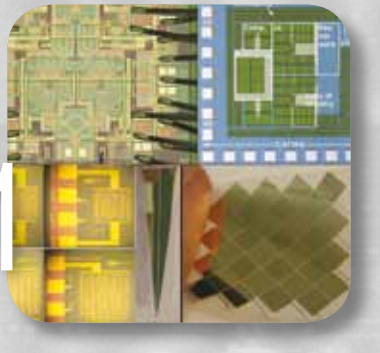
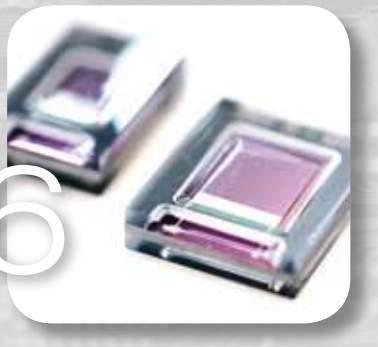
Februari '12 Maart '12 | 13de jaargang - nr. 1 | verschijnt tweemaandelijks | afgiftekantoor: 2800 Mechelen 1 | www.dspvalley.com | P2A6695

DSP VALLEY newsletter 1

Verantw. Uitg.: Peter Simkens • DSP Valley vzw. - Gaston Geenslaan 9 - 3001 Leuven (Belgium) • tel. +32 (0) 16 24 14 40 • fax +32 (0) 16 24 14 49 • www.dspvalley.com

In this issue





KU Leuven ESAT-MICAS at ISSCC 2012

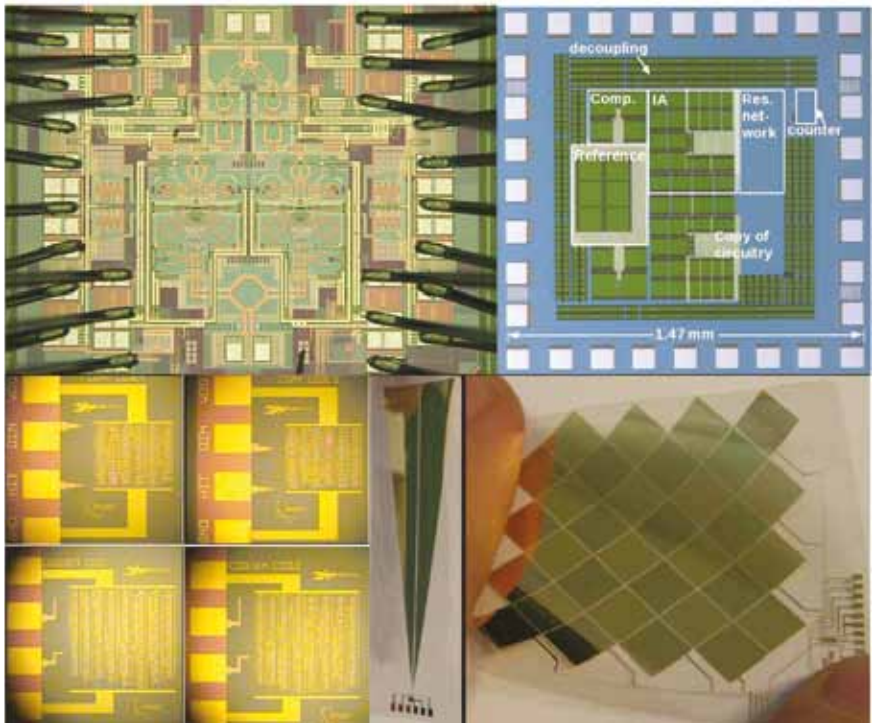
In February 2012, researchers from the KU Leuven ESAT-MICAS research group have presented four papers at the International Solid-state Circuits Conference (ISSCC) in San Francisco. ISSCC is the annual industry's premier venue for presentations on new developments in the integrated-circuit industry. The ESAT-MICAS papers span a broad area of applications and acknowledge the groups' expertise in mm-wave, RF, analog and digital circuit design.

continuation on page 2

continuation from page 1

The mm-wave and RF expertise is demonstrated by paper 9.5, **"A 60GHz Outphasing Transmitter in 40nm CMOS with 15.6dBm Output Power"** by Dixian Zhao, Shailesh Kulkarni and Prof. Patrick Reynaert. A 60GHz outphasing transmitter that reconstructs the complex modulation by vector summing two constant-amplitude phase-modulated signals is implemented in 40nm digital CMOS. The proposed TX achieves 15.6dBm linear output power with 25% PAE, measures 0.33mm^2 in active area and consumes 220mW from a 1V supply voltage. Compared to the state-of-the-art, this work achieves an improvement of a factor 4 in linear output power and a reduction by two in power consumption compared to existing solutions. This low power consumption is a key benefit as 60GHz will also be used for mobile applications.

The ESAT-MICAS has a well-known and established expertise in analog circuit design, as confirmed by paper 21.8: **"On-Chip gain-reconfigurable 1.2 V 24 µW chopping instrumentation amplifier with automatic resistor matching in 0.13 µm CMOS"** by Fridolin Michel and Prof. Michiel Steyaert. In this paper, a 1.2 V 24 µW fully integrated direct-current feedback instrumentation amplifier with rail-to-rail output is introduced. Feedback resistors are integrated on-chip for small size and low cost. Automatic matching of the on-chip resistors by using a highly accurate reference scaling technique guarantees low gain error drift over temperature, device aging and intra die variations.



The circuit innovation at ESAT-MICAS is fairly independent of the technology. The widening from a strong CMOS orientation in the past to various technologies today is clearly visible by two papers that present transistor-level circuit innovation in organic electronics on plastic foil. Hagen Marien and Prof. Michiel Steyaert of ESAT-MICAS are co-authors of paper 18.2: **"1D and 2D analog 1.5kHz air-stable organic capacitive touch sensors on plastic foil"**. In this work a triangular 1D and a 4x4 2D organic capacitive touch sensor integrated on foil with a sample rate of 1.5kHz are presented. The analog output of the sensor read-out is determined by a ratio of capacitances and air-stable. The sensor reaches a localization accuracy of around 1mm and consumes 6µA from a 15V supply. Finally, the fourth paper of the group is in the same research field. Kris Myny and Prof. Wim Dehaene from ESAT-MICAS are co-authors of paper 18.3: **"Bi-directional communication in an HF hybrid organic/solution-processed metal-oxide RFID tag"**. In this work the RFID tag is for the first time bidirectional, based on the 'reader-talks-first' principle. It is also one of the first circuits in a fully complementary hybrid organic/oxide technology. This enhances both the performance and the robustness of the tag. ■

Call for Cross-border Innovation Projects on the "Smart Home"

Preface

Since more than a year, DSP Valley is project partner in the Interreg 4A project "TTC" (Towards Top Technology Clusters), aiming at stimulating cross-border cooperation in innovation projects, in 4 selected technology domains: ICT, life sciences, energy and new materials.

In 2012 this project will get an additional dimension, when a second related project will be approved: with the project GCS ("Grensoverschrijdende Cluster Stimulering" / Cross-border Cluster Stimulation), we will have a dedicated funding instrument as an additional financial stimulus for setting up innovation projects with cross-border teams.

The preparation of project idea stimulation has already started. Based upon a concept created by our project partner LIOF, the working groups for each of the four above mentioned technology domains will develop a roadmap about a selected hot topic in their domain, as a source for project ideas. The project idea stimulation will then be continued in some interactive workshops with industrial participants, with some self-explaining names as "Just imagine" and "Room with a View".

PRAGMADEV

real time development tools

PragmaDev is a privately held company based in Paris France that provides a set of modeling and testing tools for the development of real time and embedded software:

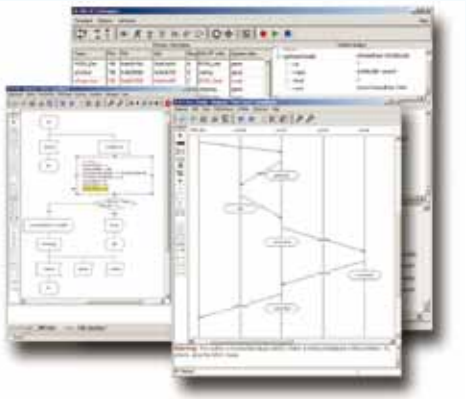
- "Real Time Developer Studio" targets all development teams working on communicating systems looking for a serious modeling technology based on standard languages, and the
- "MSC Tracer" is a free on-line or off-line tracing tool generating live sequence diagrams.

