On hardware security and trust for chiplet-based 2.5D and 3D ICs: Challenges and Innovations

Suzano Da Fonseca Juan, Abouzeid Fady, Giorgio Di Natale, Philippe Anthony, Roche Philippe

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 24 January 2024, accepted 13 February 2024, date of publication 22 February 2024, date of current version 29 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3368152

SURVEY

On Hardware Security and Trust for Chiplet-Based 2.5D and 3D ICs: Challenges and Innovations

JUAN SUZANO[1,2,3], FADY ABOUZEID[1], GIORGIO DI NATALE[3], (Senior Member, IEEE), ANTHONY PHILIPPE[2], AND PHILIPE ROCHE[1], (Member, IEEE)

[1]STMicroelectronics, 38920 Crolles, France
[2]CEA, LETI MINATEC Campus, Université Grenoble Alpes, 38054 Grenoble, France
[3]TIMA, CNRS, Grenoble INP, Institute of Engineering, Université Grenoble Alpes, 38000 Grenoble, France

Corresponding author: Juan Suzano (juan.suzano@st.com)

ABSTRACT The relentless pace of transistor miniaturization has enabled developers to continuously increase chip complexity since the beginning of the information age. However, as transistors get smaller and chips become larger, the cost of manufacturing ICs becomes increasingly prohibitive. As Moore's Law is coming to an end, industry and academia have been exploring new paradigms to keep up with the ever-increasing demand for performance and functionality while dealing with the constraints of power consumption, area, and yield. In this context, 3DICs are considered the future of the IC industry as they enable designers to fulfill both the ''More Moore'' and the ''More than Moore'' paradigm. A key feature of the 3DIC is that it can be manufactured by assembling multiple chiplets. Chiplets are single-purpose dies that must be assembled with other chiplets to form a complete system. Researchers and industry leaders believe that a chiplet market will form and that products with off-the-shelf chiplets will emerge. This scenario offers many economic opportunities. However, it also raises concerns regarding the security and trust (S&T) of chiplet-based designs. Malicious chiplets, hardware trojans, and chiplet intellectual property theft are threats that must be addressed as the industry moves towards the ''chiplet age''. In this survey, we introduce the different types of 3DICs and their production chain. We then define the threats that threaten the different steps of the 3DIC manufacturing process. Finally, we present and discuss the state of the art in hardware S&T techniques for chiplet-based 3DICs.

INDEX TERMS 2.5DIC, 3D integration, 3DIC, chiplet, interposer, hardware security, hardware trojan (HT), hardware trust, malicious chiplet, untrusted chiplet.

I. INTRODUCTION

Since 1965, when Gordon Moore stated that the number of transistors in an integrated circuit (IC) would double every 18 months, the miniaturization of transistors has been the main driving force behind the improvement of performance, power consumption and area (PPA) in ICs. This phenomenon is known as Moore's Law [1]. However, as technology nodes approach the 5nm mark, experts affirm that Moore's Law is nearing its limits [2]. The ever-increasing challenges associated with advanced technology nodes (such as pitch scaling, routing congestion and process variations) and the need to further improve PPA have prompted industry and academia to look for alternatives to miniaturization. This trend is known as More Moore [3]. At the same time, designers are also considering more disruptive ways to increase the functionality of ICs. The integration of digital and analog circuits in a single die and the use of different materials, such as organic substrates, are two examples of techniques that can improve functionality beyond miniaturization. This is referred to as ''More than Moore [4].

In this context, 2.5D and 3D heterogeneous integration emerge as an alternative way to improve functionality and performance. These technologies are the natural evolution of

The associate editor coordinating the review of this manuscript and approving it for publication was Harikrishnan Ramiah.

traditional System-On-Chip (SoC) manufacturing. While a traditional SoC contains only one transistor layer, 2.5D and 3D ICs are manufactured by assembling multiple dies in an interposer (2.5D) or in a stack (3D). Large 2D SoC designs can be disaggregated into smaller circuits and manufactured as specific function dies called chiplets, which can be assembled into a multidie system. This method allows better flexibility and optimization for designers, as each design function can be manufactured in the optimal technology and assembled in a package instead of a printed circuit board (PCB) [5].

The chiplet paradigm also creates economic opportunities. As 2.5D and 3D ICs become more popular, researchers and industry leaders expect a chiplet market to emerge. Designers will be able to build 2.5D and 3D ICs leveraging of-the-shelf chiplets, reducing the time- to- market, manufacturing time and development cost. This scenario raises several concerns regarding the hardware security and trust (S&T) of chiplet-based systems.

Due to the increased number of actors involved in the production of a chiplet-based IC, a chiplet-based production chain would also create opportunities for malicious users to jeopardize the integrity of the multidie SoC. Malicious chiplets with hidden functionality may pollute the chiplet market and hardware trojans may be more difficult to prevent. In addition, intellectual property (IP) theft may become more appealing to adversaries in a chiplet-based production chain than it is in the traditional 2D SoC production chain.

The goal of this survey is to discuss the S&T aspects of the emergin chiplet-based IC industry. It highlights the S&T threats arising from the transition to chiplet-based ICs and presents various 2.5D- and 3D-specific countermeasures that have been documented in the literature. In addition, this survey discusses the research landscape in 2.5D and 3D hardware S&T, highlighting its importance, especially as the industry moves towards a chiplet-based production chain. In doing so, it emphasizes the need for continued exploration and innovation in this area to ensure the S&T of future chiplet-based hardware systems.

The rest of this work is organized as follows: We first introduce the 2.5D and 3D integration technologies in Section II. Next, we present the chiplet paradigm and an overview of the possible production chain for a chiplet-based IC in Section III, and how the integrity of such ICs can be threatened by an attacker placed at different phases of the manufacturing process in Section IV. We also explore how an attacker may retrieve secret information about the 3DIC during fabrication, thus infringing on the IP. In Section V, we present the state-of-the-art countermeasures for protecting both the integrity and IP of 3DICs. Lastly, we discuss the research space on 3DIC hardware S&T in Section VI and conclude our work on Section VII

II. 2.5D AND 3D HETEROGENEOUS INTEGRATION

Historically, SoCs have been composed of only one layer of transistor logic. This means that there used to be only two ways for SoCs to expand: increasing the density of transistors on the die or increasing the area of the die. A natural evolution made possible by advances in IC manufacturing capabilities is to have multiple layers of transistor logic on the same SoC. There are different manufacturing techniques to integrate multiple transistor layers into the same package: 2.5D heterogeneous integration, 3D heterogeneous integration, and 3D monolithic integration, as illustrated in Fig. 1.

In the 2.5D scheme, multiple dies are assembled in an interconnect die called Interposer. In the stacked 3D scheme, multiple dies are stacked vertically on the same package. Finally, in the monolithic 3D (M3D) scheme, multiple layers of transistors are manufactured on the same wafer in an advanced sequential manufacturing process.

In this survey, we are interested in the S&T implications of building integrated systems through the assembling of multiple dies. Therefore, M3D ICs, which are based on a single manufacturing step as classical SoCs, are considered out-of-scope of this work. In the remainder of this survey, we refer to stacked 3DICs and interposed-based 2.5DICs as 3DICs, and the distinction is only made when necessary.

At the foundation of 3DIC design is the concept of chip disaggregation. It refers to a process in which designs are disaggregated into smaller circuits called chiplets. Chiplets are defined as IC dies with specific functions that are designed to be assembled with other chiplets to form a 3DIC. Chiplets are manufactured through their own manufacturing processes and assembled via 2.5D or 3D integration [6]. This approach contrasts with traditional 2D SoC development where each IP block of an SoC design is implemented on the same monolithic die. The benefits of chiplet-based systems are discussed in Chapter III.

Although chiplets are just emerging as a trend, their application in the industry has already started, marking an early adoption of this technology. Intel is making chiplets and heterogeneous integration its focus for future manufacturing strategy with products like Foveros already on the market [7]. AMD has already launched several generations of chiplet-based consumer products, such as the recent AMD Ryzen Series iterations with 3DV-Cache chiplet [8]. Apple has switched from Intel to its in-house chiplet-based processor across all its personal and professional computers [9]. Tesla has developed its in-house supercomputer for machine learning with chiplets [10]. Biren Technology launched its dual die chiplet-based general-purpose GPU [11]. Although these examples do not leverage the decentralized production chain that chiplets allow, initiatives are being developed to enable the emergence of an open chiplet ecosystem. The Open Compute Project Foundation (OCP) and JEDEC started a collaboration to develop standard models for the documentation and sharing of thermal, physical, mechanical, IP, behavioral, and power information between chiplet vendors and designers [12]. This work in progress has been considered one of the foundations for the upcoming chiplet ecosystem [13].

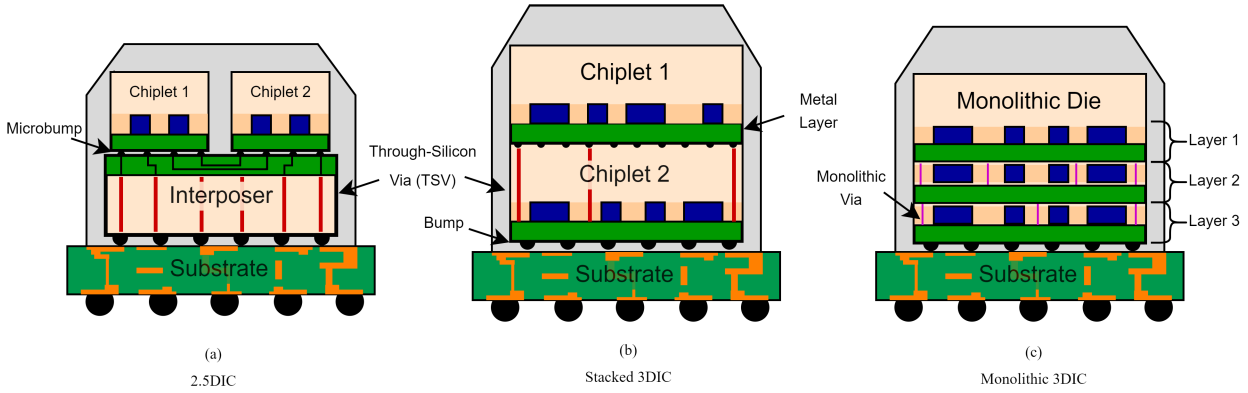

FIGURE 1. The flavors of 3DIC; (a) A chip composed of two chiplets assembled in an interposer; (b) A chip composed of two chiplets assembled in a stack; (c) A chip composed of one monolithic multilayer die.

In the remainder of this chapter, we present details of both 2.5D and 3D heterogeneous integration techniques.

A. 2.5D HETEROGENEOUS INTEGRATION

The 2.5DIC assembly scheme is characterized by the use of an interposer to integrate multiple dies. This scheme is the miniaturization of the approach of assembling chips on a PCB. However, performing the assembling at the diel evel allows for better performance due to higher interconnect density and lower power consumption. The interposer can be passive or active. A passive interposer is composed of only interconnection metal layers. An active interposer is composed of metal layers and transistors to implement some simple computing logic [14], [15].

Active interposers can incorporate several features that facilitate the integration of chiplets, such as signal conditioning, protocol conversion, error correction, Design-For-Testability (DFT) functions and power management [16], [17]. What distinguishes an active interposer-based assembly from a stacked 3D assembly is that the main purpose of the interposer is limited to the system infrastructure and interconnections.

Chiplets assembled in an interposer can be manufactured using different manufacturing processes. Chiplet stacks can also be assembled in the interposer. The assembly scheme where stacks are integrated on the interposer is referred to as 5.5D (the addition of 2.5D and 3D). The 2.5DIC manufacturing process is different depending on the type of interposer. Passive interposers are manufactured by foundries using the Back-End-Of-Line (BEOL) process, as they do not contain active Front-End-Of-Line (FEOL) elements. Active interposers, on the other hand, are manufactured in a similar way to a traditional die and undergo both FEOL and BEOL processes. In this case, the active logic must be kept at a minimum to prevent yield deterioration [18].

