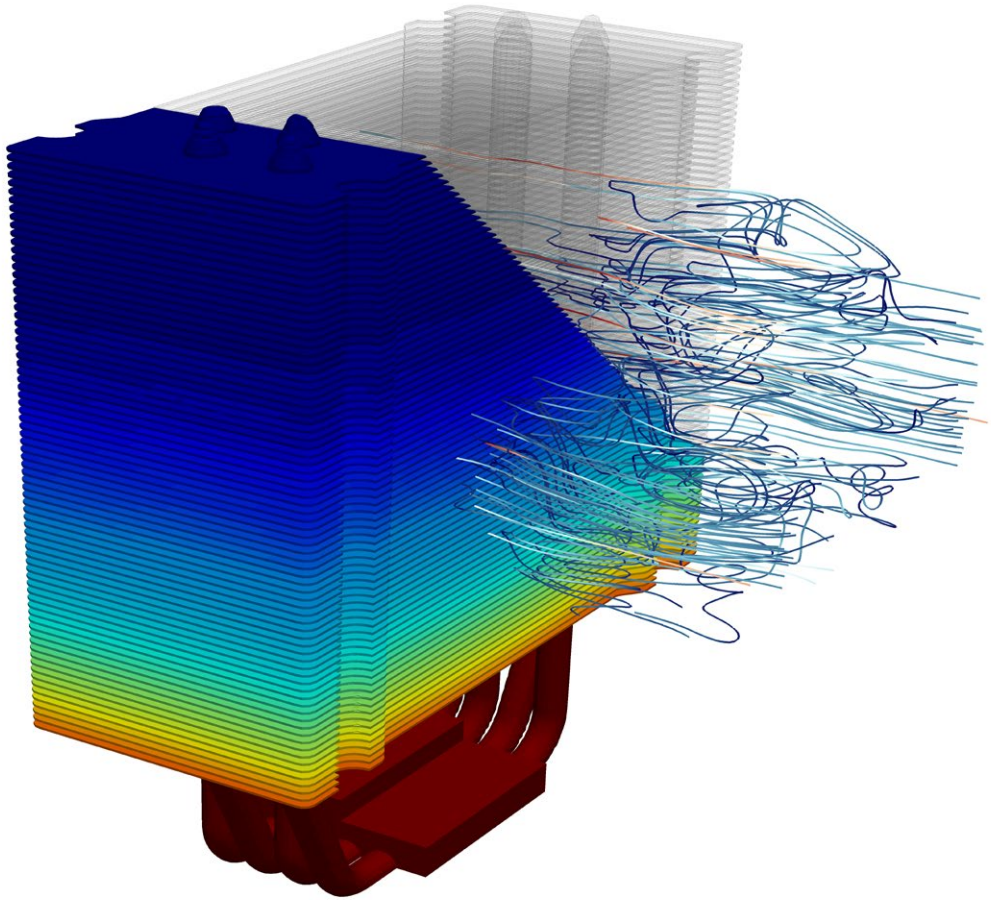
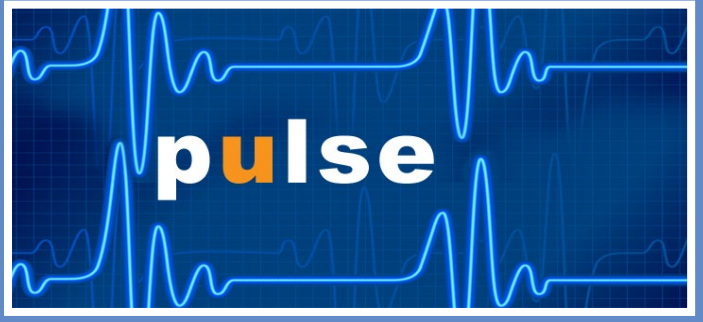
EDN europe

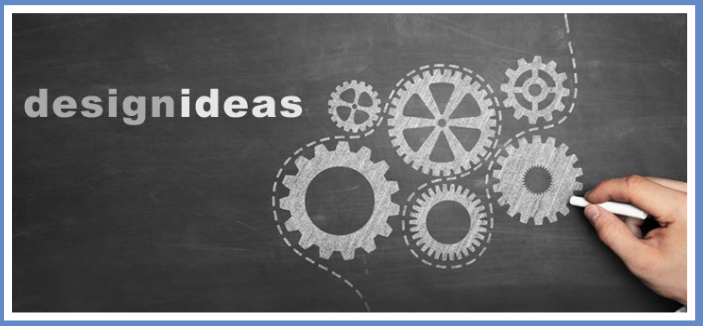
MARCH 2017

www.edn-europe.com



Web-based virtual thermal prototyping





IMPORTANT MESSAGE FOR OUR READERS

Dear readers,

This issue of your monthly electronics design magazine will be the last one bearing the EDN Europe Title. As of the April issue, your favourite magazine will be titled eeDesign News Europe.
This change in branding is due to changes in the USA which for once not of Mr Trump's doing, but have to do with the acquisition of EDN in the USA by Aspencore, a division of Arrow who have decided to no longer license the brand after many years of successful cooperation.
Effective April 1st, the EDN Europe web site will also use a new URL www.eedesignnewseurope.com but we'll make sure the old URLs are redirected to the new one so everyone will have a direct access to the new site.
There will be no change to our talented editorial team who will continue to inform you on a daily basis online and in newsletters about all the latest designs and technologies available from around the world - you can subscribe to the newsletters directly from the website - and monthly in our digital edition.
European Business Press SA, publisher of eeNews Europe, eeDesignNews and MWee is an independent international publishing company based in Belgium that was created 20 years ago to offer a panEuropean view to the electronics industry in Europe. EBP manage their own data bases with strict respect of privacy and have leading edge in-house production services.
We thank you for your support and hope you will continue enjoy reading our publications!

André Rousselot
Publisher

eeNews EUROPE

eeDesign EUROPE

MWee RF - Microwave

COVER

Virtual thermal prototyping on a web-based platform

Belgian startup Diabatix is offering access to efficient thermal design through its web-based solution platform. The solution as a service makes thermal know-how accessible to any engineer. It guides them in simulating and optimizing cooling systems better and faster, without CFD consultants and traditional software licenses.
The tool has the capability to autonomously suggest cooling system geometries in natural free-form shapes, pushing thermal performance to the limit. Critical thermal applications addressed with the Diabatix solution platform, with supercomputers under the skin, yield claimed cooling performance improvements up to 30%.
Liquid cooling is key in precision and industrial machines as well as battery cooling for electric cars. Unfortunately, developing proper cooling is easier said than done for the involved manufacturers. Despite capable CFD software tools, they struggle with trial-and-error engineering, physical prototyping, lengthy simulations and use of consultants.
The company says that its platform offered as a service is a user-friendly software environment that no longer requires engineers and designers to be thermal specialists. The Diabatix solution platform allows any engineer to design, simulate and optimise cooling systems starting from the functional thermal requirements.
Read the complete item here

FEATUREARTICLES

ONLINE THIS MONTH

Static analysis in a secure software development lifecycle *by Billl Graham, GrammaTech*

White Paper; Intersil: The right battery chemistry for automotive applications

White Paper; PRQA: Developing secure embedded software

White Paper; Mentor Graphics: Fundamentals of signal integrity analysis

EDN's columns

THE NEW NORMAL

by Graham Prophet, Editor

In February 2017, the Economist Intelligence Unit (London), with sponsorship from ARM and IBM, published this year's results of its Internet of Things Business Index. This global survey posed a series of questions on attitudes to, and adoption of, the IoT. In contrast to the perspective we normally feature in these pages – that of the design community charged with bringing the hardware and software of the IoT into meaningful existence – this analysis provides an insight into the thinking of those whose task it is to translate the broad concepts into workable business models that will yield revenue or, at least, control costs.

The survey sought opinions from an even spread of respondents across ten business sectors, with 30% from North America; 30% from Europe; 30% from Asia-Pacific, and the balance from the rest of the world. It targeted a range of departments, including IT, finance, operations and production, strategy and business development: there was a cross section of management seniority, and of business size by turnover.

From that base, the survey charted answers to a range of questions structured to show how far the IoT is being adopted, where it is having a real business impact, and how far along the path to the predicted future of IoT ubiquity we have come. Comparing the replies to those of surveys in previous years, the overall impression is one of measured progress.

The EIU's analysts report that many respondents say that the IoT has already had a marked impact on their business model, allowing them to generate greater revenue and leading to innovation within their organisations. One-fifth have already seen a major impact on their industry, and a further 30% believe they will see significant impacts in the near future.

However, many executives feel that the IoT has not progressed quite as fast as they had expected three years ago. So far, fewer than one in ten companies surveyed have achieved “extensive” implementation of the IoT for both external and internal operations. External means, broadly, the effect on business as it faces the outside world; provision of products and services. Internal relates to matters such as improving operating efficiency, and cutting costs.

Although underlying technologies and high-level business models have matured, says the survey, companies are discovering that there are considerable organisational challenges to be addressed before the IoT will become a mass-market tool, such as the need to understand how companies must adapt their internal structures, as well as their market strategies. That will include how they work with suppliers.

What do they see as key challenges? ARM's CTO Mike Muller offers some gleanings; when asked what are the key barriers, survey respondents cite the cost of investment in IoT infrastructure; security and privacy concerns; and lack of senior management knowledge – as the top three.

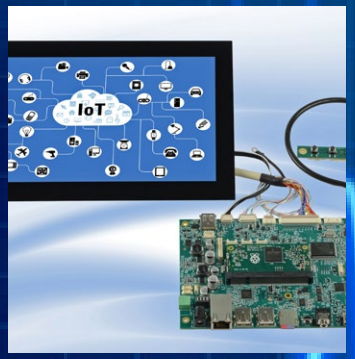
But these concerns,Muller comments, are a step onwards from the earlier stage of worrying about doing anything at all. And the intentions going forward appear to be “more of the same” - typically involving modest increases in investment plans.

ARM itself, Muller notes, has focussed on three specific areas (among others); development of hardware architectures, particularly as they manage issues of trust and security; provision of firmware to ease development; and building a “chips to cloud” infrastructure. This last is key, Muller says, noting the move to active management of devices.

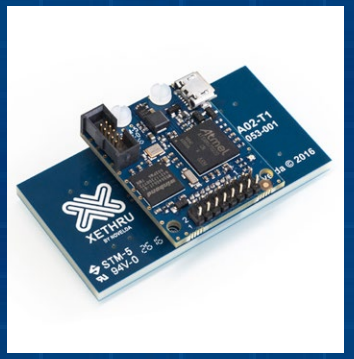
So the IoT is a story of, in some areas, slower-than-expected uptake and in one measure, actually a small step backwards. To which we might add the following thought. The failure, if it is a failure, to find spectacular growth stories and overwhelming enthusiasm may also be a reflection of the extent to which what we might term IoT thinking has already become mainstream.

Stripped of “IoT hype”, there is the realisation that interconnectedness is simply the norm for systems going forward, and as well as making that happen, we have to tentatively work towards extracting the maximum value from the phenomenon.