Real Time Developer Studio provides three levels of modeling: informal, semi-formal, and fully formal. While informal modeling, the most common, is mainly used for documentation; the most advanced level of modeling allows simulation, prototyping, verification, full code generation, debug on target, test generation, and test of the model.

Real Time Developer Studio integrates a standard testing technology that can be used on any model level. The key feature is to be able to start testing very early in the development process with the model and the test cases to be simulated against each other. When the model is further refined down to its implementation on target, code can also be generated from the test cases and executed on the same target or on a separate tester.

The overall picture is that PragmaDev modeling technology provides a consistent environment for continuous integration along the whole development lifecycle.

Technically speaking Real Time Developer Studio is a consistent integration of standards such as SDL, SDL-RT, UML, TTCN-3, ASN.1, and C/C++ editors. Models can be executed and verified with a powerful built-in simulator and a third-party exhaustive simulator. Test cases can be generated from the model or from use cases and executed against the abstract model or its implementation. The tool can generate full C or C++ code including RTOS adaptation or a built-in scheduler. Its connection with cross debuggers allows graphical debugging in the model and generation of live graphical traces. The tool can also generate full documentation and connect to traceability tools.



PragmaDev Real Time Developer Studio covers requirements, specification, prototyping, design, debug on target, and testing. Its main benefits have been measured:

- Increased quality by a ratio of 5,
- Reduced development time by an average of 35%,
- Self-documented application,
- Portable applications from one RTOS to another,
- Model checking capabilities,
- Traceability information.

Its pragmatic approach and reasonable price makes it easy to use and guarantees a quick return on investment.

PragmaDev customers include key accounts in the industry such as Airbus, Renault, Alcatel-Lucent, or the European Space Agency. In all cases our customers are generating code out of their models making PragmaDev the tool choice for serious software modelers. Last but not least PragmaDev has developed a University program that counts more than 600 active licenses around the world.

DSP Valley, together with the other partners in the ICT working group, has selected the "Smart Home" as the hot topic for the roadmap and the subsequent workshops. The "Smart Home" is considered as a very promising application domain, not only crossing geographical borders for cooperation, but also interdisciplinary technology borders between ICT and energy. Therefore, the focus for the "Smart Home", as developed in our roadmap, will be on ICT-enabled applications for optimizing the energy consumption in the home environment.

You will soon receive some invitations for the "Just Imaging" and "Room with a View" workshops on the "Smart Home". If you already have some excellent idea for an innovation project right now, please let us know, and we will be very glad to help you in finding the right partners, and finding the right way to financial support through the new upcoming GCS-project.

Best regards,
Peter Simkens
Managing director

InGaAs cameras for OCT applications

Moving from biomedical to industrial applications: OCT Enables Hi-Res Non-Destructive Depth Analysis

Optical coherence tomography (OCT) has evolved to a standard non-invasive biomedical analysis technique yielding a detail-rich cross-sectional image of living tissue. It spreads with breathtaking velocity and advances in the industrial market. Promising industrial applications of OCT are emerging as cost-efficient quality improvement tools for in-line inspection of multi-layered objects in manufacturing processes. For these tasks, advanced high-speed InGaAs cameras are universally suited.

Xenics
Infrared Solutions

The Promising Potential of OCT

That OCT has an enormous future potential is proven by a study carried out by the Millennium Research Group and published in October 2010 [1]. According to their five-year forecast the OCT market will see average growth rates of 60 percent per year. Obviously, this extremely positive estimate is based primarily on the market segment of medical electronics, which has become the first broad application area of OCT since it was introduced in 1991 by Dr. James Fujimoto of the Massachusetts Institute of Technology (MIT).

At that time it became immediately clear that OCT can deliver detail-rich images from the deeper layers of living tissue – which is of special value and utility to ophthalmologists. Next in line is a multitude of other medical applications, such as measuring the thickness and uniformity of functional layers in pharmaceutical products, which is of importance for the controlled dispensing of certain agents. Another promising application of OCT is the examination of blood vessels, or three-dimensional imaging of the kidneys [2].

There is a strong indication that OCT imaging will have an impact on a multitude of established medical procedures, which in turn will change current practices. Just one example: today's "gold standard" in the early detection of cancerous growth in the larynx is performing a biopsy - extracting a small, suspicious tissue probe and treating it to a microscopic examination in the lab. However, a biopsy of larynx tissue is a serious invasive procedure that necessitates local anesthetics and may leave the patient permanently hoarse.

Here, OCT combined with video laryngoscopy can serve as a much milder alternative replacing biopsy by an outpatient tomography of surface and deeper tissue irregularities - without the need for anesthetics and avoiding direct physical contact with the affected tissue. The example is a good pointer to the industrial uses of OCT, where similar examination constraints may apply. The advantages of OCT will come in the form of cost saving and quality improvement realized through an accelerated process flow.

As a high-frequency analog to and a possible replacement of ultrasound examination techniques optical coherence tomography delivers images of a much higher resolution – well into the micrometer realm. The penetration depth achievable with OCT is determined by the type of material under test and the wavelength used (Figure 1). OCT penetration can reach 6 mm and more. Thus, OCT is able to bridge the realms of confocal microscopy and ultrasound, as well as other computer tomography (CT) methods such as magnetic resonance imaging (MRI).

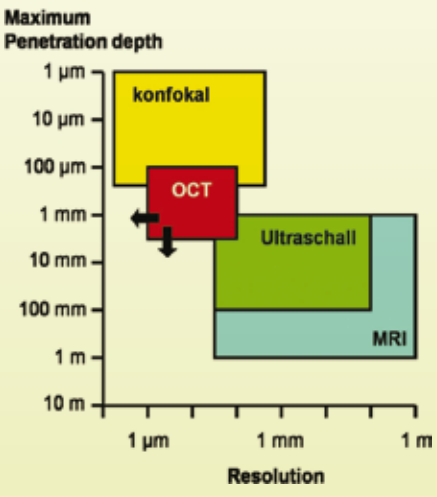


Figure 1. Examination methods for analyzing depth structures, penetration depth andresolution.

OCT - how it works

OCT delivers cross-sectional images from within material objects without the need of touching them or using destructive procedures. Figure 2 shows several cross sections of a MEMS pressure sensor at various depth levels (above left) achieved by penetrating it through its membrane [3]. As a consequence, OCT is opening innovative ways for industrial quality assurance and process control. Real-time OCT can be used to monitor continuous manufacturing and assembly processes.

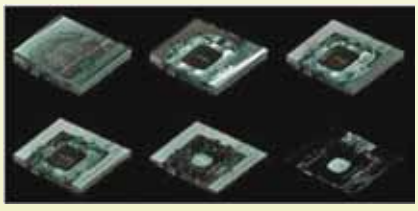


Figure 2. Penetrating the membrane of an MEMS pressure sensor (above left), OCT yields cross-sectional images at various depth levels to unveil details of its internal structure.
Source: National Physical Laboratory

[1][2][3] see p.15 Literature

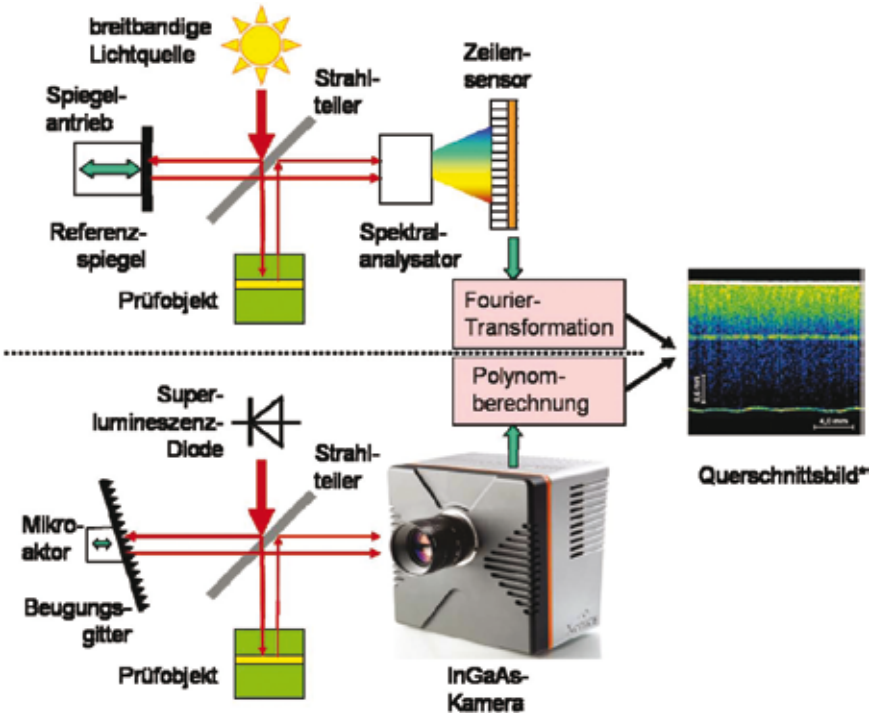


Figure 3. Two concepts of optical coherence tomography (OCT): high-resolution line camera Lynx and very fast 2D camera Cheetah-640 CL, used for a cross-sectional examination of a plastic, three-layer container wall.
Source of cross sectional image: Fraunhofer ILT