Currently, 3DIC manufacturing is a vertical process and multiple steps of the manufacturing process are performed by the foundry, including the assembly of the dies on the interposer. However, it is expected that outsourced semiconductor assembly and testing (OSAT) facilities will develop the necessary infrastructure to provide this service. Pre-bond testing of the interposer is still difficult due to multiple reasons [19]. However, pre-bond testing of interposers is critical to minimize the yield loss from stacking Know Good Dies (KGD) on defective interposers [20].

B. 3D HETEROGENEOUS INTEGRATION

Stacked 3DIC is the assemble scheme that gives the name to the umbrella term 3DIC. As the name suggests, it is composed by the stacking of multiple dies. The connection between the dies is made by microstructures such as the Trough-Silicon Vias (TSV). The TSV is an electrical connection that traverses the silicon layer. This technology allows stacked dies to connect with each other, or with the bumps, depending on the manufacturing process. There are different methods for stacking the dies: Wafer-to-Wafer (W2W), Die-to-Wafer (D2W), and Die-to-Die (D2D).

The W2F, D2W, and D2D assembly methods are illustrated in Fig. 2. In the W2W process, two wafers are stacked directly and the stacked dies are extracted from the stacked wafers. This technique offers fast assembly throughput but requires the dies on each wafer to have the same footprint [21]. Because the stacking process is performed at the wafer level, it is not possible to avoid stacking a good die with a defective die.

On D2W an individual die is extracted from one wafer and it is assembled on another die in a wafer. This method solves the problem of stacking good dies with defective dies, resulting in a better yield than W2W. It also enables the integration of two different sizes dies [22].

D2D is the most expensive and versatile assembly process. It enables the individual testing of both dies, as well as the integration of different-sized dies and the stacking of multiple dies. It is also the only method in which the assembly process can be carried out by an external assembler [23].

Different bonding styles can be applied with regard to the direction in which the dies are connected: Face-to-Back (F2B), Face-to-Face (F2F), and Back-to-Back (B2B).

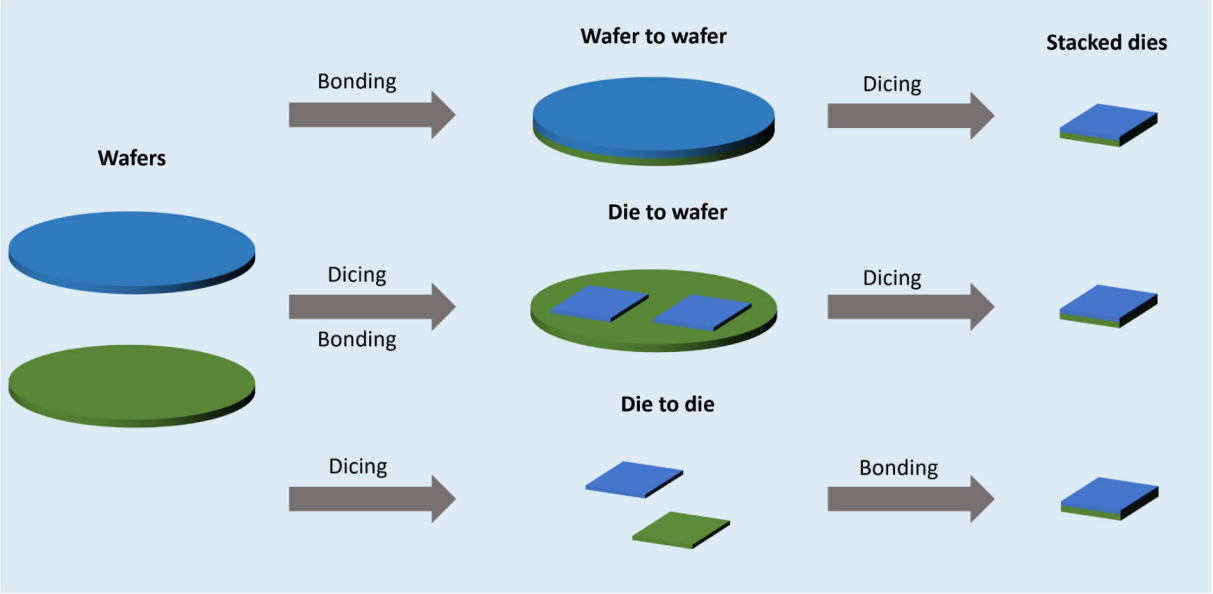

FIGURE 2. The image illustrates the Wafer-to-Wafer, Die-to-Wafer, and Die-to-Die assembly methods; In the Wafer-to-Wafer the blue wafer is bonded on the green wafer and the 3DIC is diced from the blue and green wafer stack; In the Die-to-Wafer the chiplets are diced from the blue wafer and bonded on the green wafer. The 3DIC is then diced from the green wafer with blue dies; In the Die-to-Die, the dies are diced from the blue and from the green wafer. The dies are then bonded together to form the 3DIC.

"Face" and "Back" refer to one of the sides of the die. The face side contains the metal layers, while the back side is the passive silicon layer. In the F2F style, metal vias are used to connect both layers. The area and parasitic of a metal via are much smaller than in TSV. As a result, the signal delay is reduced, and Place and Route (P&R) is easier when compared with F2B and B2B, where TSV is used to connect the dies. However, this style only allows the stacking of two dies without mixing bonding techniques. In both the F2B and B2B techniques, the interconnection between the dies is made via TSVs. However, the former allows the stacking of multiple dies using fewer TSVs than B2B [24].

Finally, there are three options for the placement of the TSV on the stacked 3DIC manufacturing process: via-first, via-middle, and via-last. In the via-first scheme, TSVs are manufactured before the FEOL steps [25]. Via-middle TSVs are fabricated between the FEOL steps and the BEOL, which inserts the metal layers. Finally, via-last TSVs are manufactured after the BEOL process. Via-last TSVs can be manufactured by an external packaging facility [23]. The via-middle scheme is the most popular scheme for stacked 3DICS and interposer-based ICs [26].

The assembly and testing of stacked 3DICs is performed by the foundry, but could also be performed by the OSATs in the future. The testing process of stacked dies is difficulted by the fact that the dies may not have access to the package pinout. The IEEE 1838 DFT standard [27] intends to solve this problem. The standard defines the infrastructure for testing dies before and after stacking. Compliant dies have the necessary infrastructure for standalone pre-bond testing. After stacking, the DFT of each compliant die forms a DFT network that can be controlled by the "master" die.

C. DISCUSSION: 2.5D, 3D, AND CHIPLETS

2.5D and 3D technologies do not compete for the best option for assembling chiplets. 2.5D technology is considered a good tradeoff between the benefits of 3D integration and its manufacturing cost and complexity. Interposer-based products have been on the market for over a decade. Xilinx launched the first interposer-based FPGA using TSMC technology in 2012 [28]. Additionally, different 2.5DICs reached the market in recent years. Interposer manufacturers such as TSMC already offer various interposer options for their customers [29]. The maturity of silicon interposer technology makes it the current established technology for 2.5D devices. However, researchers are already working on new disruptive interposer technologies. Organic interposers have been studied as a cheaper alternative to silicon interposer [30], although they present some mechanical properties difficulty [31]. Glass interposers have been studied as platforms for high-frequency applications such as 5G antennas [32]. The physical characteristics of glass interposers may also improve assembly yield and power reliability [33].

At the same time, stacked 3DICs also gain traction. The recently introduced AMD Zen processor with 3D V-Cache is a state-of-the-art consumer CPU that takes full advantage of 3D integration by assembling logic and memory in a stack [8]. Companies specialized in stacking CMOS image sensors with computing logic may expand their capabilities to offer

low-cost logic-on-logic or memory-on-logic stacking [34]. As D2D stacking becomes less expansive, it will gain traction, as it offers great design flexibility and allows stacks of more than two dies as well as stacks of dies of different sizes. Finally, many scientists and industry leaders believe that chiplets are at the center of this paradigm shift, and we anticipate that the combination of 2.5D and 3D (sometimes called 5.5D) will be the best platform for designers in the chiplet era.

III. CHIPLETS AND CHIPLET-BASED PRODUCTION CHAIN

It has been reported for decades that Moore's law is reaching its limits [2]. The miniaturization approach for PPA improvement is becoming increasingly and continuously more expensive [35], [36], [37]. When Gordon E. Moore predicted that it would be possible to cram as many components into a single die as it is today, he also foresaw the complexity and cost of developing and manufacturing such ICs. Accordingly, he also stated that building large systems from smaller functions might be the more sustainable approach [1]. Academics and industry leaders have advocated 3DICs as the solution that would allow developers to meet both ''More Moore'' and ''More-than-Moore'' trends simultaneously.

In the remainder of this Section, we discuss the aspects of the chiplet paradigm that are driving the industry to shift to a decentralized, chiplet-based production chain. Next, we elaborate on what a chiplet-based production chain could look like and highlight the S&T threats that could threaten a decentralized production chain.

A. BENEFITS OF CHIPLETS

Many works in the literature have discussed the benefit of multi-die designs. Here we highlight the economic, functional, die interconnection, power, and area benefits.

1) ECONOMIC BENEFITS

The manufacturing of large dies results in lower yield per wafer, as the probability of manufacturing defects correlates with die size. Therefore, smaller dies (i.e. chiplets) have a lower cost per KGD, which increases the yield [38]. It has been reported that chiplets can reduce manufacturing costs by approximately 40% when using mature manufacturing nodes even taking into account the cost overhead required to interconnect the dies [39]. The cost benefits of using chiplets vary depending on the design. In [40], the authors developed a quantitative cost model to evaluate the benefit of using chiplets in a given context. This work concludes that the closer the manufacturing technology is to Moore's limit, the more the system benefits from a chiplet-based approach. Disaggregation also enables the reuse and commercialization of chiplets as commodity hardware, which shortens the development time and thus the time-to-market. Finally, the heterogeneous integration of chiplets using different technology nodes enables flexibility in terms of design cost [41].

2) FUNCTIONAL BENEFITS

The design flexibility made possible by heterogeneous integration also has a positive impact on the overall functionality of the design. Chiplets with different functions can leverage the most suitable technology node. For example, logic and memory circuits require manufacturing processes that are optimized for transistor density, current leakage, and speed. On the other hand, I/O ICs work better on a technology optimized for high voltages [41]. with 3DIC, designers can avoid technological compromises and build an optimal system.

3) DIE INTERCONNECTION BENEFITS

In addition to the flexibility offered by heterogeneous integration, 3DICs also have benefits in terms of bandwidth. By assembling multiple dies in a 3DIC, the connection between the dies can be made via on-chip connections (faster) instead of off-chip connections (slower). This is important for High-Performance Computing (HPC), where the demand for high performance requires a large number of compute units and fast memory access [42], [43], [44], [45]. Given the ever-increasing demand for performance in everyday computing tasks, it is reasonable to imagine that this characteristic will also be important in consumer products.

4) POWER AND AREA BENEFITS

The assemblage of dies in a 3D stack or in an interposer helps to keep data ''on-chip'', which can reduce greatly the power consumption for applications that rely on memory data access [46], [47], [48], [49]. Power benefits have been demonstrated on consumer products such as in [50]. Stacking dies in 3D allows designers to keep pushing transistor densification for applications constrained by footprint and height, as vertical stacking offers a smaller footprint than multi-package assemblies [51]. Augmented Reality (AR), Internet of Things (IoT), and other mobile applications can benefit from the power and footprint advantages provided by 3DICs [52], as these types of applications are heavily implicated by power and area constraints.

B. 3DIC PRODUCTION CHAIN

As 2.5D and 3D heterogeneous integration technologies mature, we expect the industry to shift to a chiplet-based production chain. This envisaged production chain would differ from the current IC production chain in several ways and would require a different approach to design, manufacturing, assembly and testing. This transition would also introduce new S&T risks as new manufacturing processes will be required and new actors will be involved in the production chain.