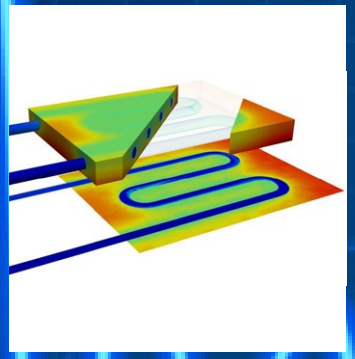
pulse

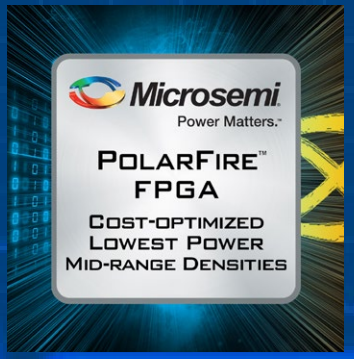

IoT

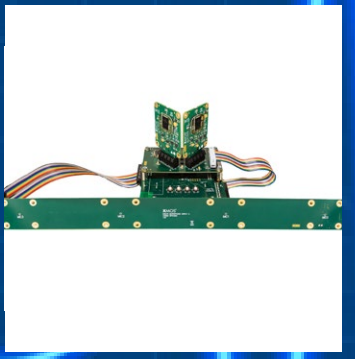

0.96 mm
1.56 mm
0.8 mm
0.8 mm
10.5mΩ/4A nFET
SLG59M1735C
33mΩ pFET
SLG59M1730C 1A
SLG59M1736C 2A

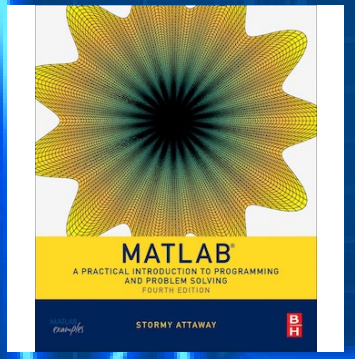

XETHRU
A02-T1
053-001


All Programmable RFSoC
Software Programmable
Hardware Programmable
Real-Time
FPGA
AIEngine
RF-Analog
XILINX




Microsemi
Power Matters.
PolarFire™
FPGA
Cost-optimized
Lowest Power
Mid-range Densities

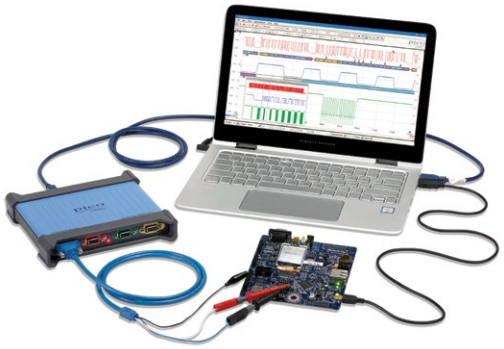



MATLAB
A PRACTICAL INTRODUCTION TO PROGRAMMING AND PROBLEM SOLVING
FOURTH EDITION
STORMY ATTAWAY

USB scope enables high-res measurements of differential voltage waveforms

USB oscilloscope specialist Pico Technology's PicoScope 4444 high-resolution differential oscilloscope features four true differential input channels and a range of accessories for measurements from millivolt to 1000V CAT III applications.

This PicoScope addresses the problem of making accurate voltage waveform measurements on circuit elements that are not ground-referenced, without the risk of short circuits that could damage the device under test or the measuring instrument. “The 4444 gives electrical engineers the freedom to make differential voltage measurements in the presence of common-mode signals,” said Trevor Smith, Business Development Manager, Test & Measurement, at Pico Technology. “The instrument has 14-bit resolution on four channels and 256 mega-sample capture memory, for precise analysis of complex waveforms ranging "from biomedical sensors to current probes and 1000 V CAT III power distribution circuits.”



To make low-voltage measurements in the presence of high common-mode noise or varying offset voltages, ground-referenced oscilloscopes require use of two input channels and an A–B math function to observe the differential signal of interest. Pico comments that as well as requiring two input channels, most scopes don’t have a high enough common-mode rejection ratio (CMRR), nor the resolution to make measurements with sufficient precision.

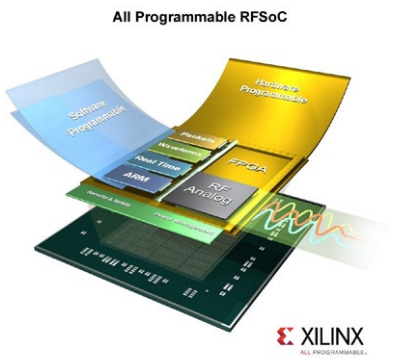
Engineers working on polyphase power distribution systems need to measure phase-to-phase AC voltages, rather than phase to ground. A ground-referenced scope can’t be used as it will cause a short circuit. External differential probes are a solution but they are quite expensive and cumbersome, with each probe requiring its own power supply. The PicoScope 4444 has differential inputs and a choice of 1:1 low-voltage and 25:1 1000V CAT III probes to address both of these problems.

A PicoScope 4444 standard kit, consisting of a PicoScope 4444, three PicoConnect 441 differential 1:1 probes and one TA271 D9-BNC adaptor is priced at $1,535 / €1,325 / £1,075.

Complete article, here

Fast RF ADCs/DACs integrated with FPGA for programmable 5G designs

Direct RF sampling radio architectures are attractive for enabling the flexibility and software-defined-radio features that will be needed for 5G wireless services. The RF is directly digitised and all signal processing takes place in the digital domain. The digital processing in such designs has typically been performed in advanced FPGAs. However, such architectures can be power hungry, not least because very high data volumes must be transferred from sampling front-ends to the processing matrix, at very high speeds, which consumes power. Xilinx has been promoting its “all-programmable” concept for some time, with products such as its Zynq range, which combine FPGA hardware (programmable by configuration) with embedded processor cores (software programma-



ble) – hence, all-programmable. Now, it has added high speed data conversion functions, integrated on-chip, to that mix. Having the sampled data on-chip offers power savings over driving that data over chip-chip lines.

Xilinx is presenting this move as a "disruptive integration and architectural breakthrough for 5G wireless, with RF-class analogue technology." Its RFSoC devices will enable 50-75% power and footprint reduction for 5G massive MIMO radio and millimeter-wave wireless backhaul, the company says. The level of integration achieved will enable an 8x8 MIMO receiver on a single (monolithic) chip.

The integrated 16nm-based RF data conversion technology includes:

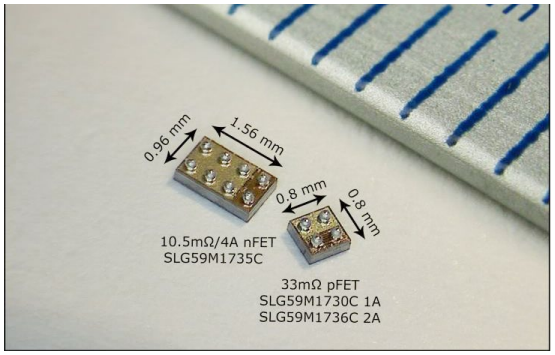
- Direct RF sampling for simplified analogue design, greater accuracy, smaller form factor, and lower power
- 12-bit ADCs at up to 4 GSPS, high channel count, with digital down-conversion
- 14-bit DACs at up to 6.4 GSPS, high channel count, with digital up conversion.

Complete article, here

Wafer-scale-packaged integrated FET switches handle 1 – 4A

Silego Technology has developed a series of integrated power switches for use in mobile and battery powered products, to carry out power gating of functional blocks within a design; the devices come in sub-mm-size chip scale packages, handle currents from 1 to 4 A, and integrate functions such as in-rush current limiting and over-current or thermal protection. Employing its own FET IP, the company has released three low-RDSON switches. These are the first products that Silego has issued in chip-scale packaging; the company hints that other devices from its range, such as the configurable-function PAC devices, may appear in similar outlines in the future. In the GFET3 Integrated Power Switch (IPS) portfolio, the three new switches are aimed at extremely PCB-space-constrained, high-performance applications in tablet PC, smartphones and fitness band markets, and offer high-side power control.

For smartphone and fitness band applications, the 0.64 mm² (0.8 x 0.8 mm) SLG59M1730C (33 mΩ/1A) and the SLG59M1736C (33 mΩ/2.2A) are low-leakage, self-powered p-FET IPSs that can operate from 2.5 V to 5.5 V supply voltages and draw very little supply current. Both products offer low-threshold ON/OFF control, fast output voltage discharge, and a controlled input current profile on startup. This can, Silego says, avoid battery-voltage 'sag' when powering from small, high-internal-resistance cells, which may cause an associated MCU to re-boot. The SLG59M1730C/SLG59M1736C offer a controlled 16.5 mA inrush current profile on startup.



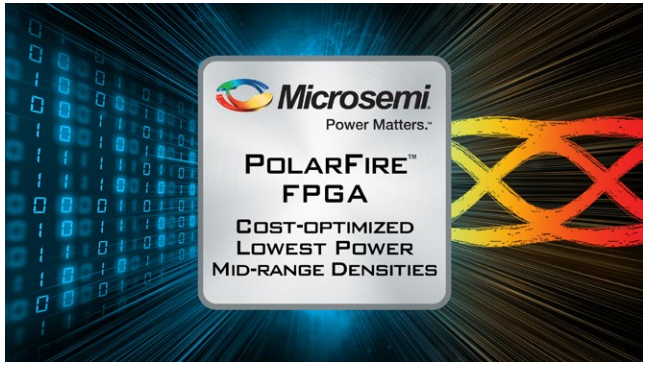
For higher-power tablet pc applications, the SLG59M1735C is a 10.5 mΩ/4A n-FET IPS with a full suite of protection features. Powered from 2.5V to 5.5V supplies, the input voltage range extends down to 0.9V to accommodate 1.0V high-current rails found in FPGA, ASIC, and processor power sequencing applications. The SLG59M1735C feature set includes: ON/OFF control, soft-start control, under-voltage detection, and two-level current-limit protection.

Complete article, here

Mid-range, flash-based FPGAs offer 500 LEs, 12.7G SerDes

Microsemi positions its PolarFire range of FPGAs as the lowest power, cost-optimized FPGA product family for access networks, wireless infrastructure, defence and industry 4.0 markets, and claims a cost advantage over alternative FPGAs of 50%.

The programmables offer up to 500k logic elements, 12.7G transceivers at up to 50% lower power than competing mid-range FPGAs, and also feature optimised security and reliability. Microsemi aims the product family for a range of applications within wireline access networks and cellular infrastructure, defence and commercial aviation markets, as well as industry 4.0 which includes the industrial automation and Internet of Things (IoT) markets.



For the communications infrastructure market, Microsemi presents these devices as providing cost-effective bandwidth processing capabilities for the increasing number of converged 10 Gpbs ports with the lowest power footprint. The new FPGA product family also contains features to address the market's concerns over cyber security threats as well as reliability concerns that face deep submicron SRAM-based FPGAs as they relate to single event upsets (SEUs) in their configuration memory. The company says that a radiation-induced event that could 'flip' a bit in the configuration SRAM of a competitive part would leave its non-volatile configuration memory unaffected. Additional features to aid with reliability include built-in single error correction and double error detection (SECDED) as well as memory interleaving on large static random access memory (LSRAMs), and system controller suspend mode for safety critical design

In collaboration with Silicon Creations, Microsemi has developed a

12.7 Gbps transceiver fully optimized to be area efficient and low power, resulting in total power of less than 90 mW at 10 Gbps. With low device static power of 25 mW at 100k logic elements (LEs), zero inrush current and its Flash*Freeze mode for standby power of 130 mW at 25C, PolarFire devices are up to 50% lower power than competing FPGAs for the same application. Microsemi provides designers with a power estimator to analyze power consumption of their designs.

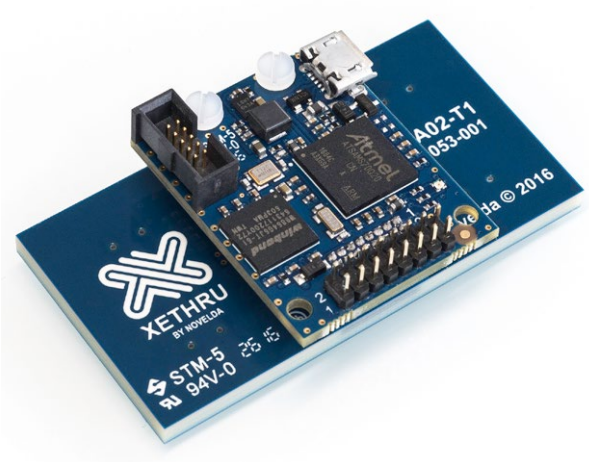
PolarFire FPGAs offer Cryptography Research Incorporated (CRI) patented differential power analysis (DPA) bitstream protection, integrated physically unclonable function (PUF), 56 kB of secure embedded non-volatile memory (eNVM), built-in tamper detectors and countermeasures, true random number generators, integrated Athena TeraFire EXP5200B Crypto Co-processors (Suite B capable) and a CRI DPA countermeasures pass-through licence.