Figure 3 delineates the fundamentals of optical coherence tomography. It is based on the interference of a direct light beam from a light source striking the object under test with the light beam reflected by the object through a semi-transmissive mirror (or beam splitter).

Line sensor camera

Of the many possible formats to achieve this interference effect, Figure 3 shows just two of them. In the upper part of Figure 3, a broadband light source radiates light of a low coherence length through a semi-transmissive mirror onto the object under test. A part of this beam is reflected by the beam splitter and guided to a reference mirror, which feeds it via the semi-transparent mirror to the input of a spectrum analyzer. There, the light reflected by the test object interferes with the reference beam. As a result, the spectrum analyzer outputs the spectrum of this interference pattern, which is then converted by an optoelectronic line sensor to an electrical intensity signal. Out of this spectral information a Fourier transformation generates the appropriate spatial intensity data. A disadvantage of this setup is the relatively large travel range of the mirror, which can be several millimeters to cover the entire
intended examination depth within the object under test.

2D OCT camera

Considerably faster is an OCT procedure depicted in the lower part of Figure 3. It uses diffractions gratings and a 2D camera in InGaAs technology [4]. This 2D camera setup works without a depth scan mechanism. The relatively small-band light beam of superluminscence diode (at a wavelength of 1,310 nm and a 3-db bandwidth of 30 nm) is led through a beam splitter yielding a reference beam going to the left, and a test beam going downwards. A cylindrical lens (not shown in Figure 3) widens the test beam to form a line on the test object. The reference beam is deflected by the diffraction grating, which is positioned in a way that a higher-order diffraction image is directed towards the camera.

Thus, the 2D camera sees an interference pattern generated by the reference and test beams. By evaluating several of these interference images, which show different phase relations, the object under test is optically examined. Diffraction gratings with micro actors, made of a piezo ceramic, enable a mirror small travel range in the realm of a few micrometers. Three interference images, each representing a shift of a third of the wavelength used, will suffice to derive an OCT image by calculating a second-order polynomial from the measured values.

The calculation of the polynomials and the Fourier transformation suited for both procedures shown in Figure 3 can be done by a regular multi-purpose computer and its appropriate programming or via a dedicated hardware solution based on a field programmable gate array (FPGA), which performs just this one function, but in a very rapid fashion.

Test object, used as an example

A three-layer plastic part, about 2.3 mm thick, that serves as the wall of a liquids container, was chosen as test object for an OCT demonstration. It consists of a high-density poly-ethylene material plus a 100 µm thin EVOH (ethyl vinyl alcohol) layer as diffusion barrier. The Fraunhofer-Institut ILT [5] has investigated the properties of this structure in the context of a project that is to explore resource-saving manufacturing methods in the plastics industry.

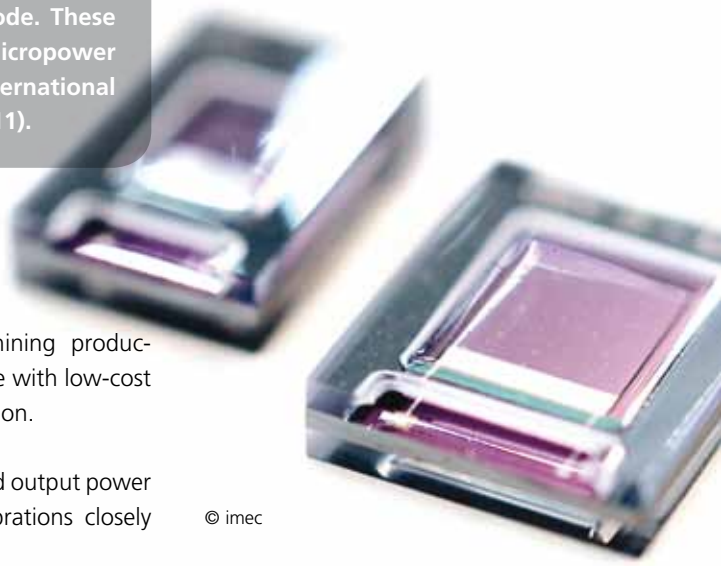
The objective was the development of an "Interferometric Inline Control System in the Production of Multi-layer Plastic Foils." OCT is used to measure the thickness and uniformity of individual thin layers in real time during a production run. Besides achieving significantly higher process security, the Fraunhofer researchers say, this OCT-enabled control technique will save material supplies amounting to 100,000 euros per year even when deployed in a medium-capacity production facility.

[4][5] see p.15 Literature

continuation on page 10

Imec presents a MEMS energy harvester suitable for shock-induced energy harvesting in car tires

Imec and Holst Centre announced that they have made a micromachined harvester for vibration energy with a record output power of 489µW. Measurements and simulation show that the harvester is also suited for shock-induced energy harvesting in car tires, where it could power built-in sensors. In a tire, at 70km/h, the new device can deliver a constant 42µW, which is enough to power a simple wireless sensor node. These results, obtained within the research center's program for Micropower Generation and Storage, were presented at the 2011 IEEE International Electron Devices Meeting (IEDM) in Washington (December 2011).



Harvesters with various dimensions. The shiny capacitor stack on top of the beam is visible through the glass package.

© imec

Imec's innovative harvester consists of a cantilever with a piezoelectric layer sandwiched between metallic electrodes, forming a capacitor. At the tip of the cantilever a mass is attached, which translates the macroscopic vibration into a vertical movement – putting strain on the piezoelectric layer and generating a voltage across the capacitor. As piezoelectric material, AlN (aluminum nitride) was chosen. The harvesters are packaged with a 6-inch wafer scale vacuum packaging process. The micromachining production process is compatible with low-cost mass-production fabrication.

The harvester has a record output power of 489µW when the vibrations closely

Smart Engine for Public Key cryptography

Every day, huge amounts of information are exchanged between billions of computers. Large quantities of information are delivered by servers over the Internet. Also, ensuring security in wireless data communications is recognized as a priority. And using secured communications for banking and e-commerce applications is of fundamental importance.

The technology to secure communications is well-known. Nevertheless, a lot of channels transporting critical information are still not correctly protected. The main reason is that security protocols rely on cryptographic algorithms that are very compute intensive.

Why symmetric and asymmetric cryptography?

Symmetric cryptography refers to encryption methods in which both parties (the sender and the receiver) use the same key. Algorithms like 3-DES or AES are widely used to protect (providing confidentiality and authentication) data payload for transmission or storage. This kind of solutions makes data transfers, communications and transactions for e-commerce secure.

The main problem with symmetric cryptography is to secure the exchange of the common key used by both parties. Asymmetric cryptography solves this issue.