In Fig. 3, we show a hypothetical 3DIC production chain and the S&T risks that occur at each step of the manufacturing process. In this example, two stacked 3DICs are assembled on an active interposer. The left side of the image illustrates the

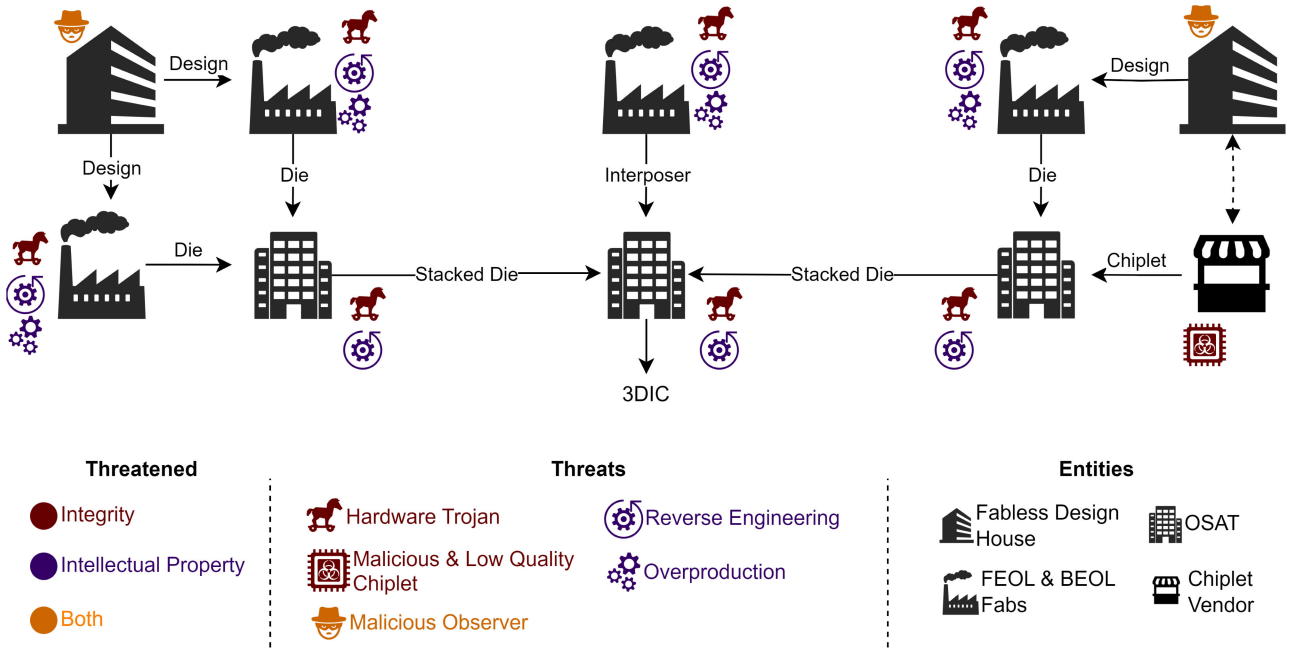

FIGURE 3. Example of a possible 3DIC production chain. Two stacked 3DICs are manufactured. The first is designed by a fabless design house. Each die is manufactured in a different foundry. Dies are stacked forming the 3DIC by an OSAT. The second is designed by a fabless design house. The die is manufactured by a commissioned foundry. The die is stacked with a commodity chiplet by an OSAT. Both stacked 3DICs are assembled on an interposer; The S&T threats present in each step are illustrated.

manufacturing process of the first stacked 3DIC. A fabless design house commissions the manufacture of each die to a different foundry. An OSAT then assembles the dies in a stack. The production of the second stack can be seen on the right-hand side of the picture. The process is similar, but this time, a fabless design house commissions a foundry to manufacture one die and buys a second commodity die from a chiplet supplier. The stacking process is also carried out by an OSAT. Finally, the two stacks are assembled on an interposer.

A good analogy for this new scenario would be the current market for motherboard-based systems. A motherboard is a circuit board that contains the various electronic components of a system and enables communication between them. In consumer electronics, it is common for a system to consist of a motherboard, CPU, GPU, memory, controllers, etc., manufactured by different companies. The miniaturization of this scheme would be a chiplet-based IC with an interconnect layer acting as the motherboard and chiplets acting as individual chips.

This industrial transformation requires a revision of hardware S&T understandings, as well as the investigation of possible new security threats. The next Section discusses the S&T threats and defines attacker models against a chiplet-based production chain.

IV. SECURITY & TRUST THREATS AND ATTACKER MODEL

This Section presents the S&T threats that must be resolved to enable a trustworthy transition to the chiplet-based paradigm. The threats can be divided into two main categories: against the hardware integrity and against the IP of the chiplet. Fig. 3 illustrates a possible 3DIC production chain and the threats menacing each step of the production chain. It is important to emphasise that some threats can affect both 2D and chiplet-based 3D designs. However, this overview will focus on the particularities brought by the chiplet paradigm and how it changes our understanding of hardware S&T in these cases. Threats unrelated to chiplets and 3D integration are considered out-of-scope of this survey.

A. HARDWARE INTEGRITY

The integrity of a 3DIC can be defined as the certainty that the system is, in its completeness, intact as measured against its original specification. In this study, we are interested in the following threats to hardware integrity: hardware trojans and malicious chiplets. The difference between the two threats is their origin. Hardware trojans are inserted into the design by an attacker during any design and manufacturing step, while malicious chiplets are originally designed with hidden functionalities with the intention of creating malicious behavior.

Hardware trojans (HT) are unauthorized, malicious inclusions to a hardware design with the aim of compromising its security or causing it to malfunction. They can be designed to trigger specific actions when a certain condition is met, or they can remain inactive until activated by a trigger. Some HTs are activated by a rare internal state of the system, while others can be activated by an environmental condition, such as temperature or electromagnetic radiation [53], [54].

HT insertion is a threat that affects both 2D and 3D ICs. Researchers have demonstrated that inserting a hard-to-detect hardware trojan is possible [55]. However, the topic of HT insertion is more present in the academia than in the industry, and there are only a few actual cases that have been publicly reported. We interpret this fact to mean that critical ICs (which might be targeted by an attacker) are actually manufactured by trusted entities. Because monolithic 2D dies are manufactured by a single foundry (FEOL and BEOL), there are not many entry points for HT insertions for attackers. It would also be easy to trace where in the manufacturing process the HT originated, which would damage the foundry's reputation. Chiplets could change this scenario. If a 3DIC is built using chiplets, the attacker could be located at any of the chiplets manufacturers.

HT insertion on multidie systems is a scenario similar to that of PCBs. In [56], the authors report that a small microchip was illegally inserted into Supermicro's server motherboards. The infected products ended up on the servers of banks, government entities, and big corporations. Like chips on a PCB, chiplets from different manufacturers can be assembled in an interposer or stack. This means that every chiplet on the system and the interposer can be a gateway for the attacker. A deep-dive on HT techniques, types of payloads, and activation mechanisms can be found on [54] and [57].

HT can infect 3DICs during different stages of 3DIC fabrication. The manufacturing process varies greatly depending on the type of 3DIC in question. For the sake of simplicity, this work will decouple it into three main steps: Design, Fabrication and Assembly.

The system design includes the development of chiplets and their integration with off-the-shelf chiplets. An attacker directly involved in the design could easily introduce a HT that would be very difficult to detect. However, it is conventional to assume that the team responsible for the system design is trustworthy. An attacker who is not directly involved in the design could still compromise the integrity of the system by retrieving sensitive information about the system and working in collusion with attackers in other stages of manufacturing.

In the fabrication phase, the dies are produced for later assembly. This process consists of a series of steps that may vary depending on the technology node and type of advanced packaging. In this paper, the fabrication phase is defined as the phase in which the chips are fabricated to be later stacked during the assembly process. In the case of a fabless design house, fabrication can be outsourced to an untrusted foundry. The design house provides the layout in a Graphic Data System II (GDSII) file, which describes the position, size and shape of the transistors as well as the connections and other circuit elements. The attacker in the untrusted foundry possesses the means to modify the layout directly to include the HT [58], [59], [60], [61], [62], [63].

Assembly is the step in the production chain in which the individual chips are stacked together to form the 3DIC. This step varies greatly depending on the advanced packaging technology, as there are several methods for interconnecting the chiplets. This is a sensitive step in the manufacturing of 3DICs in terms of protection against HTs, as the attacker has various ways of inserting malicious circuitry into the system. The HT can be included in the form of an additional chiplet on the interposer or an entire layer on the 3D stack [64], [65]. 3DICs are vulnerable to some unique HT attacks. In TSV-based 3DICs, the TSVs can be used to hide the trigger or payload of an HT [60], [61]. Similarly, 2.5DICs can have their interposer targeted for the inclusion of such threats [60].

Malicious chiplet is a chiplet that contains undisclosed logic designed to act as an adversary within the 3DIC. Chiplets are function-specific circuits that can come in the form of any commodity circuitry, such as microprocessors, memories, crypto-engines, etc. The use of off-the-shelf chiplets brings many advantages for the production of ICs. However, it also represents a major vulnerability to malicious attacks. The chiplet designer has full control over the chiplet design and could add complex functions on the chiplet that are difficult to detect.

It is difficult to precisely define all the ways in which a malicious chiplet can act against the integrity of a system, since a chiplet can contain virtually any type of additional functionality. However, researchers have focused on the misbehaviour of chiplets against data transmitted over shared buses [66], [67]. The presence of untrusted chiplets on a shared bus can pose a threat to integrity as they can modify or divert data transmitted on the bus. The first case refers to a situation where a chiplet intercepts and alters data that is legally exchanged between other chiplets on a shared bus. The second case refers to a situation in which a chiplet reroutes data that is legally exchanged on a shared bus to another chiplet. Chiplets can also passively read data intended for other chiplets on a shared bus, which is referred to as snooping. Finally, chiplets can disguise themselves as other chiplets to gain access to data or services, which is called spoofing. As will be discussed later in this study, the risks of using untrusted chiplets also extend also to the preservation of the IP of the rest of the design.

Initiatives such as DARPA's Common Heterogeneous Integration and Intellectual Property Reuse Strategies (CHIPS) aim to enable and promote a more modular design flow and establish standards for the easy integration of such components [68]. This plug-and-play strategy reduces cost and time-to-market, but increases the risk of a malicious chiplet being integrated due to the lack of verification and hardware S&T solutions for secure chiplet integration. Developing ways to ensure the integrity of 3DICs is an important step towards this new paradigm in the semiconductor industry. HTs are a threat that can affect not only 3DICs, but any type of chip. However, the more decentralized supply chain allowed and incentivized by the economics associated with 3DICs creates more opportunities for an adversary to infect the chip with such malicious inclusions. Additionally, 3D integration

enables miniaturization of the motherboard and chip schema in the form of interconnects and chiplets. In this scenario, chiplets could be bought on the market without any guarantee that they are trustworthy, jeopardizing the trustworthiness of the entire system.

B. INTELLECTUAL PROPERTY

In the context of hardware design, IP defines designs owned by a company and the legal right to use these designs. It is common practice for companies to sell and license the use of their IP. In the chiplet-based IC industry, where chiplet reuse will not only be possible but also encouraged, the protection of chiplet IP becomes essential to this business model. IP theft is a known issue for 2D SoCs and the transition to a chiplet-based production chain could create new opportunities for attackers.

If an attacker were to steal the design of a state-of-the-art 2D SoC, it would be relatively easy to track its sale on the gray market. A large 2D SoC has a number of features that would allow the stolen company to identify its product on the gray market. In addition, the buyer could also notice that the product is similar to the original but comes from a different source. However, in a decentralized chiplet-based production chain, where a modern 3DIC consists of multiple chiplets, an adversary could steal the design of one of the many chiplets. It would be easier to sell a generic chiplet on the gray market than a large 2D SoC.

It can be assumed that several sources would sell generic function-specific chiplets. Therefore, the theft would masquerade as another genuine source. In this case, the buyer would be a victim of the untrusted chiplet threat model. Large 2D SoCs, on the other hand, are manufactured by fewer companies and have a more distinctive set of features than a generic chiplet. In this case, a large 2D SoC sold by an unreputed source would be suspicious. It is also reasonable to assume that state-of-the-art 2D SoC designs with important design secrets would be manufactured by the few state-of-the-art foundries that have a good reputation in the market.

Furthermore, the monolithic aspect of 2D SoCs requires the entire design to be manufactured in the same manufacturing process. Chiplet-based ICs, however, can be manufactured heterogeneously. To save costs, parts of the design that are not performance-oriented can be outsourced to less reputable foundries. This work highlights the vulnerability of IP theft through reverse engineering during the 3DIC production chain and through overproduction.