Complete article, here

Single-chip, UWB radar offers a scalable sensor development platform

Novelda (Oslo, Norway) first disclosed its single-chip radar-based sensor technology in 2015. The company employs a low-power pulsed waveform at GHz frequencies, that comprises an ultra-wideband signal; UWB is noted for its ability to provide very accurate ranging information. The company has now released its second-generation IC, for uses in medical and health monitoring, in people- (presence-)sensing, and potentially in other sensing applications.

The XeThru Developer Platform is based on Novelda's second-generation X4 ultra-wideband (UWB) impulse radar system-on-chip (SoC). With this technology, OEMs and system developers can implement sensors that can detect small movements, determine presence and room occupancy, and monitor respiration and other human vital signs with high levels of accuracy and discrimination.



The patient/infant monitoring application has been a key sector for Novelda, and remains a principal target.

The UWB radar return can detect movements of the order of 1mm or less, through dielectric materials such as bedclothes, so can detect respiration or heartbeat at a distance.

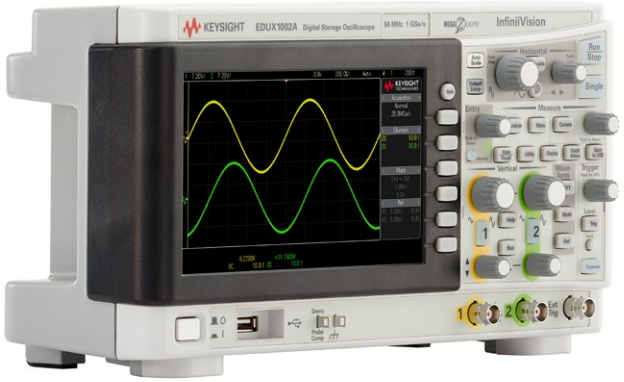
Integrated into a single chip, the X4 UWB impulse radar SoC combines a transmitter, which can operate at centre frequencies of either 7.29 GHz or 8.748 GHz for unlicensed operation in worldwide markets, with a direct RF sampling receiver and a fully programmable system controller. The X4 SoC delivers some key performance improvements over the previous design: its frame size is now configurable for different applications and the range, for simultaneous observation, has been increased from 1m to 10m. That is, the output is a 'frame' that contains a signal from every reflection out to (for example) 10m. (Those unfamiliar with radar terminology might think of it as analogous to a time-domain reflectometry trace in test & measurement terms.) It is 10x faster and much more suitable for presence detection; its on-chip advanced power management functions enable low-power duty cycle control and dramatically reducing power dissipation; and its

higher level of integration reduces external component BOM costs by more than 50%.
The company notes three areas which cause difficulty for newcomers to the technology, and says it has accommodated all of them. First is the task of handling and routing the GHz-range signals; the impulse power is very low and careful matching from CMOS chip to antenna is needed. Then, the UWB waveform needs a flat response across its full 'spread'. These factors are dealt with by provision of prototyping and low/medium volume assembled boards, and by layout assistance for OEM production. Then, there is the task of interpreting the data: this is where the API to any host computing system comes in.

Complete article, here

Low-cost, entry-level scopes by Keysight, from under €450

Keysight Technologies has released a series of oscilloscopes that while it is intended for (among other sectors) the education market, nevertheless has professional-level functionality and software analysis features; the units are available with 50 and 100 MHz analogue bandwidths.
The units have 6-in-1 instrument integration, and include a "Keysight exclusive" feature; a built-in frequency response analyzer with Bode plotting. Suitable for students and new scope users, the instruments come with an educator's resource kit with built-in training signals and, as standard, with a comprehensive oscilloscope lab guide.



With a starting price below €450, the 1000 X-Series uses Keysight's MegaZoom IV custom ASIC technology, which enables a high 50,000 waveforms per second update rate. This makes it easier to see random and infrequent glitches and anomalies that similarly-priced oscilloscopes might miss. The 1000 X-Series also has a high sampling rate of up to 2 Gsamples/sec and comes standard with two probes. In addition to being an oscilloscope, the 1000 X-Series is also a serial protocol analyzer, digital voltmeter and frequency meter—and the EDUX1002G and DSOX1102G models include a frequency response analyzer and WaveGen function generator. Bode plot fundamentals are easy to teach with the built in WaveGen and frequency response analysis.

Complete article, here

Voice recognition by sensor fusion; radar plus MEMS microphones

Infineon Technologies has collaborated with XMOS (Bristol, UK) to deliver a new building block for voice recognition. It features a combination of radar and silicon microphone sensors from Infineon and audio processor from XMOS. The devices provide far field voice capture by audio beamforming combined with radar target presence detection.
Together, the two sensing tech-

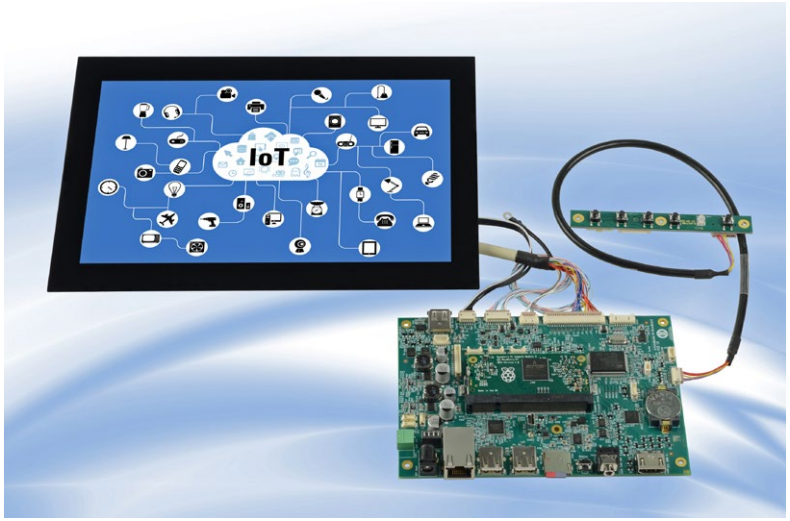
niques guarantee optimal sound recognition and flawless execution for digital voice assistance across a broad range of voice-controlled devices. Target applications are “especially smart” home, as well as smart TV and set top box, secure keyless entry systems, and other voice-operated consumer devices.

The performance of current MEMS microphone limits the effectiveness of systems: when multiple persons are speaking, the veracity and location of the voice source cannot be precisely identified and separated from inanimate object noise. Infineon’s 60 GHz 2Tx/4Rx radar IC with accompanying antenna and the 70 dB SNR microphone helps to overcome these impediments. The microphones are based on Infineon’s dual backplate MEMS technology, suited to far-field voice capture and beamforming. Improving the SNR of the microphone will further enhance the performance.

Complete article, here

Raspberry PI-based TFT controller for industrial use

Distec (Germering, Germany), a specialist in TFT flat screens and system solutions for industrial and multimedia applications, has added to its Artista TFT controller family: the Artista-IoT for Industry 4.0 and the Internet of Things (IoT).



This TFT controller is a Base-Board with a socket for the latest generation of the Raspberry PI Compute Module (CM3). "The Artista-IoT is only a simple TFT controller, but the perfect basis for cost-efficient IoT and Industry 4.0 applications," explained Matthias Keller, Head of Sales and Marketing at Distec GmbH. "Internet of Things is the keyword and a costly PC with a lot of peripherals is now superfluous: our solution enables us to network almost every device intelligently, without any license costs." The Artista-IoT allows the direct connection of almost all common TFT types without additional hardware. Distec can provide individual solutions for: Industrial HMI, medical, aviation, digital signage, and digital whiteboard.

The controller can be integrated into existing Windows and Linux environments and can be adapted to suit individual needs. Distec offers a starter set consisting of BaseBoard, CM3, 10.1-inch Super Fine TFT display with PCAP Multi-Touch and all necessary cables. The Artista-IoT is based on a full-fledged scaler chip and controls almost every TFT display and modern PCAP multi-touch screens directly. The controller board allows special functions such as DICOM pre-set, gamma correction and colour calibration. It supports 100 Mbit Ethernet and provides a real-time clock. Available interfaces include USB, GPIOs, I²C and UART.

Complete article, here

Keyword-smart microphone for voice-controlled devices

STMicroelectronics, DSP Group, and Sensory have collaborated to design ultra-low power voice processing and MEMS microphone circuitry that enables sound detection and keyword recognition in a miniaturized single package. It merges ST's MEMS microphone and packaging knowledge with DSP Group's voice-processing expertise and Sensory's voice-recognition firmware.
The small System-in-Package (SiP) device integrates a low-power ST MEMS microphone backed by DSP Group's ultra-low power voice-processing chip and Sensory's voice-recognition firmware. The solution employs ST's packaging technology to achieve a powerful and lightweight package, extremely long battery runtimes, and advanced functionality.
Although typical wake-on-sound microphones eliminate the need for users to touch the device to wake it from sleep mode, they suffer from limited processing power and wake the main system processor to recognize the received instruction. Using the computation capabilities from DSP Group, ST's microphone detects and recognizes instructions without waking the main system, enabling energy-efficient, intuitive, and seamless interactions for users speaking to voice-operated appliances such as smart speakers, TV remotes, and smart home systems.
The new microphone solution incorporates DSP Group's HDClear ultra-low power audio processing chip to significantly reduce energy consumption, extending the lifetime of battery-operated equipment for several years without the need to recharge or replace battery. Responses to voice commands are also faster, because the system acts on the instruction immediately without first having to recognize it.

Complete article, here

512 Gbit, 64-layer flash memory sampling – 1 TByte in a package is next

Toshiba has announced sampling of 64-layer, 512-gigabit 3D flash memory, the largest device it has built to date in its BiCS FLASH chip series. Using a stacked cell structure, the 64-layer device achieves its 512-gigabit (64-gigabytes) capacity with 3-bit-per-cell (triple-level cell, TLC) technology. The device will be used in applications that include enterprise and consumer SSD. Sample shipments of the chip started early in 2017, and mass production is scheduled for the second half of the calendar year.
Toshiba says it is continuing to refine BiCS FLASH, and the next milestone on its development roadmap is the industry's largest capacity, a 1-terabyte product with a 16-die stacked architecture in a single package. Plans call for the start of sample shipments in April 2017. For the 512-gigabit device, Toshiba used an advanced 64-layer stacking process to realize a 65% larger capacity per unit chip size than the 48-layer 256-gigabit (32-gigabytes) device [that it already produces], and has increased memory capacity per silicon wafer, reducing the cost per bit.

Complete article, here

BeagleBoards added for industrial and maker developers

Distribution company Farnell element14 is adding to its BeagleBoard range; three added products comprise BeagleBone Black Wireless, the element14 Wireless Connectivity Cape and the element14 4.3in. Display Cape. BeagleBone Black Wireless now has Wi-Fi and Bluetooth capabilities built in, removing the need for design or hardware workarounds. Focused on connectivity, the 10/100 Ethernet port from the BeagleBone Black is replaced with a TI WiLink WL1835 which is a high-performance 802.11 b/g/n 2.4 GHz Wi-Fi module with Bluetooth. Debian Linux is preinstalled and there is 4 GB of onboard eMMC memory. Element 14 says designers can be developing using their web browser in less than 5 minutes using just one USB cable. This BeagleBone Black Wireless is also compatible with existing cape plug-in boards designed for BeagleBone Black. For designers already working with the BeagleBone Black and element14 BeagleBone Black Industrial, wireless communication is now available through the element14 Wireless Connectivity Cape, which expands the capability of the BeagleBone device by adding a variety of wireless connectivity standards. The element14 Display Cape allows designers using the BeagleBone boards to connect a 4.3-inch colour touchscreen display directly to the board.