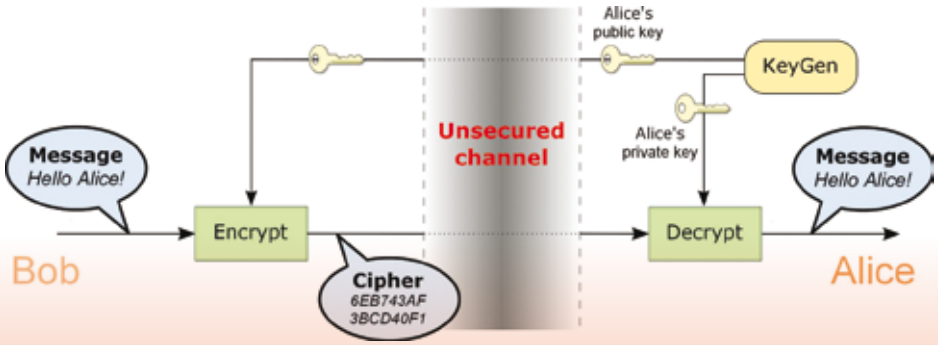


Figure 1: Asymmetric cryptography

match the MEMS' resonance vibration, which in this case is 1011Hz. Together with an automotive partner, imec also validated the use of the harvester for use in car tires. These submit the harvester to regular shocks, depending on the car's speed and the characteristics and condition of the tire. Each shock will displace the mass, after which it will start to ring down at its natural resonance frequency. During this ring-down period, which depends on the quality factor Q of the harvester, part of the mechanical energy is harvested. It is shown that in this way, a constant power output as high as 42µW can be harvested at a speed of 70km/h.

Micromachined vibration harvesters such as these are ideal devices to generate electricity from machines, engines and other industrial appliances which vibrate or undergo repetitive shocks. In these environments, they will power miniaturized autonomous sensor nodes, in situations where battery replacement is not sustainable or practical. Harvesters will allow sustainable monitoring on a massive scale. One example is Tire Pressure Monitoring Systems (TPMS) and its successors: a car tire with built-in sensors that monitor e.g. the tire integrity and pressure, the road condition, or the driving style.

■

About Holst Centre

Holst Centre is an independent open-innovation R&D center that develops generic technologies for Wireless Autonomous Transducer Solutions and for Systems-in-Foil. A key feature of Holst Centre is its partnership model with industry and academia around shared roadmaps and programs. It is this kind of cross-fertilization that enables Holst Centre to tune its scientific strategy to industrial needs.

Holst Centre was set up in 2005 by imec (Flanders, Belgium) and TNO (The Netherlands) with support from the Dutch Ministry of Economic Affairs and the Government of Flanders. It is named after Gilles Holst, a Dutch pioneer in Research and Development and first director of Philips Research. Located on High Tech Campus Eindhoven, Holst Centre benefits from the state-of-the-art on-site facilities. Holst Centre has over 150 employees from around 25 nationalities and a commitment from more than 30 industrial partners.
Visit us at www.holstcentre.com

About imec: see p. 11

As we can see in Figure 1, Alice generates a pair of keys[1].

- The public key is used to encrypt messages. It can be shared without restriction.
- The private key allows decryption of the cipher message. As such, it must be kept secret to Alice.

Bob can use the public key of Alice to send her an encrypted message. As she is the only one to know her private key, Alice is the only person able to decrypt the message.

Asymmetric cryptography is also used for authentication. Alice can generate a digital signature with her private key. Using the public key, Bob can check that Alice is well the owner of the private key.

As asymmetric cryptography allows free exchange of the public key, it is often called Public Key cryptography.

(1) *As an example, RSA uses modular arithmetic. The private key can only be retrieved from the public key by factorizing the modulus. But the chosen modulus is very large. This means that it cannot be factorized without brute force attacks.*

Performance requirement in Public Key cryptography

Public Key cryptography is a very compute-intensive part of security protocols. For instance, it involves RSA (modular exponentiation on 1024-, 2048- or 4096-bit) and ECC (Elliptic Curve Cryptography) algorithms. This kind of operations creates an important overhead on CPU workload so that the impact on system performance is significant.

For example, a typical operation in ECC is to compute the sum of two points (Point Addition). Let P=(x1,y1) and Q=(x2,y2) be 2 points on curve E over Gf(p)[2]. R=(x3,y3)=P+Q can be found by making the following computations:

$$c = (y2-y1) / (x2-x1)$$
$$x3 = c^2 - x1 - x2$$
$$y3 = c(x1-x3) - y1$$

The arithmetic operations involved in these computations are not only modular additions and subtractions. There are also more complex operations like modular multiplication, modular division and modular inversion. Depending on the width of p, all these operations involve 192-, 256-, 384- or 521-bit numbers.

In RSA cryptography, the modular exponentiation is usually computed using a repeated square-and-multiply algorithm. This algorithm involves a large amount of modular multiplications and squaring on numbers as large as 4096-bit. As an example, a 2048-bit RSA operation requires more than 20 millions of 32x32 multiplications.

As mentioned, all these operations on large numbers consume thousands of clock cycles and require a large memory bandwidth. This processing load is inefficiently addressed by CPUs or other current hardware solutions because they can only execute mathematical operations on smaller values.

(2) *Gf(p) is the Galois field of prime p.*

continuation on page 8

continuation from page 7

CPUs have limits

Performing strong encryption or decryption on an embedded CPU is always possible. But when the throughput increases, the overhead quickly becomes a problem that is impossible to solve.

With a standard embedded CPU at the heart of a System-on-Chip, executing Public Key operations becomes very challenging since it requires a lot of compute-intensive operations. This is especially the case when an embedded OS or other applications are already running on this CPU.

One solution is of course to upgrade to a faster CPU. The consequences are well known: higher clock frequency means a more complex design and an increase of the power consumption with all the consequences on system costs.

Another option is to use a second CPU. But the drawbacks are about the same. A dual CPU architecture increases the complexity of the system. And the impact on power consumption can be important.

As a matter of fact, both alternatives have a significant cost and may finally not solve the CPU overloading problem.

Need of hardware solutions

In Public Key cryptography, software solutions are often too slow. So it is not a surprise that the demand for dedicated hardware solutions is increasing. Only hardware solutions can meet the computation requirements of Public Key cryptography algorithms.

Hardware accelerators are also needed when the key size increases or when the CPU is reserved for other high level functions.

Hardware accelerator performance

The presence of a hardware accelerator in an embedded system does not automatically improve global performance. Some parameters can explain the difference between the theoretical performance of one module in standalone and its effective performance when embedded in a complete system.

In Public Key cryptography, all operations on large numbers are partitioned in elementary operations on smaller values. This means that a lot of data transfers are required between the accelerator and the memory to get an access to all operands and intermediate results.

If the hardware core is not able to collect the data and write back the results, the embedded CPU must still handle data transfers. Since data processing is continuous, a solution without internal DMA capability requires constant CPU load even with the help of an external DMA. Moreover, the common data bus is continuously occupied. As a result, the global performance of the system remains significantly affected.

We can consider that arithmetic operations are executed with RTL implementations (including local memories) to achieve the expected performance. The drawback is that these hardware solutions cannot be changed and validated in a flexible way.

Smart Engine for 100% CPU offload

The algorithms for Public Key cryptography are various and complex. Unfortunately, CPUs are not efficient for the heavy processing load required by Public Key computing. An efficient solution would actually be closer to a complex Finite State Machine. But Finite State Machines are hardware implementations. They rely on a fixed state-transition diagram. As such, they drastically lack of flexibility.

The Smart Engine concept provides the "golden" solution which is based on a micro-coded sequencer and a hardware processing unit.

As we can see in Figure 2, the hardware processing unit consists of an optimized datapath. It is built on a highly-pipelined implementation of adders, subtractors, multipliers, and local registers with a wide data bus (64-, 128-, 256-, 512-bit or larger).

This optimized datapath is controlled by the micro-coded sequencer. Unlike Finite State Machines, the micro-code run by the sequencer is easily adaptable. The integration of complex algorithms, such as RSA, is described in an explicit sequence of higher level micro-coded instructions.

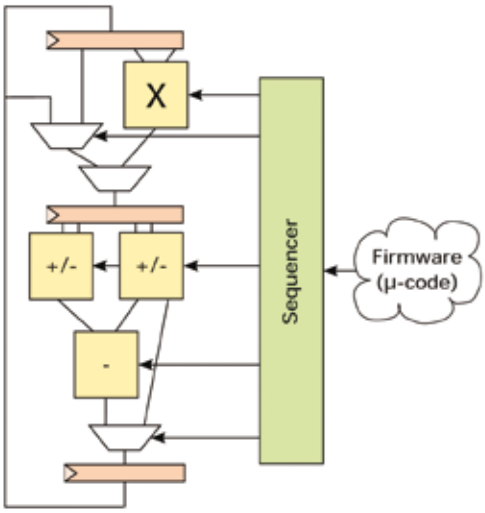


Figure 2:
Micro-coded Smart Engine concept

About Barco Silex

Barco Silex is a leader in contract engineering services, custom hardware and software development, as well as Intellectual Property (IP). Thanks to its continued stream of aggressive innovations, Barco Silex stays ahead of the competition. Barco Silex's history as a custom electronic design house (ASIC, FPGA, DSP, Board) specialized in video coding, cryptography, security and memory controllers goes back to 1991. We offer the best guarantee for continuous support throughout the complete lifecycle of products.