Reverse engineering is a process in which a system is analyzed to reveal the details of its functioning [69]. Similar to the inclusion of HTs, the infringement of IP can occur at different stages of the IC lifecycle.

Reverse engineering during the design phase does not usually concern researchers, as most works that explore the security aspects of the IC production chain are written from the perspective of the designers who own the IP and try to protect it during manufacturing, assembly, testing, and in the field. Therefore, the design phase is often considered secure. However, the IP can still be compromised during the design phase by an observer working in collusion with another attacker in a different part of the production chain. The observer can gather information that would help the attacker reverse engineer the system.

Reverse engineering during fabrication is a threat that must be addressed as the outsourcing of chiplet manufacturing will be a common practice due to the ever-increasing complexity and cost of semiconductor manufacturing. During the fabrication phase, the foundry has access to the GDSII that describes the design. Without the use of techniques that would make this more difficult, a skilled attacker can use advanced reverse engineering techniques to retrieve the complete netlist of the system [70].

Reverse engineering during testing also poses a major risk to the IP. An attacker in the test facility would have complete access to the system in a black box fashion. They can excite the functional inputs of the system and observe the outputs to deduce the internal architecture of the system. In addition, the attacker would also have access to the DFT structure. DFT is defined as the hardware structure and its utilisation protocol that enable efficient testing of the design after fabrication.

Fig. 4 (a) shows a circuit with some flip-flops connected to the input/output of the design. In this case, it would be easy to write values to these flip-flops to stimulate the combinational circuit and read the result at the output flip-flop. However, there are flip-flops that are not directly accessible via an input/output pin. Their values at a given time would not be known, so it would be difficult to determine the exact cause in the event of a malfunction. Fig. 4 (b) shows the implementation of a full scan chain. In the full scan DFT architecture, the flip-flops are replaced by scan flip-flops and connected in series. In this way, all flip-flops are accessible via a serial input/output.

The usefulness of DFT structures also poses a risk to the IP. The attacker can use hand-crafted test vectors to stimulate the circuit in a way that can expose its internal architecture, unlock keys or cryptographic keys [71], [72]. Contrary to past beliefs, it has been shown that complex DFT structures do not protect against scan attacks [73]. Furthermore, in collusion with an observer in other phases of IC production, this task may become more efficient.

The IEEE 1838 DFT standard [27] defines the hardware infrastructure for pre- and post-bond testing of multidie systems. The standard is die-centric, i.e. each die contains its own DFT specification. When assembled, compliant dies form a DFT network and all DFT elements are accessible via the I/O of the first die in the assembly. Test data is expected to be transmitted to the die under test via the shared serial path, and any die on the stack can modify, divert, sniff or spoof the test data. This allows attackers to perform reverse engineering attacks from inside the 3DIC.

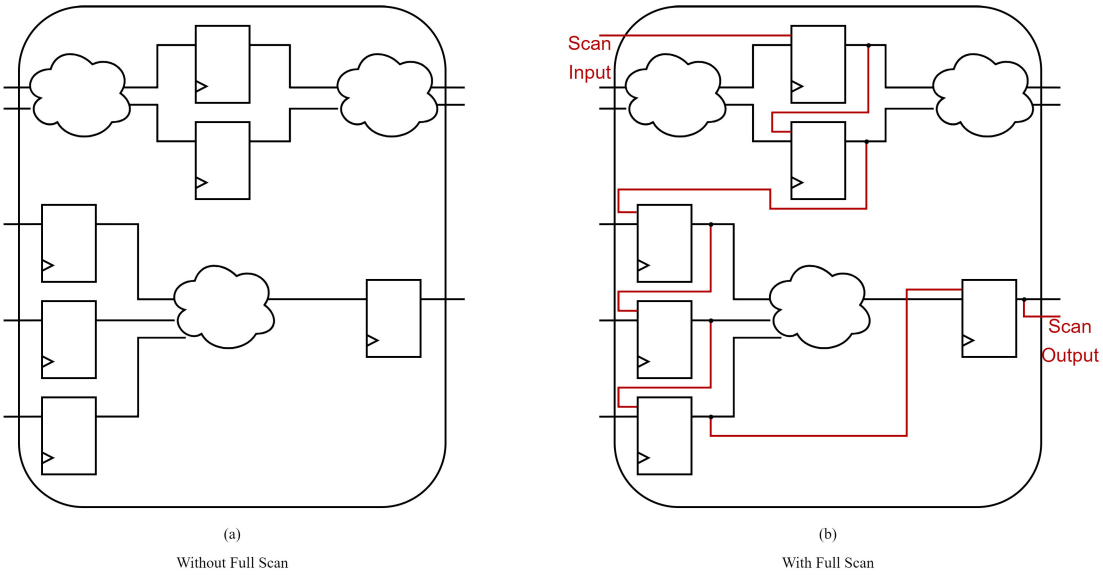

FIGURE 4. Schematic representation of a digital circuit without (a) and with (b) a DFT full scan chain scheme.

TABLE 1. Overview of the works discussed in Section V.

Reference	Threat	Attacker	Solution	Comment
Valamehr et al. [77]	Unstrusted Chiplets Malicious Software	Chiplet vendor Attacker in the field	Monitor die	Requires modification on the monitored die
Sepulveda et al. [78]	Untrusted IPs on 3DNoC	IP vendor	Execution monitor	Concept can be applied on chiplet-based designs
Nabeel et al. [66]	Untrusted Chiplets	Chiplet vendor	Interposer execution monitor	Large active interposers may present poor manufacturing yield
Bilzor et al. [79]	Hardware Trojan	Foundry	Monitor die	Concept can be applied to monitor untrusted chiplets
Alhelaly et al. [65]	Hardware Trojan (Trojan die)	Assembly facility	3D Ring Oscillators	Requires coordination between chiplet vendors
Slpsk et al. [80]	Hardware Trojan Counterfeit Chiplets	Assembly facility	Chiplet locking system based on PUF	PUF signature may change over time due to circuit aging.
Xie et al. [81]	Reverse engineering	Foundry	2.5D split manufacturing	Interposer must be manufactured securely
Patnaik et al. [82]	Reverse engineering	Foundry	3D split manufacturing	Converts a 2D design to a 3D design to protect IP.
Nigussie et al. [83]	Reverse engineering	Foundry	3D split manufacturing Obfuscation	Converts a 2D design to a 3D design to protect IP.
Slpsk et al. [80]	Scan Chain Attack	Testing facility	Scan locking mechanism	Compliant with IEEE 1838 DFT standard

Overproduction, or overbuilding, is another way in which an attacker can infringe IP in the foundry. In this case, the attacker does not try to retrieve information about the design, but rather uses the available layout masks to produce copies of the IC and sell them illegally on the market. It is logical to assume that the attacker would not apply the same quality controls and tests to these overbuilt ICs. The presence of counterfeit and inferior products on the market could therefore damage the reputation of the design company.

V. COUNTERMEASURES

In this Section, hardware and software S&T solutions for 3DICs against different attacker models are presented and discussed. This work explores the S&T countermeasures in the literature that are specific to 3DICs. The literature is rich in studies analyzing the state of the art in SoC S&T [74], [75], [76]. However, solutions purely geared towards SoC are not included in this survey. Table. 1 provides an overview of the work examined in this overview. The countermeasures presented in this Section are divided into three categories: secure chiplet integration, HT detection, and prevention of reverse engineering.

A. SECURE CHIPLET INTEGRATION

The development of methods for the secure integration of commodity chiplets on 3DICs is a crucial step towards the

chiplet-based production chain that academics and industry leaders foresee. In this context, chiplets are expected to be assembled in a plug-and-play fashion. Therefore, S&T solutions should aim at requiring little or no changes to the original design. Three different solutions are presented in this Section: Valamehr et al. proposes an optional security-driven chiplet [77]; Sepulveda et al. proposes a secure 3D Network on Chip (3DNoC) that could inspire chiplet-based solutions [78]; Nabel et al. proposes an interposer-based Root-Of-Trust (RoT) for chiplet assembly [66].

In [77], Valamehr et al. argue in favor of using an additional die to equip the computing hardware with security functions. The proposed countermeasure intends to protect the integrity of the computation from unintentional hardware design flaws or malicious software. The approach is supported by a conjunction of circuit-level primitives first introduced in [84]. The circuits act as signal elevators and allow tapping, disabling, rerouting, and overriding of the signals of the computation die. The novelty of this approach is that it allows the control plane to be completely optional with only a few changes to the computation die. After the addition of the interface circuitry, the computation die should work with and without the security die.

The proposed circuit-level primitives offer a variety of potential applications to improve security. The ''disable'' primitive can be used to isolate an untrusted chiplet from a shared communication bus to protect the exchange of sensitive data. Additionally, all primitives can be used together to monitor the activities of the computation layer in real time and effectively prevent the execution of malicious software. This infrastructure could also be used to augment the computation layer with additional security features. For example, a high-bandwidth cryptographic engine could be implemented in the control layer to enhance the functionality of the system.

The major drawback of this approach is that it requires the addition of TSV-based signal elevators on the computation die. TSVs are large and adding them to the designs may require additional P&R effort. This solution would require coordination between die designers, or a standard for the inclusion and positioning of the signal elevators. Valamehr et al. did not present the physical area and power overheads of the proposed solution.

In [78] Sepulveda et al. present a secure TSV-based 3DNoC. The secure implementation aims to address various threats related to the exchange of sensitive messages over a shared infrastructure. The authors highlight signal modification of data transmitted over TSVs and spying of messages on the shared bus. The security mechanism relies on the concept of hardware firewalls that create ''security zones'' on the 3DIC. Within the security zones, the components are considered trusted and can exchange information without security checks. Otherwise, the transactions are encoded and verified by the countermeasure components. This solution enables flexible security, as the firewalls can be expanded or contracted. The software can be mapped to the 3DNoC and its security zones as required.

Versions of the 3DNoC with different security levels are implemented in [78]. The overhead in terms of area ranges between 2% and 12%, while the power overhead is between 2% and 16%, and the latency overhead is from 2% to 16%. The comparison is made against a 3DNoC without the security features. The results suggest that monitoring the exchange of data between untrusted components in a 3DNoC is possible. A similar technique could be used in a chiplet-based 3DNoC with a standard interconnection bus. The concept of flexible firewalls could provide the necessary flexibility to allow the best compromise between performance and security depending on the application. However, the authors do not consider chiplet-based implementations. The same applies to other 3DNoC security countermeasures [85], [86]. An overview of NoC security (including 3DNoC) can be found at [87].

The idea of implementing security features directly in an active interposer is explored in [66]. Nabel et al. implement an active interposer to secure data exchange in the presence of untrusted commodity chiplets. This work addresses the following malicious behaviors: snooping, spoofing, modifying, and diverting, which are part of the man-in-the-middle attacker model [88], as well as unauthorized access and modification of shared memory. The authors assume that this type of malicious behavior can be caused by intentional malicious chiplets, HTs, or unintentional design flaws on chiplets.

The proposed design for the secure integration of untrusted chiplets is based on two key paradigms: physical segregation of components and runtime monitoring of system-level communication. The former is achieved by establishing a bus interface between each component (untrusted chiplets and security infrastructure) and the communication bus. Runtime monitoring is achieved by using a transaction monitor. Each allowed transaction must be explicitly registered in a policy register. Thus, if a compromised chiplet attempts to perform an unauthorized communication or an unauthorized read/write operation in shared memory, the action is blocked by the transaction monitor and the bus interface, protecting the system from malicious behavior.

All security countermeasures are implemented directly on the active interposer. This approach is consistent with the concept of using chiplets as plug-and-play commodity. Logically, as the number of policies to be monitored increases, the interposer becomes more and more resource-hungry. The results show that doubling the number of policies doubles the additional cost of the interposer in terms of die area, power consumption, and wire length. However, the critical delay grows linearly, indicating good scalability in terms of performance.

The authors demonstrate that the solution is able to protect against the proposed attacker model. The bus interface prevents chiplets from illegally reading data from the bus.