Complete article, here

1 GHz oscilloscopes, and ARBs, in PXIe format

Keysight Technologies has introduced 10 PXIe instruments that, in addition to general purpose test and measurement, are applicable to research in 5G communications, aerospace and defence, and quantum technologies. These arbitrary waveform generators, digitizers and oscilloscopes provide up to 1 GHz bandwidth for complex baseband IQ signal generation and analysis.
Resources include an on-card FPGA that Keysight says is accessible to non-programmers, to customize and accelerate test while accessing full performance of the FPGA. Precise timing and synchronization provide phase coherency for complex, multi-channel configurations.

Among the 10 instruments, an arbitrary waveform generator (AWG) has three highly synchronized channels for precise tuning of IQ waveforms and envelope tracking: and a module claimed as the industry's first full-featured PXI oscilloscope. The AWG and oscilloscopes provide up to 1 GHz bandwidth. The complete range includes AWGs and digitizers that allow engineers to build onto the instrument's core capabilities or insert custom algorithms into the on-board FPGAs. A graphical design environment enables adding customization for emerging technologies, research and design, while accessing the full performance and speed of the FPGA. The M3xxxA AWGs and digitizers

use the FPGA and PXI reference clock to provide real-time sequencing and multi-channel/ multi-module synchronization to support advanced multi-channel applications such as multi-user beamforming technologies and quantum computing. The M9243A PXIe oscilloscope is built with Keysight's InfiniiVision oscilloscope technology, providing up to 1 GHz bandwidth for quick analysis and troubleshooting of wideband signals. With a 1,000,000 waveforms per second update rate and advanced probing technology, the oscilloscope enables troubleshooting of random and intermittent signals.

Complete article, here

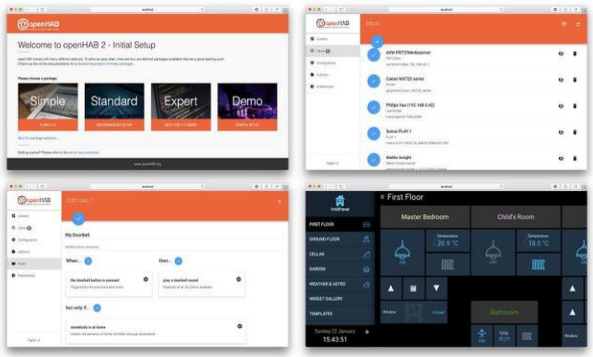
ST and USound to to make first MEMS speakers for mobiles

Miniaturized thin-film piezoelectric-MEMS actuators will build micro-speakers that offer better sound quality and efficiency, according to STMicroelectronics and audio company USound GmbH, who have announced their collaboration on the industrialization and production of the world's first MEMS actuators for smart audio systems in portable devices. The patented micro-speaker technology from USound aims to replace commonly used balanced-armature and electrodynamic receivers for handsets with a small piezo-MEMS actuator. Manufactured using ST's thin-film piezoelectric (TFP) technology, these actuators will improve scalability and cost while assuring lower power consumption and heat dissipation in "hearables" and smartphones devices, without compromising audio quality.

Complete article, here

Free and open code for smart home platform, as a Ubuntu snap

Canonical, openHAB Foundation and Azul Systems have launched the snap packaging of openHAB 2.0, a completely free open smart home platform that acts as a control hub for home IoT setups, that can be an alternative to Apple Homekit and Samsung SmartThings.
OpenHAB 2.0 can be used to control, automate and complement smart home setups. It is an open platform, and therefore is not tied into one brand and supports many protocols and technologies, which allows consumers to mix and match the IoT devices they want. openHAB is easy to install, highly customisable and comes with great performance across a wide range of hardware from PCs to Raspberry Pis.



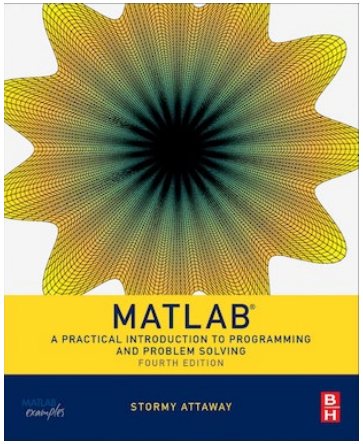
Ubuntu snap is a secure universal Linux application format, and makes applications available as a simple one-click download and install from the Ubuntu Appstore LINK. The snap packaging of openHAB makes it simpler for home automation creators to build, test and distribute their smart home services.
Azul's Zulu Embedded Java Runtime is an appropriate choice for Java applications such as openHAB on embedded devices. It is available for a wide range of hardware and provides optimal

performance on home gateways, PCs or ARM-compatible devices. This also includes the recently launched Raspberry Pi powered Nextcloud Box (Link to other gateways).
Kai Kreuzer, president of the openHAB Foundation: “There is clearly a strong demand for smart home applications and devices. However, this often means a vendor lock-in to one particular ecosystem and makes it difficult to use the devices and services that users wish. Every smart home setup is highly individual and hence the product choices vary. With openHAB we have established a universal smart home integration platform, which is vendor-neutral and fully open towards integration with any existing smart home devices and services out there. Our partnership with Ubuntu and Azul makes it simple to quickly setup openHAB in a secure way, without losing the ability for more technically advanced people to create and fine-tune their own applications.”

Complete article, here

Matlab programming manual cited for 'excellence' as textbook

“Matlab: A Practical Introduction to Programming and Problem Solving, 4th edition” by Stormy C. Attaway has been recognised in the 2017 Textbook & Academic Authors Association Textbook Excellence Award, which recognizes excellence in current textbooks and learning materials. The publisher's description of the text reads, “[It]...has been updated to reflect the functionality of the current version of MATLAB, including the new H2 Graphics system. It features new and revised end-of-chapter exercises, more engineering applications to help the reader learn this software tool in context, and a new section on object-oriented programming in MATLAB.



MATLAB has become the standard software tool for solving scientific and engineering problems due to its powerful built-in functions and its ability to program.
“Assuming no knowledge of programming, this book guides the reader both programming and [using] built-in functions to easily exploit MATLAB's extensive capabilities for tackling engineering problems. The book starts with programming concepts, such as variables, assignments, and selection statements, moves on to loops, and then solves problems using both the programming concept and the power of MATLAB.

Complete article, here

Secure Cortex-M3 flash microcontroller with XiP QuadSPI interface

Maxim Integrated has posted outline details of the MAX32552, a secure flash microcontroller based on an ARM Cortex-M3 core. Maxim's DeepCover embedded security solutions are designed to conceal sensitive data under multiple layers of advanced physical security to provide the most secure key storage possible. The microcontroller is intended to provide an interoperable, secure, and cost-effective solution to build new generations of trusted devices such as mobile chip and pin pads. The MCU is based on a Cortex-M3 processor with 1 MB of embedded flash, 384 kB of system RAM, and 8 kB of battery-backed AES self-encrypted NVSRAM. In addition to a high-performance QSPI interface for secure code execution (XiP: execture in place) and data storage, it includes most of the essential functions of mobile POS terminal including a cryptographic engine, a true random number generator, battery-backed RTC, environmental and tamper detection circuitry, a magnetic stripe reader, a smart card controller with embedded transceiver to directly support 1.8V, 3.3V, and 5V cards, and an integrated secure keypad controller. It also provides a seamless interface to monochrome graphic displays and includes an array of peripherals, SPIs, UARTs, DMA, ADC, and DAC, that add flexibility to control and differentiate the system design.

Complete article, here

TOOLS FOR EMBEDDED SOFTWARE DEVELOPMENT: A LIFE CYCLE PERSPECTIVE

Benjamin M Brosgol, AdaCore

How can we trust the software in a critical embedded system to do what it is supposed to and not do what it is not supposed to? For commercial airborne software the DO-178C standard answers this question in the form of objectives and associated activities that apply to the various software life cycle processes. This guidance is not specific to avionics; DO-178C embodies a collection of sound software engineering principles that can be exploited by any organization developing, verifying, and maintaining high-assurance embedded systems. A key takeaway is to leverage programming languages and automated tools that detect errors early.

Modern embedded systems present a number of challenges to software developers. The software has to be reliable, and in many industries it also has to comply with safety and/or security standards. Couple those demands with market pressures – fielding a profitable product in a timely manner, upgrading it periodically to meet new requirements, and perhaps porting it to new platforms – and a manager is confronted with some difficult technology decisions. Which programming languages, development and verification processes and tools, Quality Assurance methods, etc. should be adopted? These issues are becoming more and more critical as the role of embedded software, and the consequences of defects, have grown dramatically in recent years. Fortunately advances in the state of the art in software technology can offer some solutions.

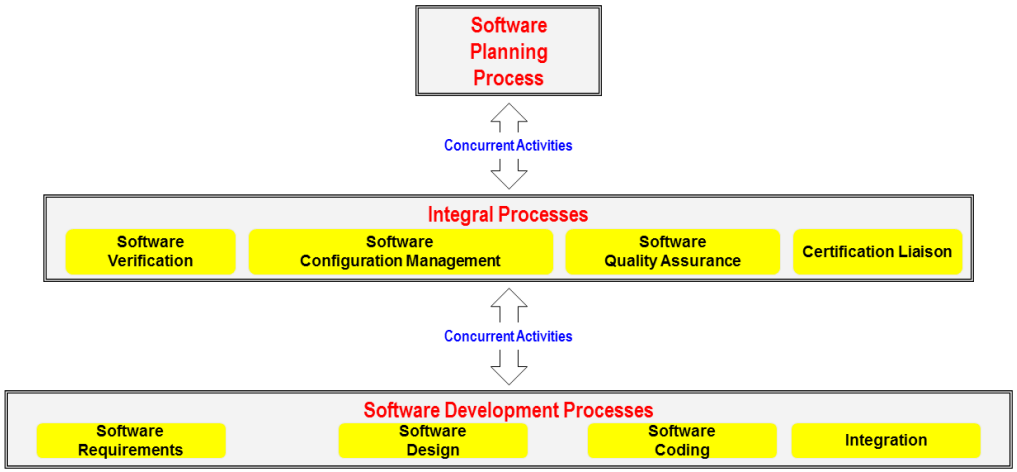


Figure 1. *DO-178C software life cycle model*

THE BIG PICTURE

The various activities that make up software production can be grouped into life-cycle processes; Figure 1 shows how these are categorized in the certification standard *Software Considerations in Airborne Systems and Equipment Certification* (DO-178C/ED-12C).

Although software verification (demonstrating that a process's output is correct) is only one of many life cycle processes, it is the target of the majority of the objectives in DO-178C and is performed concurrently with the software development processes. The aim is to catch errors early and eliminate them before they make it into the final product, as stated in Section 4.4 (Software Life Cycle Environment Planning):

"The goal of error prevention methods is to avoid errors during the software development processes that might contribute to a failure condition. The basic principle is to choose requirements development and design methods, tools, and programming languages that limit the opportunity for introducing errors, and verification methods that ensure that errors introduced are detected."

In this article we'll look at how tool and technology choices during various life cycle processes can help prevent and detect errors and otherwise contribute to reliable and maintainable software, especially at high Design Assurance Levels . DO-178C will be used to set the context, but the discussion applies more generally to the verification of high-assurance systems.