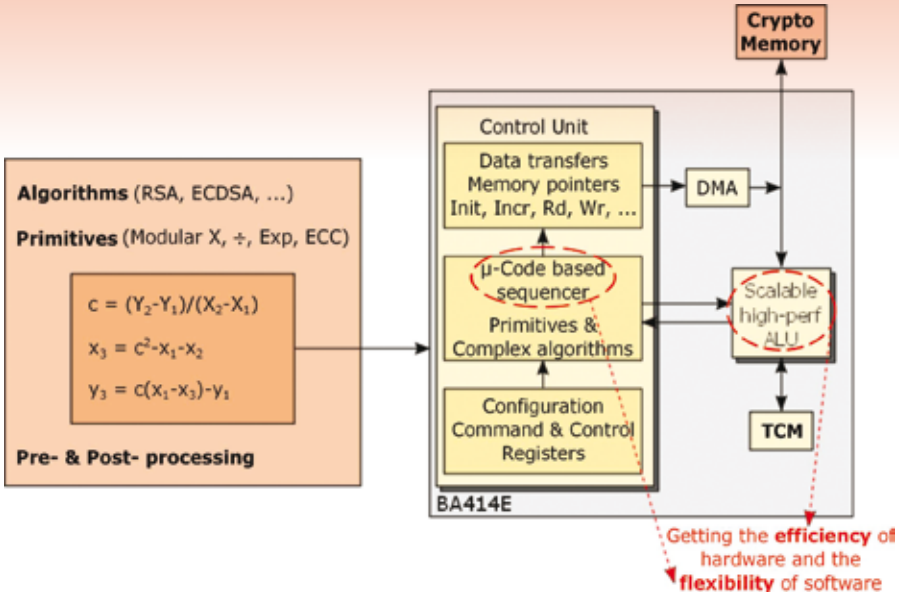


Figure 3: BA414E – Public Key crypto engine

Figure 3 shows the block schematic of the BA414E Public Key crypto engine. As we can see, the memory transfers are local to the IP (TCM and Crypto Memory). This architecture does not create any data transfer on the main bus or external memory.

As a result, the Smart Engine does not require any assistance from the main CPU:

- Various primitives can use the processing unit. (In case of RSA, this is modular multiplication and modular division.)
- Complex algorithms can be implemented by adapting the micro-code. (As an example, this is point multiplication for ECC.)
- Data transfers are handled by a micro-DMA programmed by the micro-code.

An architecture based on a hardware accelerator and a dedicated low-latency micro-coded sequencer will provide a maximum of flexibility. It will facilitate functional upgrades. And it will offer the best performances. Moreover, it will provide a solution with reduced gate-count and low power consumption.

And even more...

The Smart Engine architecture provides the highest performance, the best flexibility and even more…

The flexibility of the micro-code allows to easily and efficiently take care of the memory transfer and pre- and post-processing.

Therefore, a Smart Engine usually includes a micro-DMA which is easily programmed by the micro-code. As the main CPU is fully off-loaded of the crypto tasks, the processing can be chained (and anticipated when needed) internally at full speed.

The Smart Engine also handles all pre- and post-calculations. This makes the complete Public Key processing transparent to the user. The main CPU only needs to provide the operands and wait for an interrupt when the result is available.

Higher level algorithms like RSA in CRT mode, DSA and ECDSA (signature generation and verification) and Rabin-Miller (primality test) are also fully supported by the Smart Engine.

The Smart Engine architecture allows generating the fastest solutions on the market while keeping a high level of flexibility.

Conclusion

A few months ago, Barco Silex announced a new solution for Public Key cryptography. The BA414E is a small and flexible hardware accelerator supporting a wide range of operations in the field of asymmetric cryptography. This 100% CPU offload solution supports complex arithmetic primitives like modular exponentiation for RSA and a wide variety of complex operations and algorithms at a higher level.

The BA414E is highly pipelined and provides very high performance. With less than 35 kgates for the smallest configuration supporting the whole set of operations, the BA414E is the ideal solution for applications with strong cost and power constraints but still requiring outstanding performance. Moreover, the BA414E is flexible and can provide not only low gate count solution but also very high performance reaching up to 5000 op/s for 1024-bit RSA in standard 90 nm process.

Best of hardware + Best of software = Cost- & Power-effective Smart Engine

The BA414E makes Public Key integration affordable with easy-to-use solutions and very low-cost implementations on a wide range of FPGA or ASIC technologies.

Ease-of-integration (interfaces)

By supporting industry-standard interfaces, Barco Silex focused on making the integration of the BA414E IP as easy as possible. ■

BarcoSilex

continuation from page 5

SWIR Line Sensors in InGaAs Technology

At first glance (when looked at in the visible realm) such plastic foils and the containers made of the foils appear relatively opaque. However, this optical surface barrier can be penetrated when hit by a light beam of an appropriate wavelength in the near infrared realm. This will cause molecular resonances whose absorption spectra are typical for a given material, allowing a secure differentiation of various molecular structures.

For the measurement of these near infrared spectra the usual CMOS or CCD image sensors are not appropriate since their sensitivity is limited to the visible realm. A significantly higher SWIR sensitivity is offered by sensors in InGaAs technology (Figure 4). They are currently available as linear detectors (Lynx) with up to 2048 pixels and as a 2D camera (Cheetah-640CL) featuring 640x512 pixels.

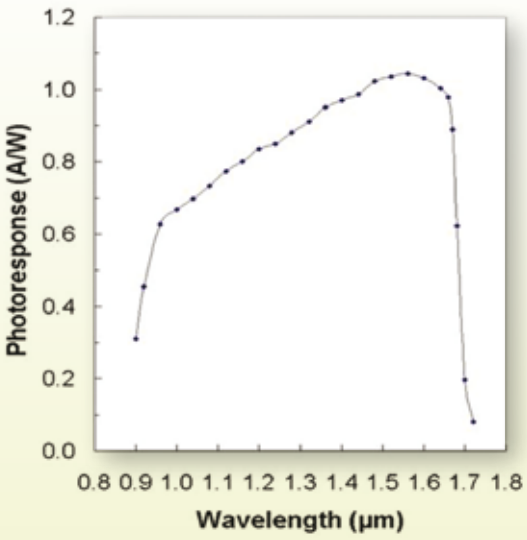


Figure 4. An InGaAs image sensor can operate in the near infrared realm.

The high resolution achieved by the Lynx line sensor is extending the application area of OCT towards higher spatial resolution (as indicated in Figure 1 by an arrow pointing to the left). And the worldwide fastest SWIR 2D camera Cheetah-640 CL, which delivers 1,730 full frames per second, transforms OCT into a dynamic, real- time control method for manufacturing processes.

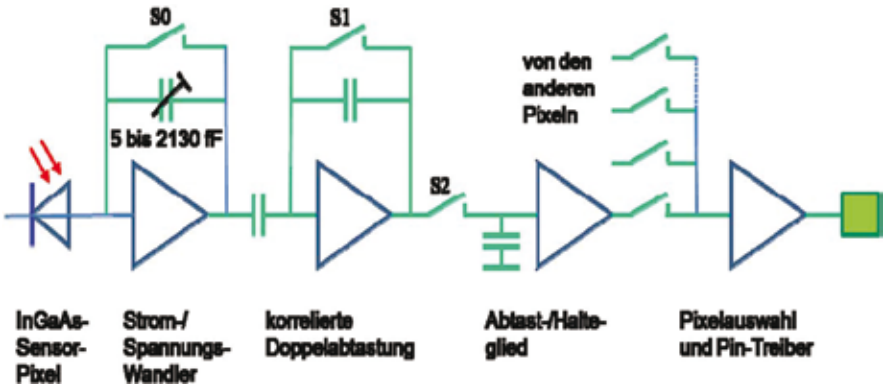


Figure 5. Pre-processing the sensor signal of a pixel with various software-settable parameters accommodates the camera to different applications.

