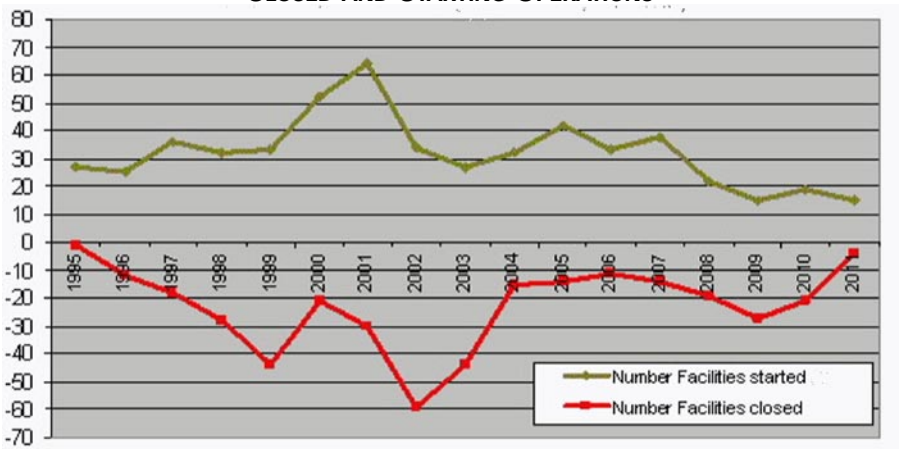
Smart Security Finds Itself in a New Situation

►►►

65nm technologies and lower. The rule has become frighteningly simple: only high revenues per wafer and products with high ASP will follow. Translation for smart security: circuits for SIM cards where ASP has already scared off NXP, Atmel and Renesas should be abandoned. With ASP below 20 cents (some circuits will be sold around 5 cents per unit), they already offer a spread of 30 cents from the ASP of a classic microcontroller (ASP: 50 cents) that nevertheless does not embed all the sophisticated apparatus of the counter-measure and security features of secure microcontrollers. "The smart security industry risks suffering considerably more than others from this situation," affirms Delesse.

Smart security in fact finds itself in a new situation. The conditions that for the past ten years allowed it to arrive at smaller than average prices are now disappearing. "Up to now, we had newcomers to supply secure ICs, now we have quitters," insists Lucien Brau, ex-CEO of Atmel SMS in Rousset, today founder and president of StarChip, a company specialized in design and industrialization of chips, in particular for the smart security industry (see below our interview). Atmel's entry and above all that of Samsung in the circle of secure sili-

1995-2011- Front-end Facilities (R&D, Pilot and Volume) Closed and Starting Operations



40 fabs were closed or planned to close in 2009-2010 (source SEMI World Fab databases -February 2010).

"The fabless model only works with highly differen

Lucien Brau, Founder, CEO and President of StarChip. Brau grew Atmel's smartcard business from $3 million to $240 million between 1999 and 2006. He was in charge of integrating Motorola's smart card business, and worked very closely with George Perlegos, Atmel's founder.

What are the observations or conclusions that led you to create StarChip and its new business model: "IC product provider"?

►First of all it was a structural analysis of the semiconductor value chain: the first observation was the emergence in Asia (Taiwan and China) of pure-play foundries such as TSMC, Chartered, Global Foundries, UMC, SMIC and elsewhere in the world, the U.S. in particular, of fabless companies that were booming, the most noteworthy of which figure among the world's leading 10: Qualcomm, Broadcom, MediaTek, Nvidia, ATI, SanDisk, etc. These fabless companies were able to develop innovative products that were highly differentiated due to their access to advanced technology (65 and 45nm) and expensive – margins for TSMC, for example, are on the order of 50% for this type of products – yet which offer decisive competitive advantages in their effort to differentiate themselves. Hence the first conclusion we reached: this fabless model works only for highly differentiated products. It doesn't work for standard products for which recourse to 65 or 45nm technology offers no real added value, because in the end the differentiators are slim, or come to very little given standards or multi-source questions. In a circuit where the purely digital component represents only 10% of the circuit, the point of shifting from 130nm towards 90 or 45nm just isn't justified. Our conclusion was thus to find a new model that would allow us to simplify the value chain, and ensure that the two combined margins for the foundry and the fabless that would reach the OEM (card makers) in the fabless models, as well as the IDM margin (the margin for internal transfer and product & service) within the classic model could all be reduced. Which is where we got the idea for our model based on three types of contracts and a system for royalties.