SOFTWARE DESIGN

The software design process takes high-level requirements and produces a software architecture and lower levels of requirements. The programming language plays an important role, especially if it supports "programming in the large" (modularization, separation of specification from implementation, object orientation) and contract-based programming (subprogram pre- and postconditions, which express low-level requirements).

Ada illustrates these properties. Figure 2 shows a generic Buffer package, derived from a high-level requirement for inserting and removing characters in FIFO fashion from fixed-length buffers. The generic package specification provides the interface (the implementation would be defined in a separate module), and the pre- and postcondition contracts reflect the low-level requirements for the various operations. (Contents'Length is the length of the string returned by the Contents function, and Contents'Old is the value of the string on entry to the Insert or Remove procedure.)

```
generic
   Max : Positive;
package Buffer is

   procedure Reset with
      Post => Contents = "";

   procedure Insert(C : Character) with
      Pre  => Contents'Length < Max,
      Post => Contents = Contents'Old & C; -- Insert at tail

   procedure Remove(C : out Character) with
      Pre  => Contents'Length > 0,
      Post => Contents'Old = C & Contents; -- Remove from head

   function Contents return String;

end Buffer;
```

Figure 2. *Ada for software design*

Contracts can be used in several ways to catch errors during code development:

—As input to a static analysis tool using formal methods to attempt to prove that, if the precondition is satisfied and the procedure returns, then the postcondition will be True

—As run-time conditions to be checked (if enabled), with an exception raised on failure

Contracts can also serve as structured and unambiguous comments to the human reader

(if checks are not enabled), which facilitates manual code inspection and review.

The design process can exploit several software methodologies that bring benefits but also raise potential issues.

Object orientation is a powerful technique for structuring a software architecture, with encapsulation and inheritance facilitating system evolution and maintenance. It can be (and has been) used in systems certified at DAL A. Class hierarchies can be represented graphically (UML class diagrams), and skeletal code for module specifications in a variety of languages can be generated by automated tools. However, object orientation can also introduce vulnerabilities; these are addressed in the *Object-Oriented Technology and Related Techniques* supplement (DO-332 / ED-217) to DO-178C. Programming language semantics can address some of these issues; for example Ada can detect instances of improper function overriding, and its rules for contract inheritance and overriding can help enforce the principle that inheritance should only be used for specialization. A project that uses Object Orientation will need to decide how much generality is needed, and to restrict or eliminate features (such as those requiring dynamic memory management) whose usage may be difficult to verify.

Another software methodology that needs to be planned during the design process is model-based development, which is used for real-time control systems in several domains. The graphical representation of the architecture (for example as Simulink and Stateflow models) and the automatic generation of source code can considerably simplify the development processes, especially if potential bugs can be detected at the model level. However, model-based techniques raise some fundamental questions, such as how to ensure that properties at the model level are preserved in the generated code. This issue and others are addressed in the Model-Based Development and Verification supplement (DO-331 / ED-218) to DO-178C.

The author continues by moving to the topic of software coding and integration; the coding and integration phases flesh out the architecture from the low-level requirements, and produce the source and object code and ultimately the executable program.... click for full-article pdf.

Download PDF of Article

Find DO-178C software life cycle model on EETsearch

CONTROLLING THE EMBEDDED SOFTWARE DEVELOPMENT PROCESS

by Sven Erik Knop and Martin Kochloefl, Perforce Software

The need for better control over the entire electronic product lifecycle - from ideation, the development of the initial concept, through to customer deployment and beyond – been never been more important. As well as the sheer growth in the volume of software embedded in today's electronic products, the increased spotlight on security and compliance standards requires greater rigor around intellectual property (IP), including digital assets. In short, more control is needed over the embedded software development process – this article looks at why and how to deal with it.

Add into the mix the demand for shorter, faster and more frequent product release cycles in many industries and it is easy to see why better management around product 'assets' of all kinds, but particularly digital ones, has become more of a challenge, from development to delivery.

Of course, some vertical markets have been experiencing this focus on having visibility and control over digital assets for some time, notably in regulated markets such as medical device, life-sciences and automotive manufacturing. However, with the growth of the IoT, with software being found coupled with advanced electronics in just about every market imaginable, then there are few organizations in the industry no longer touched by the dominance of digital.

Why does it matter? There are two sets of reasons: better management around digital assets helps organizations to do things better, but to also mitigate potential problems. Without effective management over the entire product lifecycle, including those 'soft' elements and not just the hardware, it becomes very difficult to trace problems back to their roots to diagnose and solve them. Also, without a proper, unified view of each stage of a project and its contributors, there is risk of that project going off track. Then there is the need to make sure that all those assets, which are often valuable IP, are not inadvertently exposed to security risks.

Finally, making sure that the records exist to satisfy regulatory or standards requirements really should extend to the digital asset level. For instance, if the full history of the software development processes associated with a project is not readily accessible, and if an auditor or regulator demands to see that information (as does happen), then that can mean deploying people for days, weeks or even months to "dig" back and find it, possibly not completely successfully. Conversely, if those records are tracked along the way, then dealing with regulators and auditors becomes much easier, detracting less from regular work.

A SINGLE SOURCE OF TRUTH

Ideally, organizations need to have complete visibility of the entire product development process, including anything that is software or digital, with a 'single view' across all contributors, providing a documented, traceable 'history' of a project, as well as a view of the current status (who is working on what, where and how).

This may sound ideal, but as many readers will know only too well, many electronic product design processes involve teams working in 'siloes'. For instance, analogue designers are creating binary file assets that do not naturally lend themselves to being part of 'a single source of truth'. Embedded software teams have code, library and object files, often for multiple platforms that all have separate configurations.

Finding a way for these two converging worlds to 'play nice' may sound ambitious, but it is already being achieved by electronic product design firms worldwide and is often referred to as 'a single source of truth', ideally covering digital assets of all kinds (including CAD drawings, prototypes, even draft technical manuals), enabling visibility across all teams and external third parties, all without them having to leave their existing workflows or preferred systems. Once this single source of truth is created, then it becomes simpler to, for instance, hunt down the source of a bug generated during a software development process (realistically, few software projects are without bugs). Or, it becomes easier to trace the point at which the project requirements were not properly understood and there began to be some deviations from those requirements. Another example might be an external auditor wanting to double-check that the processes were followed and requirements fully approved before work commenced.

The idea of a 'single source of truth' also supports the trend towards Component Based Development (CBD), where all the digital components associated with a product are centrally stored and tracked. When this approach is combined with the right metadata, it makes it more simple to locate and re-use these individual pieces of digital IP time and time again, thus reducing wasted time, effort and cost. For instance, since these IP elements will have already gone through testing, there is no need to repeat that process.

The concept of the 'single source of truth' is already well established in other markets, notably enterprise software, where software developers have long relied on version management, delivered via version control systems, as their defacto 'track and trace' process. Version management is a natural part of 'continuous integration' (CI), the development practice popular in the electronics industry whereby developers integrate code and other files into a shared repository several times a day. Each check-in is then verified by an automated build, allowing teams to detect problems early.

The authors continue by expanding on the idea of a 'single source of truth' that also supports the trend towards Component Based Development (CBD), where all the digital components associated with a product are centrally stored and tracked... click for full article pdf

Download PDF of Article

Find Embedded Software Development Process on EETsearch

SIMPLE DISCRETE SE-TO-DIFFERENTIAL PRECISION IN-AMP CIRCUIT

BY CHAU TRAN AND JORDYN ROMBOLA, ANALOG DEVICES

There are many applications where an ADC needs to process a small differential input signal in the presence of a large common-mode signal. Traditional instrumentation amplifiers (in-amps) are not commonly used in these applications, due to their single-ended outputs and limited common-mode range. To take advantage of their high performance and low cost, a simple circuit can be designed which can convert their single-ended output to a differential output, as well as improve their input common-mode range to be suitable for these applications.

There are many low cost in-amps with the bandwidth, DC accuracy, and low power consumption that can meet all of the system requirements. Another advantage of using an in-amp is that users do not have to build their own differential amplifiers, which requires many costly discrete components.

This article presents a simple way to build and optimize the performance of a low cost in-amp, one that is also cost and performance competitive with monolithic instrument amplifiers.

Figure 1 details the proposed precision system design to allow the user to measure differential signals in the presence of a high common-mode voltage. The circuit includes an input buffer, an ADC driver, and a voltage reference. The buffer drives the reference pin of the in-amp and converts the single-ended output to a differential output. There is a very high input common-mode voltage range. It can handle common-mode voltages up to ±270V (with ±15 V power supplies), almost 20 times above and below the power supplies, which is critical for motor control applications. Its inputs are also protected from common-mode or differential mode transients at up to ±500 V.

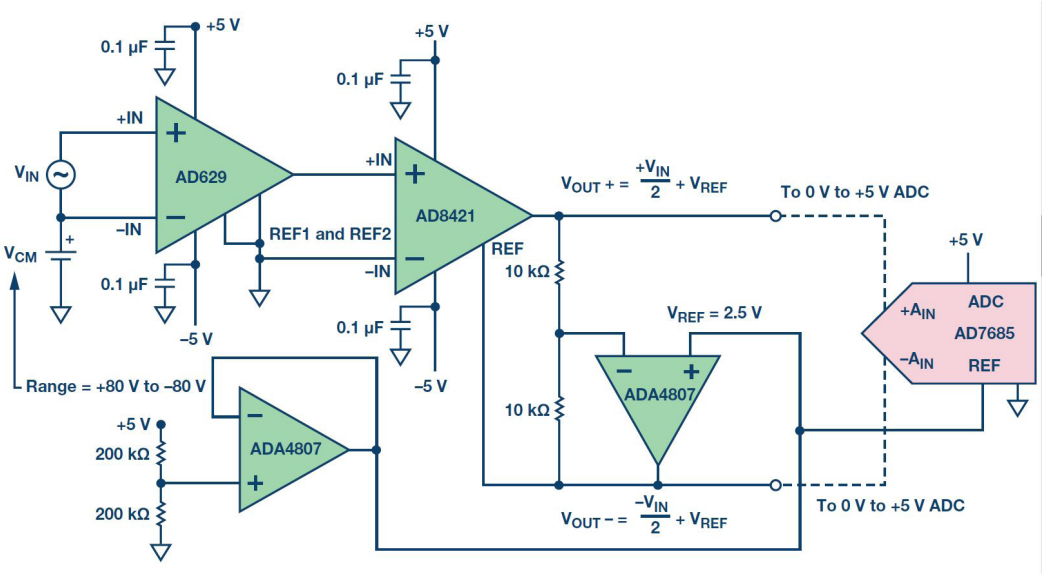


Figure 1. *The single-ended input differential output amplifier.*

For this application, ±5V supplies are used so the input voltage can have a common-mode range of ±80V.

The differential output is defined by the following equation:

$$V_{OUT\_diff} = V_{OUT+} - V_{OUT-} = \text{Gain} \times (V_{IN})$$

The common-mode output is set by the following equation:

$$V_{OUT\_CM} = (V_{OUT+} - V_{OUT-})/2 = V_{REF}$$

The advantage of this circuit is that the dc differential accuracy depends on the AD629 difference amplifier and AD8421 instrumentation amplifier, not on the op amp or the external 10 kΩ resistors. In addition, this circuit takes advantage of the precise control that the in-amp has of its output voltage relative to the reference voltage. Although the

dc performance and resistor matching of the op amp affect the dc common-mode output accuracy, these errors are likely to be rejected by the next device in the signal chain and, therefore, will have little effect on the overall system accuracy.

For the best AC performance, an op amp with a high bandwidth and slew rate is recommended. In this circuit, the choice for op amp is the ADA4807. To avoid parasitic capacitance that can make the ADA4807 unstable, keep the trace lengths from the resistors to the inverting terminal as short as possible. If the use of longer traces is unavoidable, use lower value resistors.