These sensors come standard fitted with one-stage thermoelectric cooling. If a very high signal/noise ratio is required to increase penetration depth (indicated in Figure 1 by an arrow pointing downwards), the camera cooling can be upgraded to three- stage thermoelectric cooling.

Flexible Evaluation Circuitry

Whereas InGaAs is a perfect choice for SWIR-sensitive photodiodes in line sensors, it is not really suited to integrate the read-out circuitry on the same chip. Therefore, an external read-out IC (ROIC) based on CMOS technology serves as evaluation circuitry for the InGaAs line sensor. The analog ROIC front-ends can be optimized to function as detector interfaces, and their parameter values are software settable in wide margins to cover various pixel sizes and application demands.

Figure 5 gives a simplified block diagram of the ROIC's analog functionality needed for the multi-stage pre-processing of the sensor signal. The InGaAs photodiode, featuring n-well-capacities of 0.7 to 2 million electrons, is held at a constant voltage level by the current-to-voltage converter. The converter is equipped with five charge integration capacities (5 fF, 25 fF, 100 fF, 500 fF und 2000 fF). They can be selected at runtime, either singly or combined. This results in the wide converter characteristics needed to adapt the ROIC to various pixel sizes and applications.

The subsequent stage performs a correlated double sampling (CDS), thereby compensating the offset variations of the current/voltage converter and also eliminating its reset noise. Since kTC noise is noticeable especially at the smaller integration capacity of 5 fF, the CDS stage is a must. With the larger integration capacities it is the read-out noise that becomes more prominent.

Next in line is the sample/hold stage. It decouples integration and read-out. Thereby, the charge of the actual frame exposure can be integrated while the preceding frame is being read out simultaneously. Finally, an analog multiplexer and pad driver transfer all pixel values via the IC output to an external analog/digital converter.

Conclusion

With different sensor types to choose from, ROICs with various parameter settings and multi-stage thermoelectric cooling, today's InGaAs cameras are scalable OCT platforms. They are suited for a host of scientific, industrial and medical applications enabling direct imaging and spectroscopy. Most important, they include sensors that deliver a resolution of or below one micrometer, at a penetration depth of more than the current standard of 6 mm. This empowers the system designer to implement OCT as a meaningful and detailed analysis tool for hidden structures to increase quality, throughput and yield in manufacturing processes.

Literature list on page 15

Compact, low-cost and fast hyperspectral imaging solution

At SPIE Photonics West 2012, imec demonstrated a hyperspectral camera solution based on a system-on-chip image sensor with an integrated hyperspectral sensor. Imec's solution is fast and enables small and cost-efficient camera-solutions. It targets multiple industrial vision applications.

Hyperspectral cameras combine spectroscopy and imaging, and by doing this, they can e.g. discriminate between different objects that cannot be accurately distinguished using traditional RGB (red-green-blue) imaging methods. The technology can be very useful in many application domains such as crop screening, food selection, skin cancer detection, target detection, ... However, the currently available hyperspectral cameras are large, expensive and slow. Therefore, they can often not be used for time-critical or high-throughput applications, and their use is thus limited to highly specialized research environments. Imec's chip-based technology paves the way towards the industrial application of hyperspectral imaging, as it enables small, cost-efficient and fast solutions.

Imec's fully integrated CMOS compatible hyperspectral sensor, presented at SPIE Photonics West 2012, consists of a set of spectral filters that are directly post-processed at wafer level on top of a commercially available CMOSIS CMV4000 image sensor (a 4 megapixel sensor with a maximum framerate of 180fps). The hyperspectral filter developed at imec, has 100 spectral bands between 560nm and 1000nm. The filter bandwidth (Full Width Half Max) ranges from 3nm at 560nm to 20nm at 1000nm, and the transmission efficiency of the filters is around 85%. Typical integration times used in the current prototype setup are between 2 and 10 milliseconds under halogen light illumination of 450 Watt. This indicates maximal frame rates can be achieved of up to 500fp.

Due to its integrated filter design and high spectral filter efficiency, imec's solution can obtain scanning speeds that are compatible with real industrial requirements. The speed of the demonstrated system corresponds to an equivalent speed of 2,000 lines per second, significantly exceeding current state-of-the-art hyperspectral sensors. Moreover, imec's technology can be adopted to a range of industrial vision applications. To match to specific application requirements, the image sensor can be selected (a commercially available sensor or even a custom-designed sensor), determining pixels sizes, maximal frame rate, etc.

Imec's prototype camera with imec's hyperspectral sensor.

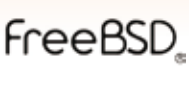
The hyperspectral filter can be tuned by changing the number of spectral bands and their spectral resolution.

Imec's prototype hyperspectral camera can capture all relevant data enabling automatic classification of different objects using state-of-the-art image processing methods. Classification results of imec's solution are equivalent to state-of-the-art hyperspectral references and recorded spectra of e.g. plant material.

About imec

Imec performs world-leading research in nanoelectronics. Imec leverages its scientific knowledge with the innovative power of its global partnerships in ICT, healthcare and energy. Imec delivers industry-relevant technology solutions. In a unique high-tech environment, its international top talent is committed to providing the building blocks for a better life in a sustainable society. Imec is headquartered in Leuven, Belgium, and has offices in Belgium, the Netherlands, Taiwan, US, China, India and Japan. Its staff of about 1,900 people includes more than 500 industrial residents and guest researchers. In 2010, imec's revenue (P&L) was 285 million euro.

Essensium - Mind helps customers make the most of open source software

Free and Open Source Software (FOSS) is today dominating the embedded systems market. And for several very good reasons: they are free from vendor lock-in, usually no license costs are involved, and the user has maximum control over the software.

However, a dangerous pitfall when dealing with FOSS is the paradox of choice. There are many options available, each with their pros and cons. At Essensium - Mind, we mainly focus on Linux but we are also aware that other systems can sometimes provide the most optimal solution for our customers. In this article, several FOSS operating systems are discussed for embedded devices.

Whenever free operating systems are considered, Linux is generally the first choice. It has by far the largest amount of hardware support, and it is deployed everywhere from the most powerful supercomputers, to the tiniest embedded devices like smart cameras. For instance, an extremely lightweight setup can fit in as small as 4MB flash. Its unmatched driver collection makes it suitable for many kinds of computer and peripheral combinations. Since its first release in 1991, Linux has an ever-growing community with an active development. Moreover, there are specialized variants like uCLinux for systems without memory management units, or Android for smartphones and multimedia devices such as tablets. But this can also lead to confusion, as there are several distributions, lots of configuration options, and a list of versions to choose from (allowing tradeoffs between more stability and more recent features). Another big downside of Linux is that it has no real-time support. This can be remedied with add-ons like Xenomai and RTAI, but the resulting system is usually hard to debug and relatively more prone to errors. Other than that, flash and memory footprint can still be a limiting factor for extremely constrained devices, and porting Linux to a new CPU is a significant task if the target processor is not already supported.

BSD variants **FreeBSD** and **NetBSD** are comparable to Linux in terms of performance and stability. However, their hardware support beyond x86 is relatively limited and communities are smaller. Still, they can be preferred for their license which permits proprietary changes.

RTEMS is a popular lightweight real-time operating system which runs as a single process with multiple threads. The typical storage footprint is in the order of 100 kilobytes, depending on the configuration. Since RTEMS does not have the advanced features of Linux like memory management, if required, these features must be developed in-house or supplied by third parties. Its license allows proprietary modules to be linked into the system code.

eCos is a slightly lighter alternative to RTEMS, with comparable API support. Similar to RTEMS, it runs in a single process with multiple threads, without memory protection. A proprietary version (eCosPro) is also available with commercial support.

FreeRTOS is one of the smallest real-time operating systems, with a typical storage footprint in the order of kilobytes. It implements several types of semaphores and can handle a large number of tasks. It supports both preemptive and cooperative multitasking. Its minimal design and small source code make FreeRTOS very easy to port. This makes it very popular for microcontroller applications. OpenRTOS is a commercially supported version of FreeRTOS with a different license.

By being the most flexible and future-proof choice, Linux is usually the way to go when designing an embedded system. It is not a coincidence that it has the largest community and commercial support in the open source world. Our experience in Essensium - Mind shows that, except on rare circumstances like extreme memory constraints, Linux is often the best choice thanks to its versatility, stability and overall performance. If needed, the sometimes complex initial porting and configuration steps can be managed by companies specialized in this field, like Essensium – Mind.