Runtime monitoring of transactions between chiplets seems to be a promising path towards secure chiplet integration. However, the need to create a policy for each allowed transaction can become a development bottleneck for complex systems. There are also concerns about manufacturing yield for large active interposers. The authors do not evaluate the level of activity of the interposer and how this would affect yield. The authors reported a 13% overhead in power and 9% overhead in standard cell area when comparing the secure 2.5D implementation against the unsecured implementation.

B. HARDWARE TROJAN DETECTION

HT insertion is not a threat specific to 3DICs. However, the decentralized production chain of 3DICs introduces new entry points for attackers. Such malicious modifications may not be completely preventable. Therefore, the development of techniques to detect HTs is crucial. In this Section, hardware solutions for detecting HT on 3DICs are presented and discussed: Bilzor proposes an additional die that can detect one type of HT [79]; Alhelaly et al. proposes different techniques for detecting a trojan die in a stack [65]; Slpsk et al. proposes the use of Physical Unclonable Function (PUF) to detect malicious modifications [80].

In one of the first published works on the subject of advanced packaging S&T, Bilzor [79] proposes to extend the S&T features of a design by stacking an optional S&T die. The proposed solution consists of an execution monitor that checks the integrity of the computation die execution. It is designed to protect the control flow logic of the processor from physical tampering. Each transition of the processor's finite state machine (FSM) and each change in the processor's signal set is checked against a previously built lookup table. An unauthorized state transition or an unexpected signal change in a given state triggers a violation flag. One of the advantages of working with chiplets is the extension of the functionality of a design by stacking an optional chipplet. This paper lacks a consideration of the feasibility of the proposed solution in a plug-and-play fashion. It also lacks a demonstration of the solution in a complex system.

A particular type of HT that only affects 3DICs is a trojan die on a chiplet stack. An untrusted assembly facility could insert a trojan die on a stack, just as a trojan chip can be inserted on a PCB. In [65], Alhelaly et al. explore the use of a 3D ring oscillator to reliably detect the additional delay caused by a trojan die on the 3D stack. The different approaches investigated are shown in Figure 5.

The first proposed method consists of n - 1 ring oscillators, where n is the number of dies in the stack. The first ring oscillator measures the delay from die 1 to die 2, the second from die 1 to die 3 and the last from die 1 to die n. Fig. 5 (a) illustrates this approach in a trojan-free 3DIC and Fig. 5 (b) shows the scheme in the presence of an HT. This technique prevents the confusion of a faulty TSV in one of the ring oscillators with a trojan die. It also allows the detection of the location of the trojan die. In addition, this approach has the advantage that all ring oscillator tests can be controlled by the base die. However, a major disadvantage of this method is the necessity of coordination from designers of the chiplets who must provide suitable ring oscillator connections on each die.

As an alternative, the authors also propose the use of smaller ring oscillators that include fewer dies in the stack. The first ring oscillator measures the delay from die 1 to 2, the second from die 2 to 3 and the last from die n -1 to n. In this way, less coordination is required on the part of the chiplet designers to make room for the test TSVs and the ring oscillator components. The scheme is illustrated in Fig. 5 (c) in the absence of an HT, and in Fig. 5 (d) with a trojan die 2 and 3. This approach reduces the coordination effort between the designers of each die. In addition, the components of the ROs are distributed on different dies, instead of placing all components on the bottom die.

The authors also discuss the possibility of including multiple TSVs for a single 3D ring oscillator between two dies as shown in Fig. 5 (a) without HT and (b) with a trojan die. This test structure is explored in order to deal with the case where the attacker tries to hide the delay introduced by a trojan die by changing the physical properties of the TSVs. By reducing the latency of the TSV (which is often designed pessimistically to maintain yield), an attacker could insert a trojan die with little impact on delay, making it indistinguishable from random process variations. However, when multiple TSVs are inserted into the same ring oscillator, the impact on delay increases, making the presence of a trojan die evident.

This approach has proven to be efficient. The results show that the proposed test structure can reliably detect the presence of a trojan die even in the presence of random process variations of up to 10%. However, it depends on each die of the stack having the appropriate infrastructure. For an in-house design, this should be feasible. However, it is difficult to imagine it becoming a standard feature on chiplets as it requires coordination between different designers. An evaluation of the area overhead for each RO scheme is necessary to better present the tradeoff of such techniques.

As part of an extensive asset management infrastructure, Slpsk et al. [80] presented a S&T solution against piracy and counterfeiting attacks[1] during assembly. The solution takes into account that the untrusted assembler can insert, modify, or replace chiplets in the original design. The solution also includes features to protect against reverse engineering attacks during testing (see Section IV-B).

During the pre-bond test, a boundary-scan PUF [89] challenge vector is applied for each IP of the die. The signature of all IPs composes the signature of the layer. The signature of all layers compose the signature of the 3DIC. The 3DIC signature is used to encrypt all security metadata used to

[1]Although piracy and counterfeiting may sometimes refer to IP theft through overproduction, in this case, the authors refers to the replacement or modification of the original design.

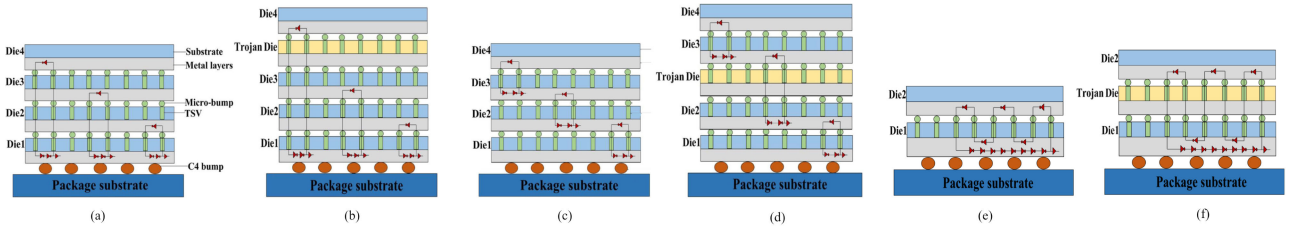

FIGURE 5. Three trojan detection methods using ROs. (a), (c), and (e) shows the respective approach without a trojan die; (b), (d) and (f) shows the respective approach with a trojan die on the stack; Image adapted from [65].

unlock the individual chiplets after assembly. A malicious modification during integration could potentially disrupt the boundary-scan path. In this case, the PUF signature would change, and it would not be possible to decrypt the chiplets' unlocking metadata.

The PUF solution implemented in this work can generate a unique and collision-resistant signature with low overhead. However, the reliability of PUFs over a long period of time still needs to be demonstrated. A common concern with this type of solution is that the signature may change over time due to circuit degradation. Furthermore, it is not clear whether a malicious modification to the original circuit actually disrupts the PUF signature, since the signature takes into account only the paths between the flip-flops of the boundary-scan chain. The power and area overhead of the complete solution (including the features presented in Section IV-B) are 36% and 13%, respectively.

C. REVERSE ENGINEERING PREVENTION

As discussed in Section IV, 3DICs inherit some vulnerabilities from traditional SoCs, including risks such as HT insertion and IP theft. However, as outlined in Section II, the manufacture of the chiplet itself is no different from the manufacture of a traditional 2D SoC, apart from its size, which is expected to be smaller. Therefore, IP protection and HT prevention solutions for 2D SoCs should also be considered for the secure manufacturing of chiplets. Mitigation techniques against both threats assume that it is necessary to understand the design in order to steal IP information or insert meaningful HT. Solutions to prevent reverse engineering therefore include split manufacturing [90], circuit obfuscation [91], and logic locking [92].

3D integration technology can be used to prevent reverse engineering and thus protect against HT insertions and IP theft. There are several papers in the literature that explore the concept of converting a 2D SoC design into a 3DIC design to prevent reverse engineering during manufacturing. All work assumes that the foundry or foundries commissioned to perform the FEOL processes are not trustworthy. However, the BEOL and assembly processes normally need to be performed in a trusted environment. The following approaches have been recently proposed: the 2.5D split manufacturing method proposed by Xie et al. [81]; The two different 3D split manufacturing method proposed by Patnaik et al. [82] and Nigussie et al. [83]; the IEEE 1838-compliant scan chain locking method proposed by Slpsk et al. [80].

In [81], Xie et al. propose a security-aware 2.5D split manufacturing methodology. The approach consists of dividing the design into two chiplets that can be manufactured by an untrusted foundry. The novelty of this approach is to mount the chiplets on an interposer. The authors assume that an attacker would use a proximity attack [93] and a Boolean satisfiability problem attack (SAT attack) [94] to derive the interposer connection between the chiplets, and thus expose the operation of the entire system. Therefore, the authors propose methods to divide the elements of the original design into two groups such a way that would difficult SAT attacks the most and to place the design elements on each chiplet in such a way that would difficult proximity attacks the most. The authors applied the technique on a set of benchmark circuits and were able to protect against the attacker model. On average, the solution caused a 3% area overhead and 25% power overhead.

Patnaik et al. [82] and Nigussie et al. [83] take a similar approach by partitioning the design into two dies, and stacking the dies in a 3DIC with obfuscated interconnects. In addition to the partitioning method, [82] proposes to use randomly placed F2F vias and obfuscated switchboxes on the interconnection layer. While [83] also proposes to apply different obfuscation techniques such as function and lookup table obfuscation or inserting redundant logic according to the best practices of the literature [95], [96], [97], [98]. This ad hoc approach to the obfuscation technique makes it possible to optimize the proposed procedure for each application. However, it also makes the presented results less generalizable.

Finally, we would like to highlight the solution presented in [80] for reverse engineering by preventing scan chain attacks. Slpsk et al. implemented the scan chain protection mechanism first presented in [99]. The solution consists of feeding the output of N scan flip-flops to a pattern matching block (PMB). To unlock the output of the scan chain, you need to push a bitstream through the scan chain that contains the M unlock patterns required by the PMB. Without knowing information about the selected scan flip-flops or the PMB, it is virtually impossible to guess the M unlock vectors of size N. If an attacker were to try to provide random test vectors, the probability of guessing the one key of length N would

be $1/2^N$. Since there are M keys, the probability would drop to $1/2^{N*M}$. The novelty of [80] is that it is compliant with the IEEE 1838 DFT standard for 3DICs.

VI. DISCUSSION

There are many benefits in building chips with chiplets. The chip-based approach will gain popularity with the popularisation of 2.5D and 3D heterogeneous integration. This will create many commercial opportunities that will lead to a chiplet market. The commercialization of chiplets would reduce manufacturing costs and time-to-market in the same way that the commercialization of IP for 2D SoCs has done. This scenario creates an incentive for attackers to attempt to infect the market with malicious chiplets, necessitating techniques for secure chiplet integration. For example, in [66], the authors implement an interesting proof of concept where chiplets are integrated into an AHB-Lite bus, along with hardware S&T countermeasures against possible misbehaviour of chiplets. Implementing S&T features, such as transaction monitoring, on an active interposer seems to be the best approach for secure chiplet integration. There are also other approaches, such as extending the functionality of the design by adding a control die. However, it is not yet clear how to do this in a plug-and-play fashion. In addition, progress has recently been made in the standardization of chiplet interconnects, with the Universal Chiplet Interconnect Express (UCIe) [100] emerging as the best option. Hardware S&T countermeasures for chiplets integration should aim to be compliant with the UCIe specification, but as far as we know, there is no such work in the literature.

HT is a threat that affects both 2D and 3D ICs. However, the 3D paradigm allows for scenarios where there are multiple entry points for attackers. One can easily imagine a scenario where a fabless design house designs a 3DIC using different dies manufactured by different foundries. By taking the precautionary approach of assuming that no system is 100% secure, HT detection mechanisms should be at 3DIC designers' disposal. From the literature, it appears that the most appropriate approach is to add hardware infrastructure that can change its behavior in the presence of such inclusions, such as PUFs and ring oscillators. The solutions presented in Section V-B rely on signal propagation timing to detect the presence of HTs. Although the work has efficiently demonstrated their solutions, their reliability over long periods of time has yet to be demonstrated, especially for PUFs.

HT prevention techniques are also needed to mitigate the efforts of bad actors in untrusted foundries. Design obfuscation through split manufacturing is a technique that has been efficiently explored in the HT prevention literature. It is based on the idea that it is necessary to understand the system in order to insert meaningful HT. Reference [82] proposes flows to partition the design such that design obfuscation is achieved while keeping the overhead reasonable. However, this work suffers from the lack of EDA tools that support non-2D designs, which requires the development of a flow that utilises conventional EDA tools. Adequate support from EDA tools is important to achieve scalability, especially for S&T features that are often considered optional.