High performance ADCs typically run on single 5 V supplies and have their own reference voltage. This reference voltage is used as the common-mode voltage for the differential output, eliminating the need for a voltage reference. Therefore, the output is ratio-metric to the ADC, meaning any change to the VREF of the ADC does not affect the performance of the system.

The ability of this differential amplifier to reject a common-mode voltage is determined by the ratio match of the AD629 differential amp's internal trimmed resistors. Therefore, it is superior to an in-amp built with discrete amplifiers.

For discrete amplifiers with 0.1% external resistors, the CMR is limited to 54 dB. With integrated precision laser-trimmed resistors, the in-amps allow the system to achieve a CMR of 80 dB or better. These resistors are also manufactured from the same low drift, thin film material, so their ratio match over temperature is excellent.

The ADC can operate on single 5 V supplies with a low impedance 2.5V source on the reference pin. This sets the output to midsupply and raises the common-mode voltage seen at the ADC inputs.

An oscilloscope plot of the output waveforms is shown in Figure 2. Both in-amps are in a gain of 1. V_{IN} is a 1 Vpp 10 kHz sine wave riding on a large common-mode voltage. V_{OUT+} and V_{OUT-} are ±0.5 Vpp sine and cosine waves. V_{OUT_diff} is the differential output voltage of 1 Vpp, which is just V_{IN} with the common mode removed.

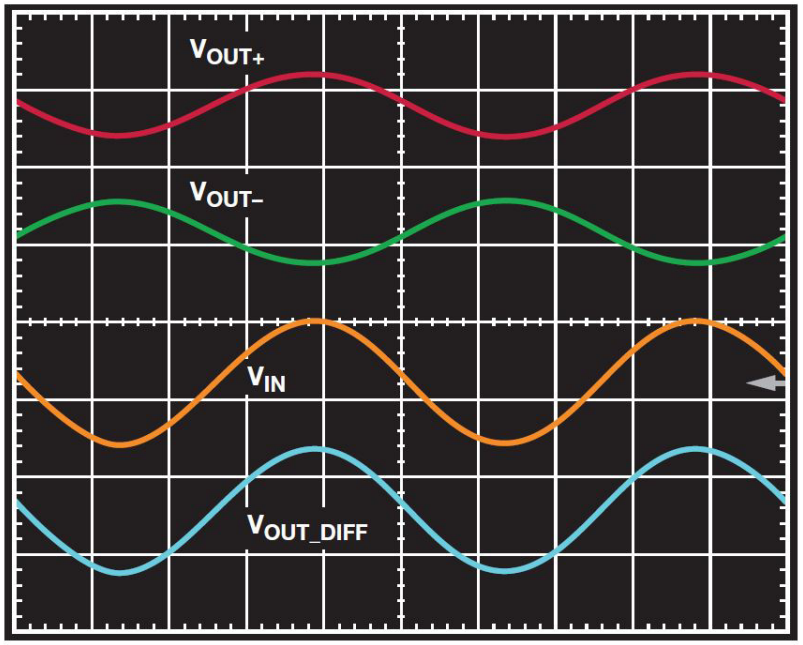


Figure 2. *The performance of the circuit: Top: two complementary outputs, Middle: input voltage with large common mode, Bottom: the differential output.*

Gain = 1 + (9.9 kΩ/RG)

This circuit can also be used in power sensitive applications. With a total quiescent current of 5 mA and a dual 5 V power supply, it consumes about 50 mW, which is 50% less than other solutions with primary ADC drivers (for example, the AD8138 and AD8131 differential driver amplifiers) or discrete amplifiers.

ABOUT THE AUTHORS

Jordyn Rombola *[jordyn.rombola@analog.com] is a product engineer in the Linear and Precision Technology (LPT) Group. She joined Analog Devices in January 2014 after finishing her bachelor's degree in electrical and computer engineering from Worcester Polytechnic Institute (WPI).*

Chau Tran *[chau.tran@analog.com] joined Analog Devices in 1984 and works in the Linear and Precision Technology Group in Wilmington, MA.*

SECURITY & RELIABILITY ARE KEY IN WIRELESS NETWORKS FOR IIOT

by Ross Yu, Linear Technology

The Industrial Internet of Things (IoT) calls for wireless sensing and control nodes to be used in a wide range of applications from factories and industrial process plants to building energy efficiency, smart parking applications and commercial agriculture. In all of these applications, Industrial IoT wireless solutions are expected to operate for many years, often in harsh RF environments and extreme atmospheric conditions.

Unlike consumer applications, where cost is often the most important system attribute, industrial applications typically rate reliability and security at the top of the list. In OnWorld's global survey of industrial wireless sensor network (WSN) users, reliability and security are the two most important concerns cited. This is not surprising if you consider that a company's profitability, the quality and efficiency with which they produce goods, and their worker's safety often rely on these networks. Indeed, Industrial IoT solution providers identified the selection of WSN platform to be pivotal to the success of their wireless Industrial IoT business. This article explains the importance of data reliability and network security in Industrial IoT applications, examines real-life case studies, and discusses key considerations when selecting an Industrial IoT wireless solution.

DATA RELIABILITY IN A WIRELESS SENSOR NETWORK

In an industrial plant or factory, the need for high reliability is well understood since a single missing data point could result in a factory shutdown or safety issues. In the broader set of industrial applications, although the intermittent loss of data packets may be tolerated, extended periods of communications outage are not acceptable. Even a 1% data failure rate is too high, since it translates to 3.65 days per year of unscheduled downtime. Industrial IoT solution providers have noted that one half-day of communications outage would result in irate customers and the cost of an on-site technician visit. If a second such outage were to occur, there is a high likelihood of losing their customer. Therefore, industrial applications demand >99.999% data reliability to overcome the wide variety of RF problems they will likely experience over years of operation.

In order for a wireless network to run virtually maintenance-free for many years, it must be architected with multiple means of overcoming problems. One general principle in designing a network for reliability is redundancy, where failover mechanisms for likely problems enable systems to recover without data loss. In a wireless sensor network, there are two basic opportunities to harness this redundancy. First is the concept of spatial redundancy, where every wireless node has at least two other nodes with which it can communicate, and a routing scheme that allows data to be relayed to either node, but still reach the intended final destination. A properly formed mesh network—one in which every node can communicate with two or more adjacent nodes—enjoys higher reliability than a point-to-point network by automatically sending data on an alternate path if the first path is unavailable.

The second level of redundancy can be achieved by using multiple channels available in the RF spectrum. The concept of channel hopping ensures that pairs of nodes can change channels on every transmission, thereby averting temporary issues with any given channel in the ever changing and harsh RF environment typical of industrial applications. Within the IEEE 802.15.4 2.4GHz standard, there are fifteen spread spectrum channels available for hopping, affording channel hopping systems much more resilience than non-hopping (single channel) systems. There are several wireless mesh networking stan-

dards that include this dual spatial and channel redundancy known as Time Slotted Channel Hopping (TSCH), including IEC62591 (WirelessHART) and the forthcoming IETF 6TiSCH standard. These mesh networking standards, which utilize radios in the globally available unlicensed 2.4 GHz spectrum, evolved out of work by Linear Technology's Dust Networks group, which pioneered the use of TSCH protocols on low power, resource constrained devices starting in 2002 with SmartMesh products.
While TSCH is an essential building block for data reliability in harsh RF environments, the creation and maintenance of the mesh network is key for continuous, problem-free multi-year operation. Over its lifetime, an industrial wireless network will be subject to vastly different RF challenges and data transmission requirements. Therefore, the final ingredient required for wire-like reliability is intelligent network management software that dynamically optimizes the network topology, continuously monitoring link quality to maximize throughput despite interference or changes to the RF environment.

TSCH NETWORK IN A SEMICONDUCTOR WAFER FABRICATION FACILITY

In the first case study, Linear Technology's TSCH-based SmartMesh IP has been deployed at its wafer fabrication (fab) facility in Silicon Valley to monitor pressure for hundreds of specialty gas cylinders used in the various etching and cleaning stages of wafer fabrication. Previously, each cylinder's pressure was checked manually three times a day, absorbing a total of 4 hours of manual work per day. A SmartMesh IP network was deployed to automate the measurements and send the readings directly to the facility's control centre software. In the gas bunker, 32 wireless nodes were deployed with each node measuring a pair of cylinders for tank pressure and regulated pressure. The network generates an aggregate of 3 kilobits per second of sensor data. RF conditions in the fab are typical of an industrial environment, with wireless nodes surrounded by metal, concrete and with work crew and equipment moving in the area throughout the day. The network has been in operation over 83 days continuously, has sent over 18.8 gigabits of data and has experienced over "7 nine"s (>99.99999%) reliability.

Number of Wireless Nodes	32 (each with 4 sensors generating data)
Mesh Network Depth	4 Hops from Furthest Node to Gateway
Data Generation Rate of Entire Network	3kbits per second
Total Data Sent	>18.8 gigabits Over 83 Days
Data Reliability	>99.999996% Data Reliability – Seven Nines of Reliability

Table 1. *Network Statistics - SmartMesh IP network at Linear Technology wafer fab facility*

Figure 1. *Dense metal and concrete - wireless nodes must perform reliably even when located among metal equipment and gas distribution pipes*

***Ross Yu** concludes this article with a further practical example/case study, and sets out the arguments for default application of the highest levels of security in wireless networks... click for full-article pdf*

CHALLENGES AND CHOICES IN IOT SYSTEM EVALUATION AND DEVELOPMENT

by John Jones, Avnet Silica

The Internet of Things offers a technological revolution that can deliver higher efficiencies and enhanced productivity in existing equipment infrastructure. More than this, building on cloud-based IT technologies and capabilities that are becoming increasingly powerful, the implementation of real-time data analysis can enable autonomous decision-making and create the potential for new services and revenue streams for companies.

However, it can be a complicated, fragmented and potentially fraught transformation for many, especially those in operating in industrial sectors. For example, the industrial world comes with decades of legacy equipment and existing infrastructure that cannot easily be replaced quickly or cost effectively. Introducing new embedded hardware and software to connect smart sensor technologies with the cloud and enterprise software, potentially via an Internet gateway in many cases, brings issues of connectivity, interoperability, security and scalability. All of which can present a serious challenge in connecting up previously unconnected systems and devices, especially when dealing with solutions from multiple vendors.

MARKETS AND APPLICATIONS

Today there are widely varying estimates for the IoT market – but to choose one from many, market analyst firm IHS predicts rapid expansion over the next few years, resulting in an installed base of more than 50 billion Internet-connected devices by 2025 with new connected device shipments predicted to be more than 12 billion per year. A large share of the installed base is expected to be in industrial application sectors with approximately 20 billion connected devices deployed across a range of markets including industrial automation, building and home automation, smart metering and in alarm and security products and systems.

This growth is being driven by numerous new applications and capabilities. A classic IoT application is predictive maintenance, where for example manufacturing or operation data is collected via sensors located within or near to equipment and sent into the cloud for real-time data analysis. This enables the ability to accurately diagnose and prevent equipment failure, which can be a significant advantage for manufacturing companies and vital for critical-service infrastructure. Predictive maintenance can provide a significant impact in high-tech manufacturing and smart factories and in what is being called the Industry 4.0 revolution in Germany.

Another key application is track and trace for transport and logistics markets. The installation of low-power narrowband transmitters within vehicles or large assets, in conjunction with data analytics in the cloud, can enable the real-time tracking of shipments, providing improvements in delivery as well as for insurance purposes. It can also deliver the potential to optimize logistics routes or warehouse capacity. Another example is the installation of fire alarms in homes, where the inclusion of connectivity with additional devices such as presence sensors can deliver a higher level of service as well as the potential to offer completely applications and services to end customers.