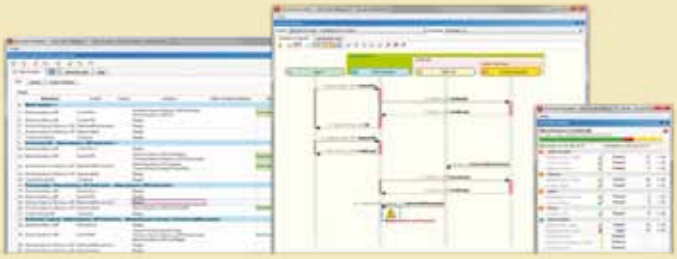
mind
embedded development
an ESSENSIUM division

ESSENSIUM

5-Year Contract Renewal for the ASD:Suite makes ASD technology available worldwide

verum®

Tools for building mathematically verified software



Verum Software Technologies announced that one of the world's largest multinational electronics companies has signed a five-year contract for the licensing of the ASD:Suite. The contract is the largest ASD:Suite licensing agreement to date, making it especially significant for Verum.

The contract renewal represents the extension of a long and successful partnership with the Netherlands-based firm that began in 2006. The renewal also marks the start of an expanded deployment of the Analytical Software Design (ASD) technology within the company, enabling broader, global usage of the ASD:Suite.

In addition to its healthcare division, which was the first division to employ the technology, all other divisions will now have access to the ASD:Suite, reinforcing the importance of the development platform within the company's different development organizations. The contract also facilitates for global rollout of the ASD:Suite, which enables developers outside of the Netherlands the opportunity to employ the ASD technology.

Robert Howe, Verum's CEO, commented on the news, *"We couldn't be more delighted that one of our leading customers has decided to use the ASD:Suite across a wider range of software design projects. Their commitment to product quality and innovation makes them ideal partners for Verum and strong supporters of the revolutionary approach to design enabled by ASD:Suite."* ■

About Verum Software Technologies

Verum Software Technologies supplies Software Design Automation that enables software designers to develop complex systems in less time and with zero defects. Experience shows that customers using the ASD:Suite can reduce their software development costs while speeding up development time, recouping their investment in less than three months. The ASD:Suite also reduces software rework and maintenance, which in turn leads to much greater customer satisfaction and lower lifecycle management costs. The difference between the ASD:Suite and comparable products is that Verum's ASD:Suite is built on a patented formal verification approach that guarantees the completeness and correctness of a software design.

How good are your software tests?

Testwell CTC++ Test Coverage Analyser will show you

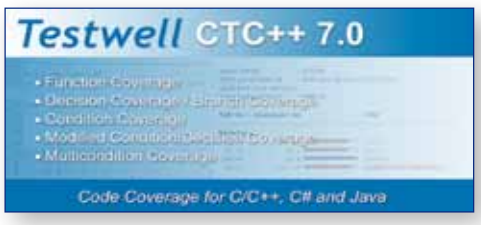
Verifysoft TECHNOLOGY

Softwaretest- und Analysetools

Test coverage is used to evaluate the completeness of software tests. There are many standards which require test coverage measurements. ISO 26262 Road Vehicules Functional Safety requires according to the Safety Integrity Level statement coverage, branch coverage or MC/DC (Modified Condition/ Decision Coverage). The aeronautics standard DO178-B/C requires test coverage up to MC/DC coverage. Coverage analysis is also widely used in healthcare industry and companies which are aware of higher software quality. The environment for software unit testing shall correspond as closely as possible to the target environment.

Testwell CTC++ is the ideal coverage tool to respond to this requirement, because it analyses for test coverage in any (even smallest) embedded targets.

The tool shows all coverage levels. It works with any compiler and supports C, C++, Java and C#. ■



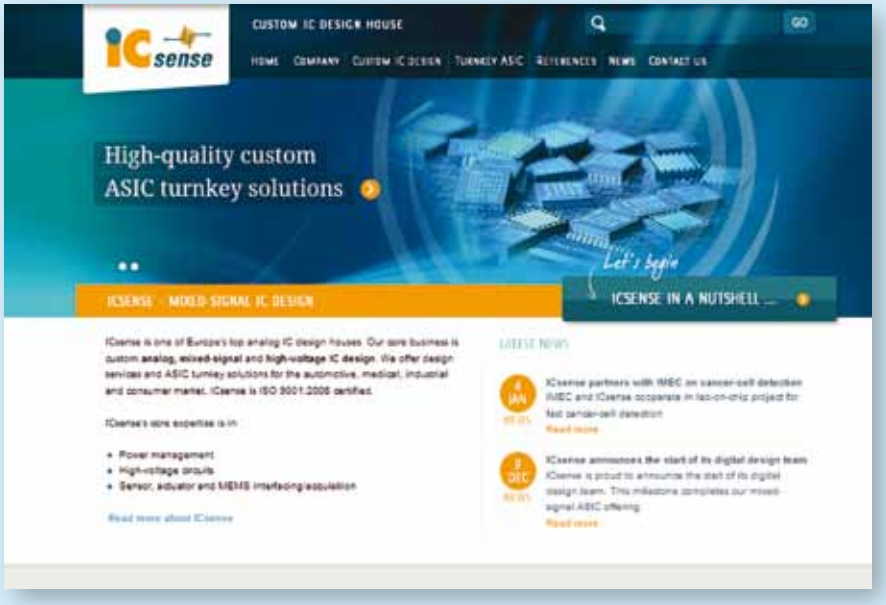
About Verifysoft Technology

Testing Solutions for Productivity and Quality

Verifysoft Technology is provider of software testing and analysis tools. The tool offering includes static and dynamic code analysis, complexity measures, unit test tools, code coverage, test and project management tools, automatic test case generation and execution and software diagnostics. Verifysoft provides also trainings and consulting. The company is headquartered in Offenburg, Germany.

ICsense expands innovative mixed-signal ASIC offering

Since its start in 2004, ICsense has been developing full mixed-signal ASICs for medical, industrial, automotive and consumer customers. To complete this mixed-signal ASIC offering, ICsense has started its own digital design team and set up a state-of-the-art mixed-signal verification flow.



"The combination of senior digital resources and industry-standard digital tools allows us to more efficiently and reliably develop complex mixed-signal ASICs, internally or together with our digital partner Easics," explains CEO Bram De Muer. *"In addition, we have invested in a fast and reliable simulation methodology for maximal mixed-signal chip-level simulation coverage. Our priority remains first-time functional silicon."*

More than 50 business cases

"On top of the technical quality of the ASICs, customers require a solid partner to handle their ASIC development and supply. We guide them from business case validation to end product," explains Sales Manager Jeroen Van Ham, *"Iteration on the specs and close cooperation is the key to success. In the end, our customers know their application best and we know how to translate it successfully into an ASIC. To illustrate what is possible, ICsense added more than 50 business cases to their brand new website."* Have a look at www.icsense.com to find out more.

Innovation at ISSCC

To stay at the top in the mixed-signal IC design world, ICsense strongly focuses on innovation through internal research and customer collaboration. *"We regularly invent new circuits and file or help file patents to protect the ideas. A good example is the architecture that ICsense created to generate high-voltages in standard low-voltage technologies,"* says De Muer, *"We presented it at the ISSCC conference in San Francisco this month. This is the annual industry's premier venue on new developments in the integrated-circuit industry."* The innovative technique has already been used in an IP-block in 40nm CMOS technology. The IO IP-block enables the interface from an ASIC to legacy off-chip components or data cards without the extra cost of expensive 2.5V/3.3V masks. De Muer: *"This IP block shows that we can leverage the internal research effort into successful innovative products that offer our customer a substantial cost reduction while maintaining performance."*

About ICsense

ICsense is a foundry independent IC design house offering advanced IC design services and turnkey ASIC solutions. The core business of ICsense is analog, mixed-signal and high-voltage IC design.

ICsense has key design expertise in power management, high-efficient DC/DC conversion, HV IC design, drivers, MEMS, sensor and actuator interfacing, ADC-DAC, timing circuits and ultra low power design. ICsense is an ISO 9001:2008 certified company.