3DICs not only have a production chain that is more prone to HT insertion, but also more places to hide a HT. The interposer on 2.5DICs and the TSVs on 3DICs can hide the trigger or payload of an HT. To the best of our knowledge, solutions to this type of threat have not yet been published.

IP protection is also critical to the viability of the chiplet ecosystem under discussion. IP theft is not a problem exclusive to 3DICs, but may have different implications in this context. An attacker may be more interested in stealing a commodity chiplet that can be easily sold on the open market than a complete end product that may be easier to trace or already have an internal S&T function implemented. The grey market for ICs is already an ongoing concern for product quality. Grey market suppliers sell returned, obsolete, defective or counterfeit units. In fact, studies suggest that the market for counterfeit ICs is worth over 75 billion dollars worldwide [101]. As the IC production chain becomes decentralised and the chiplet market evolves, this issue will only grow [102]. Furthermore, in times of high demand, OEMs may relax their quality control procedures or S&T constraints to avoid losing market share. They could end up relying on inferior components from the grey market.

As discussed in Section IV, the threats of HT insertion and IP theft overlap in many ways. Therefore, solutions for one threat may also be applicable to the other, as the literature indicates that the threat model for both threats involves the attacker gaining privileged information about the system through some sort of reverse engineering technique. Design obfuscation through split manufacturing has been explored to prevent untrusted foundries from retrieving design secrets. The concept is analogous to HT prevention, where researchers try to find the best technique to split the system into multiple dies and obfuscate the connection between the dies. It could be observed that both [81], [83] had to construct a 2.5D and a 3D split manufacturing flow using 2D EDA tools. The researchers will need to extend their work to leverage 3D-specific EDA tools once they become widely available.

Secure testing of 2.5DICs and 3DICs is a missing milestone towards the popularization of such designs. 3DICs must be tested pre- and post-bond, adding one testing phase to the traditional SoC testing scheme. This provides more opportunities for an attacker. In addition, untrusted chiplets or HTs could go undetected during testing, which could lead to theft of test information. The IEEE 1838 DFT standard defines the test infrastructure required for testing 3DICs. However, it does not specify any security protocols. The authors in [80] implement a simple but efficient scan chain locking technique. However, a secure implementation of the IEEE 1838 infrastructure has not yet been published.

There is a lack of methods for secure communication between the chiplet and the outside of the 3DIC. In a stack, the only communication path with the chiplet may be a shared interposer or DFT network. Thus, any confidential communication directed to the chiplet is exposed to the other components of the design. Such an infrastructure could be used to avoid overproduction of chiplets. A chiplet could require an activation key that is transmitted from the IP owner to the chiplet via the secure communication mechanism. Indeed, the overproduction of 3DICs is an issue that still needs to be explored. Foundries could overproduce chiplets to sell them illegally on the grey market. Techniques to prevent this type of IP theft may include logic locking of chiplets and authentication of users during the test phase or even after deployment in the field.

Finally, this work has not addressed the problem of side channels, fault injection, and other physical attacks. However, 3DICs can also provide opportunities as the stacked structure can be more resilient to these types of threats [103], [104], [105], [106], [107].

VII. CONCLUSION

In this work, we introduced the different types of 3DICs and the specifics of their manufacturing processes and supply chains. We also show how vulnerable the 3D supply chain can be to various threats. We divide these threats into two main categories: against the integrity of the system and against intellectual property. The first category includes untrusted chiplets and HTs. The second category includes theft of IP during manufacturing, integration, and testing. We also present and discuss the state-of-the-art hardware and software countermeasures against various threat models. We come to the following conclusions:

- Additional dies can be assembled on a 3DIC to provide optional S&T features, but it is not known how this can be done in a plug-and-play fashion.
- An active interposer with integrated S&T features may be the best approach for secure chiplet integration.
- HT detection solutions rely on techniques that may become unreliable as the chip ages.
- HT insertion and IP theft can be mitigated by preventing reverse engineering attacks.
- Design obfuscation through 3D split manufacturing can be used to secure a 2D SoC design by converting it into a 3DIC.
- There is an opportunity for the development of hardware infrastructures for secure chiplet integration that are compliant with the emerging UCIe standard.
- There is a need for a secure post-bond test procedure that is compliant with the IEEE 1838 DFT standard.
- There is a research gap in secure communication mechanisms with a chiplet on a stack.

We have shown that there are multiple entry points for attackers in the 3DIC production chain. Many papers have been published that extend the understanding of the know-how to build trustworthy chiplet-based systems, but various proposed solutions are still far from industrial application. The actual 3DIC production is mainly vertical. Companies assemble their own chiplets in 2.5D and 3D. Therefore, many topics related to the multidie system S&T still need to be explored. However, initiatives such as DARPA and the collaboration between OCP and JEDEC form the basis for the expectation that a chiplet-based production chain will form. We expect significant growth in the 3DIC hardware S&T field as chiplet-based systems enter the market.

REFERENCES

[1] G. E. Moore, "Cramming more components onto integrated circuits, reprinted from electronics, volume 38, number 8, April 19, 1965, pp.114 ff." *IEEE Solid-State Circuits Soc. Newslett.*, vol. 11, no. 3, pp. 33–35, Sep. 2006.

[2] T. N. Theis and H.-S. P. Wong, "The end of Moore's law: A new beginning for information technology," *Comput. Sci. Eng.*, vol. 19, no. 2, pp. 41–50, Mar. 2017.

[3] H. Wong, "On the CMOS device downsizing, more Moore, more than Moore, and more-than-Moore for more Moore," in *Proc. IEEE 32nd Int. Conf. Microelectron. (MIEL)*, Sep. 2021, pp. 9–15.

[4] W. Arden, M. Brillouët, P. Cogez, M. Graef, B. Huizing, and R. Mahnkopf, "More-than-Moore white paper," *White Paper*, vol. 1, pp. 1–31, Jan. 2010.

[5] T. Li, J. Hou, J. Yan, R. Liu, H. Yang, and Z. Sun, "Chiplet heterogeneous integration technology—Status and challenges," *Electronics*, vol. 9, no. 4, p. 670, Apr. 2020.

[6] D. Dutoit, "Chiplet partitioning can balance among performance, flexibility, and scalability," Chiplet Summit, San Jose, CA, USA, Tech. Rep. A-201, Jan. 2023.

[7] I. Cutress, "Intel's process roadmap to 2025: With 4 nm, 3 nm, 20 A and 18 A?!" AnandTech, New York, NY, USA, Oct. 2016. [Online]. Available: https://www.anandtech.com/show/16823/intel-accelerated-offensive-process-roadmap-updates-to-10nm-7nm-4nm-3nm-20a-18a-packaging-foundry-emib-foveros

[8] *AMD Ryzen™ 7 5800X3D Gaming Processor*, AMD, Santa Clara, CA, USA, 2022. Accessed: Oct. 16, 2023. [Online]. Available: https://www.amd.com/en/products/cpu/amd-ryzen-7-5800x3d

[9] *Apple Announces Mac Transition to Apple Silicon*, Apple, Cupertino, CA, USA, 2020. Accessed: Oct. 16, 2023. [Online]. Available: https://www.apple.com/newsroom/2020/06/apple-announces-mac-transition-to-apple-silicon/

[10] S. Dickens, "Tesla's Dojo supercomputer: A paradigm shift in supercomputing?" Forbes, Jersey City, NJ, USA, 2023. Accessed: Oct. 16, 2023. [Online]. Available: https://www.forbes.com/sites/stevendickens/2023/09/11/teslas-dojo-supercomputer-a-paradigm-shift-in-supercomputing/

[11] O. Peckham, "Chinese startup Biren details BR100 GPU," HPCwire, San Diego, CA, USA, Oct. 2023. [Online]. Available: https://www.hpcwire.com/2022/08/22/chinese-startup-biren-details-br100-gpu/

[12] A. Mastroianni, B. Kerr, J. Nasrullah, K. Cameron, H. J. Wong, D. Ratchkov, and J. Reynick, "Proposed standardization of heterogenous integrated chiplet models," in *Proc. IEEE Int. 3D Syst. Integr. Conf. (3DIC)*, Oct. 2021, pp. 1–8.

[13] G. Adeline, "JEDEC and open compute project foundation pave the way for a new era of chiplet innovation," Yole Group, Villeurbanne, France, Oct. 2023. [Online]. Available: https://www.yolegroup.com/industry-news/jedec-and-open-compute-project-foundation-pave-the-way-for-a-new-era-of-chiplet-innovation/

[14] D. Stow, Y. Xie, T. Siddiqua, and G. H. Loh, "Cost-effective design of scalable high-performance systems using active and passive interposers," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2017, pp. 728–735.

[15] *Overview of Active Interposers*, Syst. Anal., Cadence, San Jose, CA, USA, 2023. Accessed: Jan. 10, 2024. [Online]. Available: https://resources.system-analysis.cadence.com/blog/overview-of-active-interposers

[16] P. Vivet, C. Bernard, E. Guthmuller, I. Miro-Panades, Y. Thonnart, and F. Clermidy, "Interconnect challenges for 3D multi-cores: From 3D network-on-chip to cache interconnects," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI*, Jul. 2015, pp. 615–620.

[17] P. Coudrain et al., "Active interposer technology for chiplet-based advanced 3D system architectures," in *Proc. IEEE 69th Electron. Compon. Technol. Conf. (ECTC)*, May 2019, pp. 569–578.

[18] A. Kannan, N. E. Jerger, and G. H. Loh, "Enabling interposer-based disintegration of multi-core processors," in *Proc. 48th Annu. IEEE/ACM Int. Symp. Microarchitecture (MICRO)*, Dec. 2015, pp. 546–558.

[19] S. K. Goel, S. Adham, M.-J. Wang, J.-J. Chen, T.-C. Huang, A. Mehta, F. Lee, V. Chickermane, B. Keller, T. Valind, and E. J. Marinissen, "Test and debug strategy for TSMC CoWoS^{TM} stacking process based heterogeneous 3D IC: A silicon case study," in *Proc. IEEE Int. Test Conf. (ITC)*, Sep. 2013, pp. 1–10.

[20] R. Wang, Z. Li, S. Kannan, and K. Chakrabarty, "Pre-bond testing of the silicon interposer in 2.5D ICs," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2016, pp. 978–983.

[21] M. Taouil, S. Hamdioui, J. Verbree, and E. J. Marinissen, "On maximizing the compound yield for 3D wafer-to-wafer stacked ICs," in *Proc. IEEE Int. Test Conf.*, Nov. 2010, pp. 1–10.

[22] S. Reda, G. Smith, and L. Smith, "Maximizing the functional yield of wafer-to-wafer 3-D integration," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 17, no. 9, pp. 1357–1362, Sep. 2009.

[23] B. Akesson, P.-C. Huang, F. Clermidy, D. Dutoit, K. Goossens, Y.-H. Chang, T.-W. Kuo, P. Vivet, and D. Wingard, "Memory controllers for high-performance and real-time MPSoCs requirements, architectures, and future trends," in *Proc. 9th IEEE/ACM/IFIP Int. Conf. Hardw./Softw. Codesign Syst. Synth. (CODES+ISSS)*, Oct. 2011, pp. 3–12.

[24] J.-M. Lin and C.-Y. Huang, "General floorplanning methodology for 3D ICs with an arbitrary bonding style," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2018, pp. 1199–1202.

[25] M.-F. Lai, S.-W. Li, J.-Y. Shih, and K.-N. Chen, "Wafer-level three-dimensional integrated circuits (3D IC): Schemes and key technologies," *Microelectronic Eng.*, vol. 88, no. 11, pp. 3282–3286, Nov. 2011.

[26] E. Beyne, "The 3-D interconnect technology landscape," *IEEE Des. Test. IEEE Des. Test. Comput.*, vol. 33, no. 3, pp. 8–20, Jun. 2016.

[27] *IEEE Standard for Test Access Architecture for Three-Dimensional Stacked Integrated Circuits*, IEEE Standard 1838-2019, 2020, pp. 1–73.