CHALLENGES AND CONNECTIVITY CHOICES

There are many challenges for companies working to introduce IoT systems and applications. These include: the low-power requirements of edge devices, especially remote devices that will typically be required to operate from small batteries; scalability and the ability to manage potentially thousands or even millions of devices; the vexed issues of security; and interoperability of discrete solutions at different levels of the IoT chain.

There are also many choices to be made in terms of connectivity. Traditional possibilities involve short-range wireless communications usually wireless LAN, Bluetooth Smart (Low Energy profile) or ZigBee from edge devices to a gateway, often wired via Ethernet to the cloud or potentially connected via wireless LAN. Another option is cellular connectivity from the gateway or even from edge devices to send data directly into the cloud, but this brings the penalty of high power messaging that is not always suited to the small-size information packets typically required for IoT data.

However, there exist alternative connectivity options with low-power narrowband messaging provided by LPWAN (Low-Power Wide-Area) network technologies such as LoRaWAN and SIGFOX. Complementing cellular mobile network and short-range wireless, the fundamental concept for LoRaWAN and SIGFOX is that many IoT and machine-to-machine (M2M) edge devices will only need to transmit small amounts of data as well as operating from a small battery. These LPWA technologies enable significantly lower costs and better power consumption characteristics as well as supporting large networks that have many millions of battery-powered edge devices. LoRa offers data rates from 0.3 up to 22 kbps, whereas SIGFOX employs UNB (UltraNarrowBand) technology, which makes it suited to even smaller data sizes, delivering from 10 bps up to 1000 bps. Typical consumption of a SIGFOX modem for example is between 20 and 70 mA and is virtually zero when inactive. This level can enable battery life of years for edge devices, especially with occasional rather than continuous transmission demands. Today, however, network coverage is limited to an extent with SIGFOX networks, for example, being rolled out in major cities, but largely within Western Europe including Benelux, France, Portugal, Spain and the UK.

In addition, there is also a new and emerging LPWA standard: NB-IoT (NarrowBand IoT), which is backed by major telecom operators and equipment vendors worldwide. The technology is part of the GSMA's Mobile IoT Initiative to deliver low-cost and low-power communication for IoT networks using cellular standards. Today, the initiative is perhaps still in its nascent phase, but it offers much promise.

VISIBLE THINGS

To help companies looking to take advantage of the possibilities offered by the IoT, Avnet Silica has assembled all the building blocks necessary to deliver a flexible and comprehensive edge-to-enterprise evaluation and development IoT platform. The platform delivers tested, proven, secure and integrated hardware and embedded software to connect smart sensors and embedded devices via gateway solutions or LPWA networking technologies, right through to the cloud and enterprise software applications. It is designed to be a highly flexible offering that provides customers a menu of different options along the path from edge to enterprise.

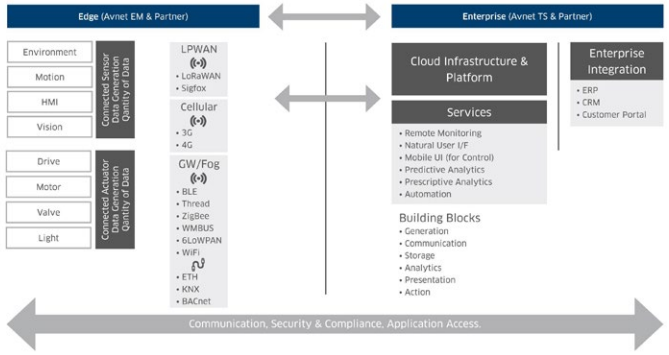


Figure 1. *Scope of the Visible Things platform*

***John Jones**' article continues with a description of the connectivity options in the package, and continues to cloud services and access to enterprise resource... click for full article pdf*

Download PDF of Article

Find IoT development on EETsearch

MEASURING THE DIELECTRIC CHARACTERISTICS OF SUBSTRATES

by Giovanni D'Amore, Keysight Technologies

As RF and microwave systems become more complex, it is increasingly important to understand the dielectric properties of the substrates upon which they are built.
There are two main ways of measuring dielectric properties using microwaves – one based on transmission-reflection (e.g. measuring in a coaxial line, waveguide, and free-space, or with an open-ended coax), and the other on resonance.

The transmission-reflection approach allows swept measurement at any point in an operating frequency range, while the resonance-based methods use a single frequency (or, at most, a few frequency points for different modes). On the other hand, resonators and cavities offer the highest accuracy measurements of real permittivity, and can handle very low loss materials that cannot be measured in other ways.

Looking at the resonance-based approach Keysight Technologies has developed a robust measurement methodology using split-post dielectric resonators (SPDR) for measuring the complex permittivity of dielectric and ferrite substrates and thin films at a single frequency from 1 to 20 GHz. Those components are built with low-loss dielectric materials that make it possible to build resonators with high Q-factors and great thermal stability.

MAKING A MEASUREMENT

To make a measurement with an SPDR, a substrate sample is placed in its cavity and then subjected to an electric field parallel to its surface, as shown on Figure 1.

Samples must have two strictly parallel faces, be thinner than the air gap in the resonator (h_G - see Figure 4), and be large enough to cover the inside of the

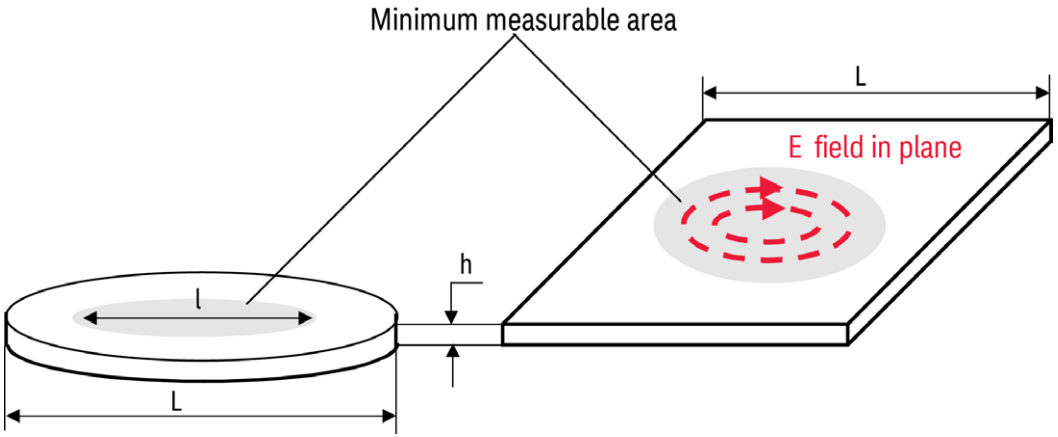


Figure 1. *Sample geometries*

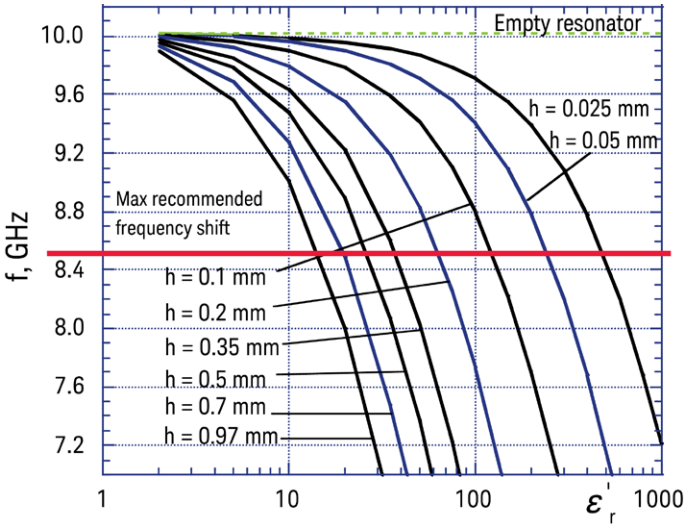


Figure 2. *Typical resonant frequency f versus permittivity εr for a 10 GHz SPDR.*

fixture. Sample thickness also depends on the dielectric constant ε_r of the material, so materials with high dielectric constants should be thinner than those with lesser dielectric constants.

For this fixture, if the permittivity of the sample ε_r is less than 10, the maximum sample thickness (h in Figure 2) must be smaller than the fixture gap thickness h_G, yet thick enough to create a large enough frequency shift to be easily measured. Conversely, if the sample permittivity ε_r is greater than 10, the sample's thickness may have to be reduced to keep the frequency shift within the recommended range. The thickness should also be chosen from Figure 2 to keep the operating frequency above 8.5 GHz.

MEASURING THIN FILMS

The SPDR technique can also be used for measuring thin films. Figure 3 shows typical resonant frequency, f, versus permittivity for a 10 GHz resonator. If a thin film is deposited on a substrate, the resonant frequency shift due to its presence is similar to Figure 3. To work out the frequency shift due to the film, it is necessary to measure the bare substrate first.

The permittivity and loss tangent of thin films deposited on substrates with a diameter of more than 20 mm can be measured (with the same systemic 1 to 2% error) using the same approach as for uniform dielectrics. This means measuring the empty resonator (f_{01},Q_{01}), then the empty resonator with a substrate only (f_S,Q_S), and then, once a film has been deposited, repeating the measurement of the empty resonator (f_{02}, Q_{02}) and the resonator with both the film and substrate (f_2,Q_2).

It is also possible to stack films that are not on a substrate for measurement, because the structure of the field means that any air gaps between the films will not affect the results.

