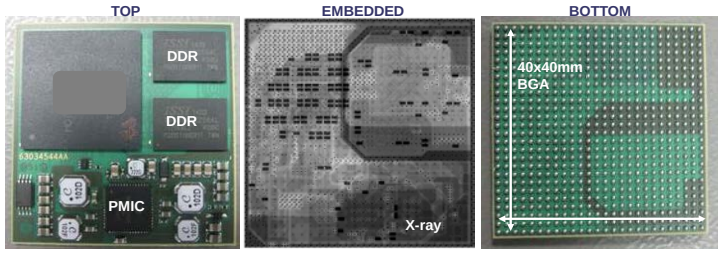


Top – secure mesh

Zoom on several RDL designs (top)

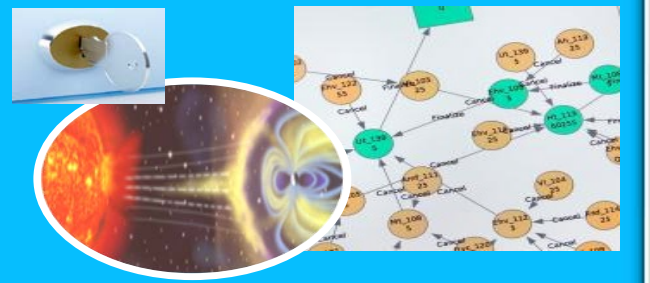


A System on Module (SoM), sometimes referred to as a Computer on Module (CoM) is designed to plug into a mother board or a carrier, and is generally a small processor module with a CPU, memories (DDR3…) and standard I/O capabilities



Infrastructure Inter-Gateways

IoT terminals and Nodes



Data storage & keys management

USE CASE categories and tool box roadmap

2016 2019 2022

Underfill on BGA

larger dies in PCB up to 10x10mm²

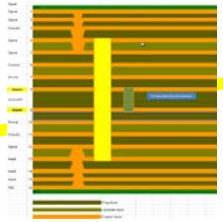
dies up to 15x15

01005

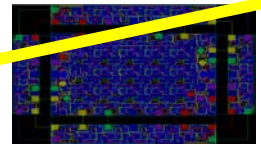
WLSiP in RDL

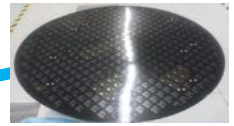
Embedded die in PCB, 5x5mm

3+1 PCB HDI Mesh 60µm

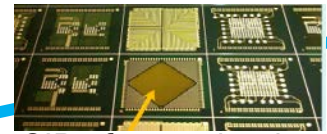


4+1 PCB VHDI Mesh 25µm





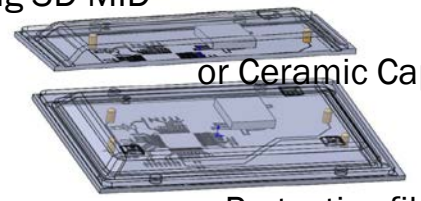
Coating mold on glue dies or packages



Multi die SiP : front + back / 2 1 layer RDL

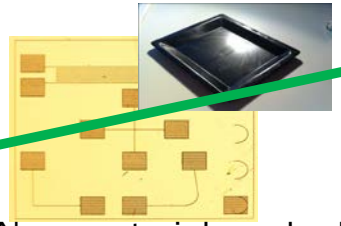
10 dies side-side & 3D stacking & TMV in Secure SiP