[28] *Virtex 7 FPGA Family*, AMD, Santa Clara, CA, USA, 2011. Accessed: Oct. 18, 2023. [Online]. Available: https://www.xilinx.com/products/silicon-devices/fpga/virtex-7.html

[29] *CoWoS®—Taiwan Semiconductor Manufacturing Company Limited*, TSMC, Hsinchu City, Taiwan, 2020. Accessed: Oct. 18, 2023. [Online]. Available: https://3dfabric.tsmc.com/english/dedicatedFoundry/technology/cowos.htm

[30] L. Li, P. Chia, P. Ton, M. Nagar, S. Patil, J. Xue, J. Delacruz, M. Voicu, J. Hellings, B. Isaacson, M. Coor, and R. Havens, "3D SiP with organic interposer for ASIC and memory integration," in *Proc. IEEE 66th Electron. Compon. Technol. Conf. (ECTC)*, May 2016, pp. 1445–1450.

[31] E. Sperling, "Return of the organic interposer," *Semicond. Eng.*, Aug. 2018. Accessed: Jan. 10, 2024. [Online]. Available: https://semiengineering.com/return-of-the-organic-interposer/

[32] M. Tanaka, S. Kuramochi, T. Tai, Y. Sato, and N. Kidera, "High frequency characteristics of glass interposer," in *Proc. IEEE 70th Electron. Compon. Technol. Conf. (ECTC)*, Jun. 2020, pp. 601–610.

[33] L. Brusberg, J. R. Grenier, S. E. Kocabas, A. R. Zakharian, L. W. Yeary, D. W. Levesque, B. J. Paddock, R. A. Bellman, R. M. Force, C. C. Terwilliger, C. G. Sutton, J. S. Clark, and K. Rousseva, "Glass interposer for high-density photonic packaging," in *Proc. Opt. Fiber Commun. Conf. Exhib. (OFC)*, Mar. 2022, pp. 1–3.

[34] M. LaPedus, "Paving the way to chiplets," *Semicond. Eng.*, Apr. 2022. Accessed: Jan. 15, 2024. [Online]. Available: https://semiengineering.com/paving-the-way-to-chiplets/

[35] R. Doering and Y. Nishi, "Limits of integrated-circuit manufacturing," *Proc. IEEE*, vol. 89, no. 3, pp. 375–393, Mar. 2001.

[36] M. LaPedus and E. Sperling, "Making chips at 3 nm and beyond," *Semicond. Eng.*, Apr. 2020. Accessed: Oct. 5, 2023. [Online]. Available: https://semiengineering.com/making-chips-at-3nm-and-beyond/

[37] J. Hertz, "Scaling down to 3 nm will require advances in fabrication technology," Allaboutcircuits, Mar. 2021. Accessed: Oct. 5, 2023. [Online]. Available: https://www.allaboutcircuits.com/news/scaling-down-3nm-require-advances-fabrication-technology/

[38] D. Velenis, M. Stucchi, E. J. Marinissen, B. Swinnen, and E. Beyne, "Impact of 3D design choices on manufacturing cost," in *Proc. IEEE Int. Conf. 3D Syst. Integr.*, Sep. 2009, pp. 1–5.

[39] L. T. Su, S. Naffziger, and M. Papermaster, "Multi-chip technologies to unleash computing performance gains over the next decade," in *IEDM Tech. Dig.*, Dec. 2017, pp. 1.1.1–1.1.8.

[40] Y. Feng and K. Ma, "Chiplet actuary: A quantitative cost model and multi-chiplet architecture exploration," 2022, *arXiv:2203.12268*.

[41] F. Sheikh, R. Nagisetty, T. Karnik, and D. Kehlet, "2.5D and 3D heterogeneous integration: Emerging applications," *IEEE Solid StateCircuits Mag.*, vol. 13, no. 4, pp. 77–87, Fall. 2021.

[42] R. Farber, "Chiplets will revolutionize the HPC sector," Data Centre Dyn. Ltd, London, U.K., Oct. 2022. Accessed: Jan. 10, 2024. [Online]. Available: https://www.datacenterdynamics.com/en/opinions/chiplets-will-revolutionize-the-hpc-sector/

[43] K. Larsen, "High-performance computing drives demand for chiplets," *Semicond. Eng.*, Sep. 2021. Accessed: Oct. 5, 2023. [Online]. Available: https://semiengineering.com/3d-ic-opportunities-challenges-and-solutions/

[44] P. Vivet et al., "IntAct: A 96-core processor with six chiplets 3D-stacked on an active interposer with distributed interconnects and integrated power management," *IEEE J. Solid-State Circuits*, vol. 56, no. 1, pp. 79–97, Jan. 2021.

[45] M.-S. Lin, T.-C. Huang, C.-C. Tsai, K.-H. Tam, K. C. Hsieh, C.-F. Chen, W.-H. Huang, C.-W. Hu, Y.-C. Chen, S. K. Goel, C.-M. Fu, S. Rusu, C.-C. Li, S.-Y. Yang, M. Wong, S.-C. Yang, and F. Lee, "A 7-nm 4-GHz arm-core-based CoWoS chiplet design for high-performance computing," *IEEE J. Solid-State Circuits*, vol. 55, no. 4, pp. 956–966, Apr. 2020.

[46] W. J. Dally, "Future directions for on-chip interconnection networks," in *Proc. OCIN Workshop*, 2006, pp. 1–29.

[47] T. M. Coughlin and W. R. Tonti, "Computing nearer to data," *Computer*, vol. 55, no. 7, pp. 82–87, Jul. 2022.

[48] J. H. Lau, "Recent advances and trends in advanced packaging," *IEEE Trans. Compon., Packag., Manuf. Technol.*, vol. 12, no. 2, pp. 228–252, Feb. 2022.

[49] R. Munoz, "Furthering Moore's law integration benefits in the chiplet era," *IEEE Design Test*, vol. 41, no. 1, pp. 81–90, Feb. 2024.

[50] J. Macri, "AMD's next generation GPU and high bandwidth memory architecture: FURY," in *Proc. IEEE Hot Chips 27 Symp. (HCS)*, Aug. 2015, pp. 1–26.

[51] K. Larsen, "3D IC: Opportunities, challenges, and solutions," *Semicond. Eng.*, Sep. 2021. Accessed: Oct. 5, 2023. [Online]. Available: https://semiengineering.com/3d-ic-opportunities-challenges-and-solutions/

[52] K. Larsen, "What is 3DIC technology?—How does it work?" Synopsys, Sunnyvale, CA, USA. Accessed: Oct. 4, 2023. [Online]. Available: https://www.synopsys.com/glossary/what-is-3dic.html

[53] V. V. Rao, A. Sasan, and I. Savidis, "Analysis of the security vulnerabilities of 2.5-D and 3-D integrated circuits," in *Proc. 23rd Int. Symp. Quality Electron. Design (ISQED)*, Apr. 2022, pp. 1–7.

[54] Z. Zhang and Q. Yu, "Modeling hardware trojans in 3D ICs," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI (ISVLSI)*, Jul. 2019, pp. 483–488.

[55] S. Bhunia and M. Tehranipoor, *The Hardware Trojan War*. Cham, Switzerland: Springer, 2018.

[56] D. Mehta, H. Lu, O. P. Paradis, M. S. M. Azhagan, M. T. Rahman, Y. Iskander, P. Chawla, D. L. Woodard, M. Tehranipoor, and N. Asadizanjani, "The big hack explained: Detection and prevention of PCB supply chain implants," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 16, no. 4, pp. 1–25, Oct. 2020.

[57] Z. Zhang, J. Dofe, P. Yellu, and Q. Yu, "Comprehensive analysis on hardware trojans in 3D ICs: Characterization and experimental impact assessment," *Social Netw. Comput. Sci.*, vol. 1, no. 4, pp. 1–13, Jul. 2020.

[58] S. F. Mossa, S. R. Hasan, and O. Elkeelany, "Hardware trojans in 3-D ICs due to NBTI effects and countermeasure," *Integration*, vol. 59, pp. 64–74, Sep. 2017.

[59] S. R. Hasan, S. F. Mossa, O. S. A. Elkeelany, and F. Awwad, "Tenacious hardware trojans due to high temperature in middle tiers of 3-D ICs," in *Proc. IEEE 58th Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Aug. 2015, pp. 1–4.

[60] J. Dofe, Q. Yu, H. Wang, and E. Salman, "Hardware security threats and potential countermeasures in emerging 3D ICs," in *Proc. Int. Great Lakes Symp. VLSI (GLSVLSI)*, May 2016, pp. 69–74.

[61] J. Dofe, P. Gu, D. Stow, Q. Yu, E. Kursun, and Y. Xie, "Security threats and countermeasures in three-dimensional integrated circuits," in *Proc. Great Lakes Symp. VLSI*, Banff, AB, Canada. New York, NY, USA: Association for Computing Machinery, May 2017, pp. 321–326.

[62] P.-L. Yang and M. Marek-Sadowska, "Making split-fabrication more secure," in *Proc. IEEE/ACM Int. Conf. Computer-Aided Design (ICCAD)*, Nov. 2016, pp. 1–8.

[63] S. Madani and M. Bayoumi, "A security-aware pre-partitioning technique for 3D integrated circuits," in *Proc. 18th Int. Workshop Microprocessor SOC Test Verification*, Dec. 2017, pp. 57–61.

[64] S. Alhelaly, J. Dworak, T. Manikas, P. Gui, K. Nepal, and A. L. Crouch, "Detecting a trojan die in 3D stacked integrated circuits," in *Proc. IEEE North Atlantic Test Workshop (NATW)*, May 2017, pp. 1–6.

[65] S. Alhelaly, J. Dworak, K. Nepal, T. Manikas, P. Gui, and A. L. Crouch, "3D ring oscillator based test structures to detect a trojan die in a 3D die stack in the presence of process variations," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 2, pp. 774–786, Apr. 2021.

[66] M. Nabeel, M. Ashraf, S. Patnaik, V. Soteriou, O. Sinanoglu, and J. Knechtel, "2.5D root of trust: Secure system-level integration of untrusted chiplets," *IEEE Trans. Comput.*, vol. 69, no. 11, pp. 1611–1625, Nov. 2020.

[67] M. Nabeel, M. Ashraf, S. Patnaik, V. Soteriou, O. Sinanoglu, and J. Knechtel, "An interposer-based root of trust: Seize the opportunity for secure system-level integration of untrusted chiplets," 2019, *arXiv:1906.02044*.

[68] T. M. Hancock and J. C. Demmin, "Heterogeneous and 3D integration at DARPA," in *Proc. Int. 3D Syst. Integr. Conf. (3DIC)*, Oct. 2019, pp. 1–4.

[69] M. G. Rekoff, "On reverse engineering," *IEEE Trans. Syst., Man, Cybern.*, vol. SMC-15, no. 2, pp. 244–252, Mar. 1985.

[70] R. Torrance and D. James, "The state-of-the-art in semiconductor reverse engineering," in *Proc. 48th ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Jun. 2011, pp. 333–338.

[71] J. Da Rolt, A. Das, G. Di Natale, M.-L. Flottes, B. Rouzeyre, and I. Verbauwhede, "Test versus security: Past and present," *IEEE Trans. Emerg. Topics Comput.*, vol. 2, no. 1, pp. 50–62, Mar. 2014.

[72] J. Da Rolt, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "New security threats against chips containing scan chain structures," in *Proc. IEEE Int. Symp. Hardware-Oriented Secur. Trust*, Jun. 2011, p. 110.

[73] J. Da Rolt, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "Are advanced DfT structures sufficient for preventing scan-attacks?" in *Proc. IEEE 30th VLSI Test Symp. (VTS)*, Apr. 2012, pp. 246–251.

[74] N. Sklavos, R. Chaves, G. Di Natale, and F. Regazzoni, *Hardware Security and Trust*. Cham, Switzerland: Springer, 2017.

[75] M. Tehranipoor, *Emerging Topics in Hardware Security*. Springer, 2021.

[76] M. Alioto, "Trends in hardware security: From basics to ASICs," *IEEE Solid StateCircuits Mag.*, vol. 11, no. 3, pp. 56–74, Summer 2019.