This system is in fact the ARM model (IP Provider) extended to product industrialization. We believe that we can thus create profits on the order of 20%.

con vendors, was in both cases a factor of the growth in competition that has resulted in greater than average dips in ASP. Does this mean that the exit of NXP, Renesas and Atmel from the SIM market has somehow brought about a rise in the ASP of SIMs? No, but no doubt it has helped to moderate the annual decline that may have attained over 35% in some years. We can already see it in the financial results of silicon vendors (see our article on page 4-5). The point-of-no-return for prices seems stronger than the decline in the impact of competition. To respond to this situation, StarChip specifically offers a new business model that we can consider as a subtle battle arm against the hegemony of Samsung in the SIM market (+60% market share), and maybe even soon in the smart security market more generally (35% currently). By building on the rise in power of pure-play foundries such as LFoundry, with which incidentally it has concluded industrial partnership accords, StarChip is now offering to reduce current silicon vendor margins by 10 to 20%, and to thus reproduce the effect of a newcomer in the tight circle of secure silicon vendors, now dominated by Samsung, Infineon, Renesas, NXP and STMicroelectronics. But a new entry that will invent new rules of the game could make all the difference.

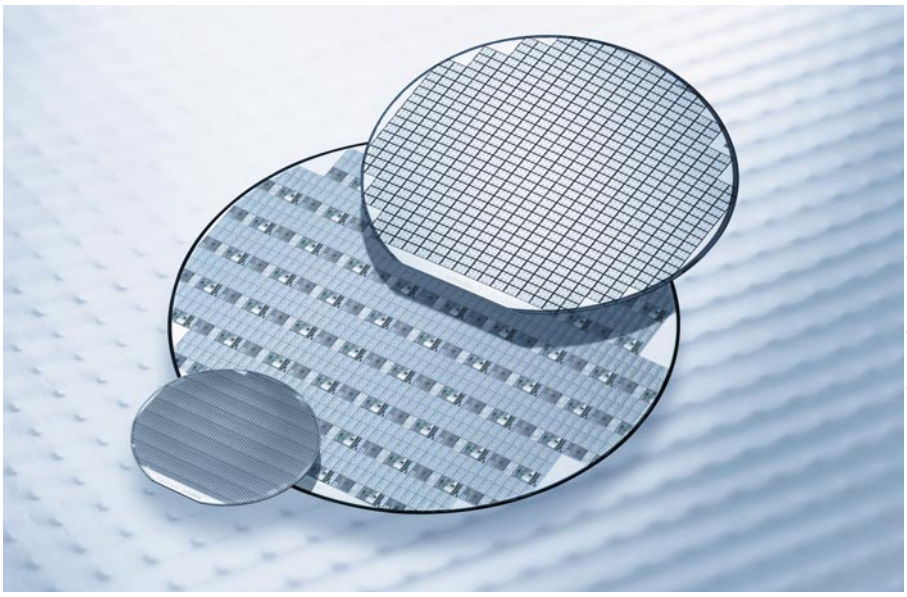


Photo Infineon Technologies

3, 6 and 8-inch wafers. The smart secure IC ASP is less than $0.20 per die. One of the lowsest among overall MCU applications, behind automotive, consumer and industrial.

It's likely that the smart security industry will enter a period where different supply chain models for secure ICs will have to co-exist. Originating with the

►►►

tiated products"

Doesn't this remodeling of the value chain that you are offering also derive partly from another development, relating to the organization of competition within smart security, which has been marked for the past ten years or so by the arrival of new players, Samsung the most recent, each time driving increased pressure on prices?

►Yes, we do feel today we've arrived at the end of a cycle in this particular competitive model. We've seen up to now new "arrivals," and are just starting to see "departures." NXP Semiconductors, Atmel, Renesas have all given up in the SIM market. As for knowing whether among IDMs that supply secure microcontrollers we'll have 100% departures, that's another story, but the question is legitimate when we look at the revenues being made in this sector, for the most part representing only a fraction of overall revenues for IDMs.

Don't these concurrent developments in the supply chain of the semiconductor and smart security favor the emergence of a new type of player: design houses? Or at least tempt card makers to design their own circuits?

►The idea of pure design is an illusion. It's true that it may seem simple to design your own circuits, but then you have to industrialize them. And it's the "then" that is the real problem, because industrialization is scary. Yet again, what is the value of the cost of protecting a specification when it's a standard product, by definition not exclusive? At the least, it could be justified for niche products, very high-end segments and Asics, in the military, for example, but you'll still have to resolve the issue of industrialization, availability of the circuit, its housing and quality. Our model, from this point of view, performs better, since it resolves all of these issues, with a realistic redefining of task-sharing. The fact that card makers are thinking about this design possibility is nothing new, but it's also because they are permanently obliged to benchmark everything on the market.

The first product you designed, which you will industrialize, is a classic example of the standard product. It's a SIM, and yet somehow, you've been able to highlight certain notable differentiating factors…

►Yes, it has four elements that distinguish it from other circuits in this market.
The first is the 32-bit core, extremely small in size (9,500 gates), which offers highly appealing performance for the price of an 8- or 16-bits classical microcontroller.
The second is the tiny embedded NOR flash, with partitioning for the code and the data, and clockspeed at 25MHz.
The third is a hardware endurance motor, which ensures several million cycles, compared to the basic 100,000.
The fourth, last but not least, is the flash personalization technology, extremely fast, where gains can be measured directly in time for card makers. ■