Existing 3D-MID

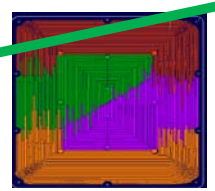


or Ceramic Cap

or Protective film



Nanomaterial meshed cap



Inkjeted mesh within Secure SiP

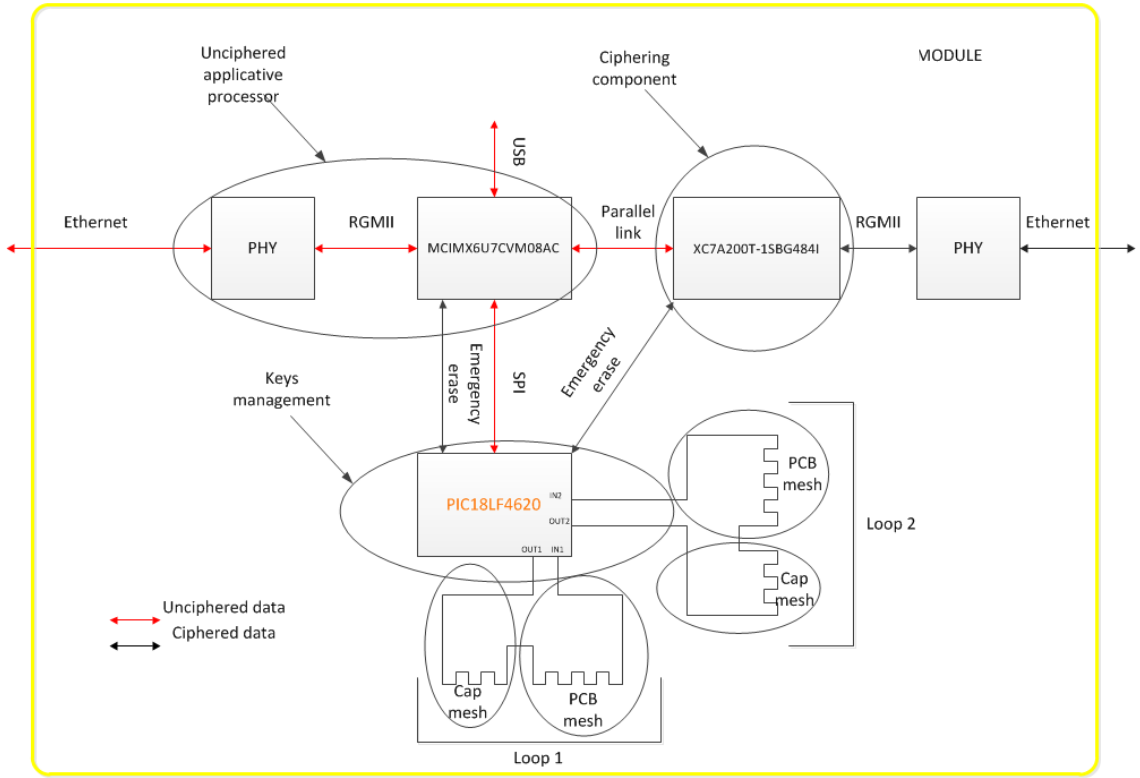
A Question about references for secure electronic packaging and interconnect

- A Protection Profile is needed for secure boxes and secure electronic modules, as part of :
- Common Criteria EAL4
- FIPS 140 Level 4
- IT Security Lab assessment

To make a measure, it is about to compare an unknown physical quantity with a size of similar item about the same type of nature, taken as reference by means of an instrument.

Conclusions

- New additive manufacturing upon nano-material aerosol jet printing is promising for resistive sensor mesh in the protective cap.
  - *Fine pitch with good electrical conductive paths on relevant surface materials with good adhesion , controlled and reproducible;*
  - *Applicable to 3D Cap on PCB module as well next to SiP package*
  - *Customisable*
- Die embedding in Printed Circuit Board together with complex PCB HDI interconnect based shield are achievable today



Schematic of the anti-tamper test vehicle

Acknowledgements

- T.Schwartz and H.Stahr AT&S, Austria, embedded die PCB
- F.Roscher and N. Saeidi, Fraunhofer ENAS Germany, nano ink additive manufacturing and multilayer Mesh
- A.Cardoso and E.Fernandes, Nanium SA, Portugal, multi die WLP SiP
- Ch. Hannauer and C.Marron Thales Communications & Security, France, anti-tamper Hardware architectures
- M.Brizoux and A. Lecavelier des Etangs-Levallois, Thales Global Services, France, Manufacturability and reliability analysis

The program is performed in the framework of European FP7-SEC UNSETH project (Grant Agreement No. FP7-SECU-312701).

References

[1] HERMES

[2] Embedded Die and Fan-Out Technologies and Market Trends, Yole Report, 2015, Yole Development.