[77] J. Valamehr, T. Sherwood, R. Kastner, D. Marangoni-Simonsen, T. Huffmire, C. Irvine, and T. Levin, "A 3-D split manufacturing approach to trustworthy system development," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 32, no. 4, pp. 611–615, Apr. 2013.

[78] J. Sepulveda, G. Gogniat, D. Flórez, J.-P. Diguet, C. Zeferino, and M. Strum, "Elastic security zones for NoC-based 3D-MPSoCs," in *Proc. 21st IEEE Int. Conf. Electron., Circuits Syst. (ICECS)*, Dec. 2014, pp. 506–509.

[79] M. Bilzor, "3D execution monitor (3D-EM): Using 3D circuits to detect hardware malicious inclusions in general purpose processors," in *Proc. 6th Int. Conf. Inf. Warfare Secur.*, 2011, p. 288.

[80] S. L. P. S. K. Patanjali, S. Ray, and S. Bhunia, "TREEHOUSE: A secure asset management infrastructure for protecting 3DIC designs," *IEEE Trans. Comput.*, 2023.

[81] Y. Xie, C. Bao, and A. Srivastava, "Security-aware 2.5D integrated circuit design flow against hardware IP piracy," *Computer*, vol. 50, no. 5, pp. 62–71, May 2017.

[82] S. Patnaik, M. Ashraf, O. Sinanoglu, and J. Knechtel, "A modern approach to IP protection and trojan prevention: Split manufacturing for 3D ICs and obfuscation of vertical interconnects," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 4, pp. 1815–1834, Oct. 2021.

[83] T. Nigussie, J. C. Schabel, S. Lipa, L. McIlrath, R. Patti, and P. Franzon, "Design obfuscation through 3-D split fabrication with smart partitioning," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 30, no. 9, pp. 1230–1243, Sep. 2022.

[84] J. Valamehr, M. Tiwari, T. Sherwood, R. Kastner, T. Huffmire, C. Irvine, and T. Levin, "Hardware assistance for trustworthy systems through 3-D integration," in *Proc. 26th Annu. Comput. Secur. Appl. Conf.*, Austin, TX, USA. New York, NY, USA: Association for Computing Machinery, Dec. 2010, pp. 199–210.

[85] J. Sepulveda, G. Gogniat, D. Flórez, J.-P. Diguet, C. Pedraza, and M. Strum, "3D-LeukoNoC: A dynamic NoC protection," in *Proc. Int. Conf. ReConFigurable Comput. FPGAs (ReConFig14)*, Dec. 2014, pp. 1–6.

[86] J. Sepúlveda, G. Gogniat, D. Flórez, J.-P. Diguet, R. Pires, and M. Strum, "TSV protection: Towards secure 3D-MPSoC," in *Proc. IEEE 6th Latin Amer. Symp. Circuits Syst. (LASCAS)*, Feb. 2015, pp. 1–4.

[87] A. Sarihi, A. Patooghy, A. Khalid, M. Hasanzadeh, M. Said, and A. A. Badawy, "A survey on the security of wired, wireless, and 3D network-on-chips," *IEEE Access*, vol. 9, pp. 107625–107656, 2021.

[88] M. A. Elakrat and J. C. Jung, "Development of field programmable gate array-based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication network," *Nucl. Eng. Technol.*, vol. 50, no. 5, pp. 780–787, Jun. 2018.

[89] Y. Zheng, A. R. Krishna, and S. Bhunia, "ScanPUF: Robust ultralow-overhead PUF using scan chain," in *Proc. 18th Asia South Pacific Design Autom. Conf. (ASP-DAC)*, Jan. 2013, pp. 626–631.

[90] K. Vaidyanathan, B. P. Das, E. Sumbul, R. Liu, and L. Pileggi, "Building trusted ICs using split fabrication," in *Proc. IEEE Int. Symp. Hardware-Oriented Secur. Trust (HOST)*, May 2014, pp. 1–6.

[91] P.-S. Ba, S. Dupuis, M. Palanichamy, M.-L. Flottes, G. Di Natale, and B. Rouzeyre, "Hardware trust through layout filling: A hardware trojan prevention technique," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI (ISVLSI)*, Jul. 2016, pp. 254–259.

[92] J. Rajendran, A. K. Kanuparthi, M. Zahran, S. K. Addepalli, G. Ormazabal, and R. Karri, "Securing processors against insider attacks: A circuit-microarchitecture co-design approach," *IEEE Des. Test. IEEE Des. Test. Comput.*, vol. 30, no. 2, pp. 35–44, Apr. 2013.

[93] J. Magaña, D. Shi, J. Melchert, and A. Davoodi, "Are proximity attacks a threat to the security of split manufacturing of integrated circuits?" *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 25, no. 12, pp. 3406–3419, Dec. 2017.

[94] P. Subramanyan, S. Ray, and S. Malik, "Evaluating the security of logic encryption algorithms," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2015, pp. 137–143.

[95] D. Forte, S. Bhunia, and M. M. Tehranipoor, *Hardware Protection Through Obfuscation*. Springer, 2017.

[96] B. Colombier and L. Bossuet, "Survey of hardware protection of design data for integrated circuits and intellectual properties," *IET Comput. Digit. Techn.*, vol. 8, no. 6, pp. 274–287, Nov. 2014.

[97] J. Rajendran, H. Zhang, C. Zhang, G. S. Rose, Y. Pino, O. Sinanoglu, and R. Karri, "Fault analysis-based logic encryption," *IEEE Trans. Comput.*, vol. 64, no. 2, pp. 410–424, Feb. 2015.

[98] C. Linn and S. Debray, "Obfuscation of executable code to improve resistance to static disassembly," in *Proc. 10th ACM Conf. Comput. Commun. Secur.*, Oct. 2003, pp. 290–299.

[99] S. Paul, R. Subhra Chakraborty, and S. Bhunia, "VIm-scan: A low overhead scan design approach for protection of secret key in scan-based secure chips," in *Proc. 25th IEEE VLSI Test Symp. (VTS)*, May 2007, pp. 455–460.

[100] D. Das Sharma, G. Pasdast, Z. Qian, and K. Aygun, "Universal chiplet interconnect express (UCIe): An open industry standard for innovations with chiplets at package level," *IEEE Trans. Compon., Packag., Manuf. Technol.*, vol. 12, no. 9, pp. 1423–1431, Sep. 2022.

[101] M. Shindell, T. Kramer, and S. Salot Jr., "The 'ticking time bomb' of counterfeit electronic parts," Industryweek, Independence, OH, USA, Jul. 2013. Accessed: Oct. 10, 2023. [Online]. Available: https://www.industryweek.com/supply-chain/procurement/article/21960820/the-ticking-time-bomb-of-counterfeit-electronic-parts

[102] E. Sperling, "Security risks widen with commercial chiplets," *Semicond. Eng.*, Jul. 2022. Accessed: Oct. 10, 2023. [Online]. Available: https://semiengineering.com/security-risks-widen-with-commercial-chiplets/

[103] P. Gu, D. Stow, R. Barnes, E. Kursun, and Y. Xie, "Thermal-aware 3D design for side-channel information leakage," in *Proc. IEEE 34th Int. Conf. Comput. Design (ICCD)*, Oct. 2016, pp. 520–527.

[104] J. Knechtel, S. Patnaik, and O. Sinanoglu, "3D integration: Another dimension toward hardware security," in *Proc. IEEE 25th Int. Symp. On-Line Test. Robust Syst. Design (IOLTS)*, Jul. 2019, pp. 147–150.

[105] C. Bao and A. Srivastava, "Reducing timing side-channel information leakage using 3D integration," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 4, pp. 665–678, Jul. 2019.

[106] J. Knechtel, "Hardware security for and beyond CMOS technology," in *Proc. Int. Symp. Phys. Design*. New York, NY, USA: ACM, Mar. 2021.

[107] J. Dofe, "Thermal side-channel leakage protection in monolithic three dimensional integrated circuits," in *Proc. IEEE 35th Int. System-on-Chip Conf. (SOCC)*, Sep. 2022, pp. 1–2.

JUAN SUZANO received the B.S. degree in computer engineering from Universidade Federal do Rio Grande do Sul and the M.S. degree from École Supérieure de Chímie Physique Électonique de Lyon through the excellence double degree program BRAFITEC, in 2022. He is currently pursuing the Ph.D. degree in micro and nano electronics with Université Grenoble Alpes in partnership with STMicroelectronics and the Commissariat A L'Energie Atomique Et Aux Energies Alternatives (CEA).

During his graduation, he worked on research projects on hardware reliability in harsh environments for aerospace applications and he participated as the coauthor in two conference papers. Now, he is invested in the research and development of hardware solutions for chiplet-based 2.5D and 3D integrated circuits.

FADY ABOUZEID received the M.S. and Ph.D. degrees in micro and nano electronics from Université Grenoble Alpes, France, in 2007 and 2010, respectively. Since 2007, he has been with STMicroelectronics, Central Research and Development, Crolles, France, in a research and development group in charge of hardening and qualifying IPs for space and terrestrial environments, and ultra-low voltage and high energy efficiency circuit design. He was in charge of the design activities, enabling research and implementation of CPU embedded hardening and low power mechanisms, advance embedded radiation effects capture systems, and test vehicles for radiation qualification. Since 2020, his research activities are now focused on the enablement of 2.5D/3D chiplets solutions and autonomous microcontrollers.

GIORGIO DI NATALE (Senior Member, IEEE) received the Ph.D. degree in computer engineering from Politecnico di Torino, in 2003.

He is currently the Director of Research for the French National Research Center (CNRS). He has been the Director of the TIMA Laboratory, Grenoble, since January 2021. His research interests include hardware security and trust, secure circuits design and test, reliability evaluation and fault tolerance, and VLSI testing. He has published two books and nine book chapters, 50 journal articles, and more than 150 conference and symposium papers in these domains. He has been involved in projects funded by the EU, Italy, and France. He has been the action Chair of the COST Action TRUDEVICE (Trustworthy Manufacturing and Utilization of Secure Devices), the biggest European research network on hardware security and trust.

Dr. Di Natale is a Golden Core Member of the Computer Society. He also actively contributed in the organization of the main international conferences in his domain (the General Chair of DATE20, the Program Chair of DATE17, the Program Chair of ETS16, a member of the Executive Committee of DATE, since 2012, and a member of Organizing Committee of ETS and VTS, since 2010). He belongs to the program committees of many conferences, such as DATE, ETS, IOLTS, DSD, DTIS, FDTC, GLSVLSI, HOST, and CS2. He served as the Chair for the IEEE Computer Society TTTC. He serves as an Associate Editor for IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS and IEEE TRANSACTIONS ON COMPUTERS.

ANTHONY PHILIPPE received the Graduate degree from Central-Supelec Engineer School, France. After 17 years in STMicrolectronics as a System Architect defining complex system on chip in different technology nodes, including 28FDSOI. He joined the CEA as a Research Engineer, in December 2014. He is currently involved in system-on-chip architecture for high performance IP, computing, and 3D integrated circuit projects. He has been the Lead Architect of several designs all combining low power, high speed communication links, many core architecture, and network-on-Chip. He strongly participates to the roadmap, definition and specification of the next generation of communication and computing components, and actively participated to the architecture definition of the computing silicon developed within the H2020 FETHPC ExaNoDe Project.

PHILIPE ROCHE (Member, IEEE) received the M.S. and Ph.D. degrees in semiconductor physics, in 1995 and 1999, respectively. His primary activities are single event effects and total ionizing dose, and ultra low voltage IPs, from sub-0.25μm technologies down to FinFET 3nm. He has been serving in conferences, since 1997, as the Session Chair and a short course Instructor. He has coauthored more than 300 articles and filed more than 75 patents and three trade marks in radiation hardening. He was appointed as a Regional Fellow and a Technical Director Research and Development, in 2013, then elected by the ST Technology Advisory Board as a Corporate Fellow, in 2020. After five years in a product organization designing ASICs, he is back to ST Central R&D (FTM/TDP), in charge of new research and development explorations, such as 3D/GaN/Safety/RF/batteries with a team of senior experts, also acting as the Head of Labs & Ecosystems management, with LETI, CNRS, ANRT, and CIME-P as a key partners.