With 34 experts in the field of high-performance analog, mixed-signal and high-voltage design, ICsense is amongst the top of European IC design houses.

continuation from page 10

Literature

[1] Millennium Research Group: OCT market forecasted for 60 % annual growth through 2015. BioOpticsWorld. October 2010.

[2] Laurie Morgus: Medical Imaging: Optical coherence tomography finds value in both art and science. LaserFocusWorld. August 2010.

[3] Barbara G. Goode: Optical Coherence Tomography: OCT aims for industrial application. LaserFocusWorld. Vol. 45, Nr. 9, September 2009.

[4] Yuuki Watanabe, Kazuhiko Yamada, Manabu Sato: In vivo non-mechanical scanning grating-generated optical coherence tomography using an InGaAs digital camera. Optics Communications. Vol. 261, 2006, pp. 376 – 380.

[5] Fraunhofer ILT: Optische Kohärenz-Tomographie in der kunststoffverarbeitenden Industrie. http://www.ilt.fraunhofer.de/ger/101678.html

[6] Xenics: Cheetah-640CL World's fastest InGaAs-camera. http://www.xenics.com/documents/20101101_Cheetah-640CL_Scientific.pdf

Embedded World

February 28-March 1, 2012
Nürnberg, Germany

embeddedworld2012 Exhibition&Conference ... it's a smarter world

This year, DSP Valley will again participate in the main exhibition regarding embedded technology, Embedded World in Nürnberg. From February 28th, until March 1st, DSP Valley will be present in the exhibition area on a group booth, together with Easics, ICsense, Essensium, Deltatec, Byte Paradigm, Luperco, Sigasi and Emweb. Make sure to visit us in hall 4, booth nr. 109!

Android Training

http://www.mind.be/?page=training

March 5-7, 2012
Brussels, Belgium

mind embedded development an ESSENSIUM division

Overview:

This 3 days training is intended for developers who want to learn to write Android applications.

In a 50 to 60% lab-time approach, the participants get a real hands-on experience and they learn how to work with Android and how to avoid classical pitfalls. The training first describes the Android architecture, and then covers all major parts of the API and application through theory and exercises.

During the training, all attendees get direct feed-back in an interactive manner, and at the end of the training they are ready to work on their first real Android projects.
During the training, all attendees also receive an Android based device so that they can continue to experiment later.

Seminar: Mobility Management today and tomorrow

http://www.verotech.be/mobiliteitsbeheer-vandaag-en-morgen

March 21, 2012
Brabanthal, Leuven, Belgium

In 2011, more than 570.000 new cars were registered in Belgium: a new record. On the other hand, a total length in traffic jams of over 300km is no longer an exception nowadays. The capacity of our transport system is at certain times of day and at certain locations insufficient.

Nevertheless, there exist ways to move more efficient, more sustainable, and safer, or in short: smarter. Using Smart Mobility and advanced Traffic Management, the driver can benefit from information about the different traffic options by receiving them in an adequate manner.

This seminar gathers a number of players from this domain to focus on the challenges ahead and to elaborate on the innovative solutions and achieved results. Applications of Road Pricing as well as Floating Car Data will be addressed during this event. The panel discussion will offer an excellent possibility to discuss solutions for today's mobility problems.

VERCTECH a community of experts creating your future

Program:

13u30: Registration participants
14u00: Welcome by Leuven Inc and VeroTech
14u15: Traffic management: general frame and opportunities
Sven Maerivoet, Consultant Transport & Mobility Leuven, TML
14u45: Smart road user charging for trucks: perspectives in Belgium and the link with Car Safety. Frank Daems, Director Business Management, NXP and Liesbeth Gommé, Consultant VeroTech
15u15: Smart mobility in Leuven: results field test for Road Pricing
Sven Maerivoet, Consultant Transport & Mobility Leuven
15u45: Queue waves with Floating Car Data. Steven Logghe, Chief Traffic Be-Mobile
16u15: Panel
16u50: Conclusions
17u00: Networking Drink

The seminar is in Dutch. More information and registration can be found on the seminar website.

ECUMICT, the European Conference on the Use of Modern Information and Communication Technologies

www.ecumict.be

March 22, 23, 2012
KAHO St Lieven,
Gent, Belgium

On the 22nd en 23th of March 2012 the 5th edition of ECUMICT, the European Conference on the Use of Modern Information and Communication Technologies, is organized.

ECUMICT will be a two-days conference on the use of modern information and communication technologies, organized by the engineering department of KAH0 St Lieven, Technologie campus Gent, in cooperation with a scientific committee composed of experts from universities and institutes of higher education in Europe.

The fifth edition of ECUMICT has a special focus on wireless and mobile applications. ECUMICT 2012 wants to offer a forum for researchers to discuss on recent developments and future cooperation in this domain.
For further information and registration we refer to the seminar website.

Acivs 2012: Advanced Concepts for Intelligent Vision Systems

http://acivs.org/acivs2012

Sept. 4-7 2012
Brno University of Technology,
Brno, Czech Republic

Acivs 2012 is a conference focusing on techniques for building adaptive, intelligent, safe and secure imaging systems. Acivs 2012 consists of four days of lecture sessions, both regular (25 minutes) and invited presentations, poster sessions. The proceedings of Acivs 2012 will be published by Springer Verlag in the Lecture Notes in Computer Science series (pending approval) and are listed in the ISI proceedings index.

Acivs 2012 will also feature a conference dinner, and other social activities.

Both classical research papers and application papers are welcome. The submission process can be found on the Acivs 2012 website (http://acivs.org/acivs2012/).

Important deadlines

- → March 12, 2012 Full paper submission
- → May 21, 2012 Notification of acceptance
- → June 18, 2012 Camera-ready papers due
- → June 30, 2012 Registration deadline for authors of accepted papers
- → July 15, 2012 Early registration deadline
- → Sept. 4-7 2012 Acivs 2012

Contact Information

KU Leuven ESAT-MICAS at ISSCC 2012 • p.1
Prof. Patrick Reynaert, Prof. Michiel Steyaert, Prof. Wim Dehaene, ESAT-MICAS group KU Leuven
Tel. +32 16 321077 • Fax +32 16 321975 • www.esat.kuleuven.be/micas
patrick.reynaert@esat.kuleuven.be • michiel.steyaert@esat.kuleuven.be • wim.dehaene@esat.kuleuven.be

PragmaDev • p.3 Mr. Emmanuel Gaudin, Founder & CEO PragmaDev
Tel. +33 1 42 741538 • Fax +33 1 42 741558 • www.pragmadev.com • emmanuel.gaudin@pragmadev.com

InGaAs cameras for OCT applications • p.4
Mr. Bob Grietens, CEO Xenics • Mr. Patrick Merken • Tel. +32 16 389900 • www.xenics.com • bob.grietens@xenics.com

Imec presents a MEMS energy harvester suitable for shock-induced energy harvesting in car tires • p.6
Compact, low-cost and fast hyperspectral imaging solution • p.11
Hanne Degans, External Communications Officer imec • Tel. +32 16 281769 • Mobile +32 486 065175
www.imec.be • hanne.degans@imec.be

Smart Engine for Public Key cryptography • p.6 Mr. Thierry Pauwels, Technical Marketing Barco Silex
Tel. +32 10 454904 • Fax +32 10 454934 • www.barco-silex.com/crypto • thierry.pauwels@barco.com

Essensium - Mind helps customers make the most of open source software • p.12
Mr. Adrien Ampélas, Operations Essensium-Mind • Tel. +32 16 286500 • Fax +32 16 286501
www.essensium.com • adrien.ampelas@essensium.com

5-Year Contract Renewal for the ASD: Suite makes ASD technology available worldwide • p.13
Mr. Maarten van Alphen, Marketing Manager Verum • Tel. +31 402 359090 • Fax +31 402 359099
www.verum.com • maarten.van.alphen@verum.com

How good are your software tests? • p.13 Mr. Klaus Lambertz, Managing Director VerifySoft
Tel. +49 781 127 8118-0 • Fax +49 781 63 92 029 • www.verifysoft.com • lambertz@verifysoft.com

ICsense expands innovative mixed-signal ASIC offering • p.14
Mr. Bram De Muer, CEO ICsense • Tel. +32 16 589702 • Fax +32 16 589720 • www.icsense.com • demuer@icsense.com

Interreg Vlaanderen Nederland
Europa investeert in uw regio

This publication has been realized with the support of IWT and the European Union (EFRO).