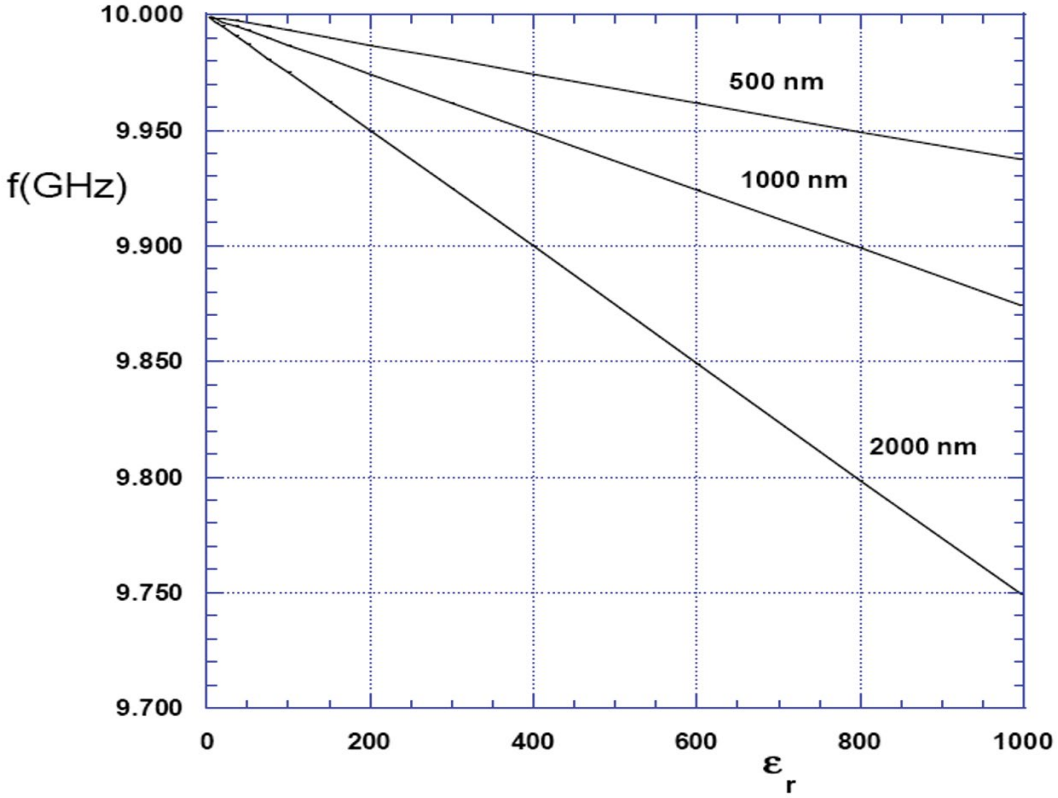
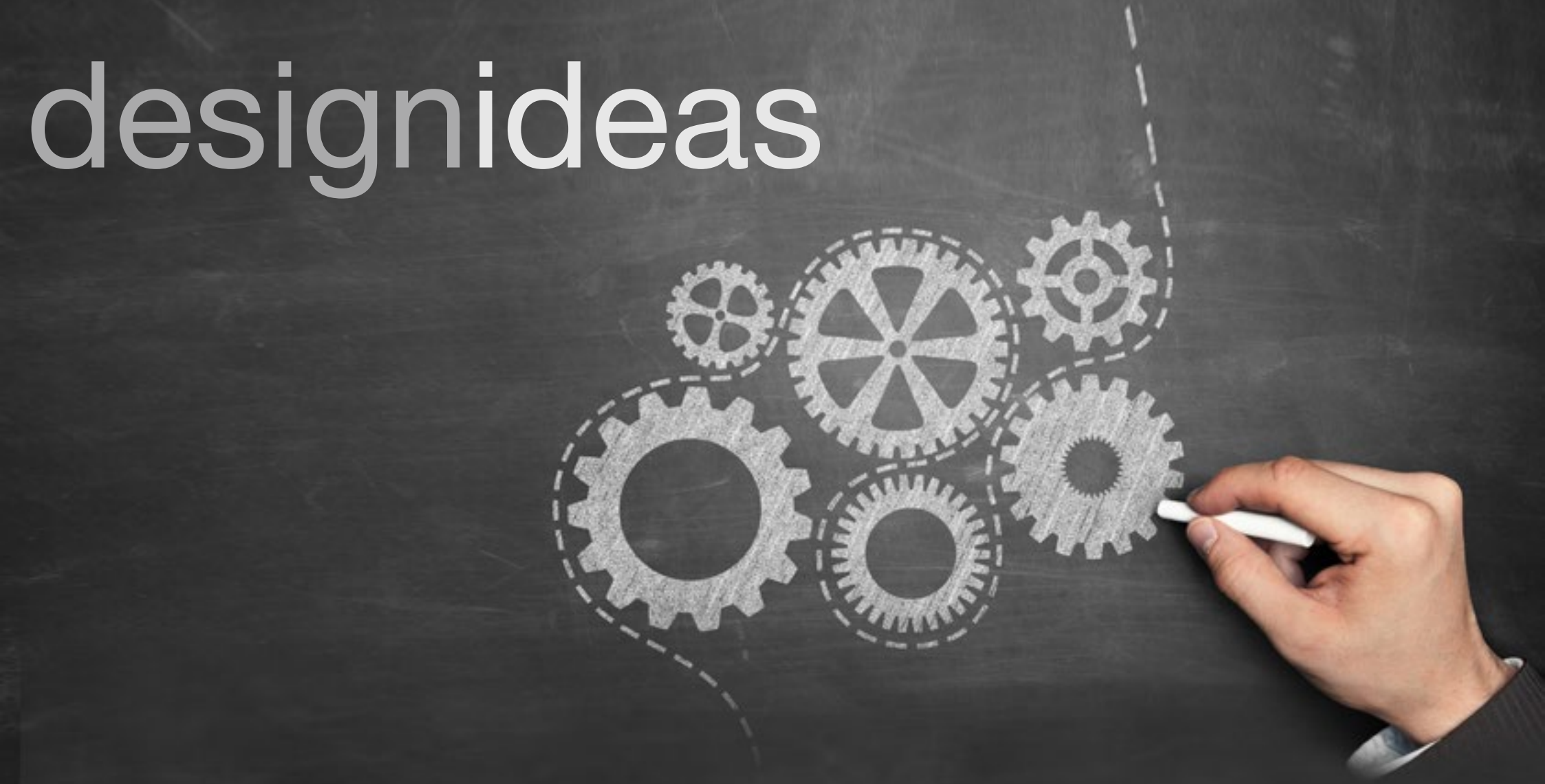


Figure 3. *Resonant frequency versus permittivity of a thin film deposited on artificial substrate with ε_r = 1 for a 10 GHz split-post resonator*

This article continues with a description of the setup of an SPDR measurement, and interpretation of the results... click for full-article pdf.

designideas



- Prototyping your solar powered IoT WLAN temperature & humidity sensor

Prototyping your solar powered IoT WLAN temperature & humidity sensor

By Hans-Günter Kremser, Texas Instruments

According to many studies IoT (Internet of Things) -applications are the future which will generate a multi-million market. May areas such as wearable electronics, white goods, safety and healthcare will be abundantly equipped with IoT devices.

This article describes how to bring sensor data into the cloud, making that data accessible from any place in the world. The whole system proposed here is solar powered. All evaluation boards are available from the Texas Instruments eStore (Link 5, below) and the cloud service is free of charge for a limited number of devices.

It is easy to calculate the energy consumption of any hardware but it is more difficult to configure the battery- and panel-size for a solar powered application. In addition one has to consider the on- and off-times of the equipment. As the light conditions at the final location of the end-equipment are difficult or even impossible to predict, a complete, autonomous WLAN Temperature- and Humidity-Sensor with battery monitoring has been built with TI Evaluation-Boards only.

A 13 x 15 cm, cheap poly-crystalline 2.5W solar panel, a 4.2V Li-Ion mobile phone battery plus the following Evaluation-Boards (EVM) have been used to build this prototype: CC3200EVM, TPL5110EVM, BQ25505EVM, HDC1010EVM and TPS82690EVM.

Depending on the required duty-cycle and light conditions it is possible to measure the real power consumption and this eases the dimensioning of the battery and solar panel. Thanks to the TPL5110 timer IC the quiescent current during the off-time is below 400 nA, according the data sheet. The active power-on-time of the DC/DC converter, sensor IC and WLAN module is dependent on the internet connection, router capabilities, server load, etc.

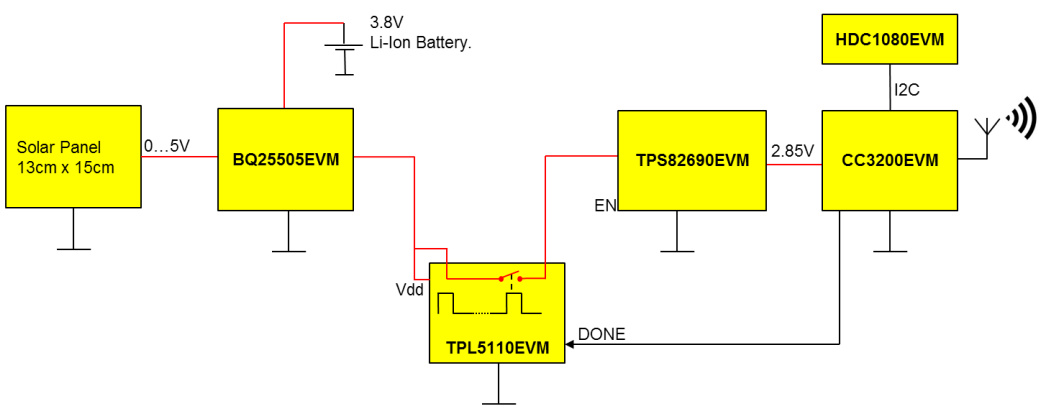


Figure 1. *Block diagram*

SYSTEM OVERVIEW

The whole battery-management including overvoltage protection is controlled by the BQ25505EVM. This one takes the varying voltage provided by the solar panel and charges the Li-Ion battery with the integrated boost-converter starting at a voltage of about 0.3V if the battery is completely discharged. Usually the battery is pre-charged and in that case the energy harvesting starts at about 120 mV.

The most important part for power savings in that system is the TPL5110EVM which is set up to work in timer-mode. The on-board potentiometer allows time intervals between 100 msec and 2h. The power switching MOSFET has been replaced by a more powerful 1.3A transistor because of the WLAN module, which draws most of the power during transmission. The duty-cycle has been set to 10min and the transmission takes about 10s (see Figure 2). The integral over a time period of 10s results in a required energy of 2.13 Wsec while the quiescent energy is calculated based on the data sheet values to 2.06 mWsec. With a fully charged battery with 7.98 Wh the theoretical lifetime is calculated to 114 days:

$$T_{bat} = \frac{Capacity[Ws]}{required\ energy[Ws] \cdot number\ of\ transmission\frac{}{h}} = \frac{7.98Ws \cdot h}{2.13Ws \cdot 5} = 2733h$$

This shows that the selected battery is far too big because we expect the battery to be charged during the day. Under ideal conditions the system is powered by the battery during darkness and it is charged during day light. But this could be less than 4 hours in winter time in Munich. Assuming an outdoor sunlight power of 1 kW per m² [1] and an estimated efficiency of 15% the power of the solar panel can be calculated to approximately 150W x (0.15m x 0.13m) = 2.9W which almost matches with the specified 2.5W of the panel used.

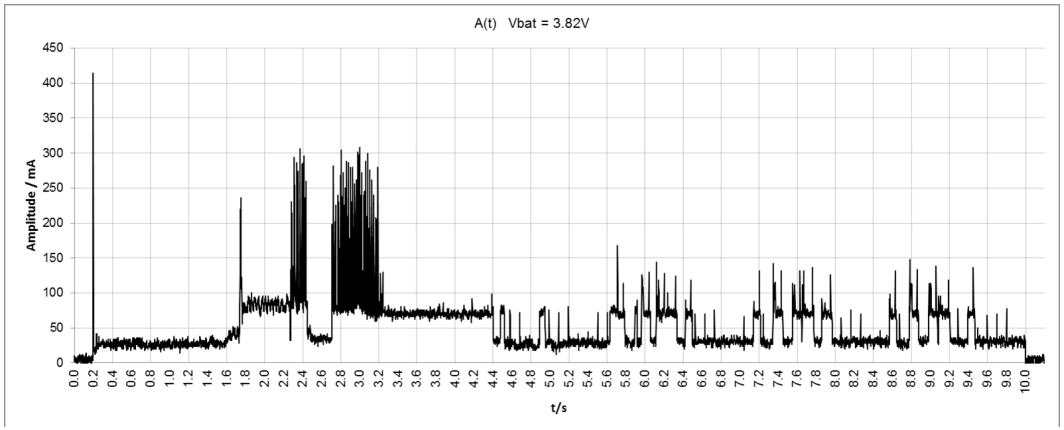


Figure 2. *Power consumption for one transmission cycle*

The TPS82690EVM is a simple buck converter power module to generate the regulated 2.85V out of the variable battery voltage for the wireless LAN module CC3200EVM.

The temperature is measured with an accuracy of typical ±0.2% and the humidity is measured with an accuracy of typical 2% with the HDC1080EVM. This EVM is connected to the CC3200EVM via an I²C interface and also powered by the WLAN module.

A battery monitor has been implemented with a high impedance resistor divider directly connected to the battery and the voltage is measured with the integrated ADC of the CC3200.

The software has been written with the Energia Development Platform and all measured parameters such as temperature, humidity and battery-voltage are sent into the cloud onto www.m2x.att.com once the CC3200 is connected to a WiFi network. Many other cloud services are available [6]. Example software can be found at [2] and [3] and the whole source code can be found at [4].

CONCLUSION

A complete solar powered IoT application can be built simply by connecting some evaluation-boards plus a few external components. As shown in Figure 3 the battery voltage is quite constant over a time period of 30 days and the battery is almost fully charged. A declining curve indicates that the battery will be dis-charged and the duty cycle needs to be reduced.

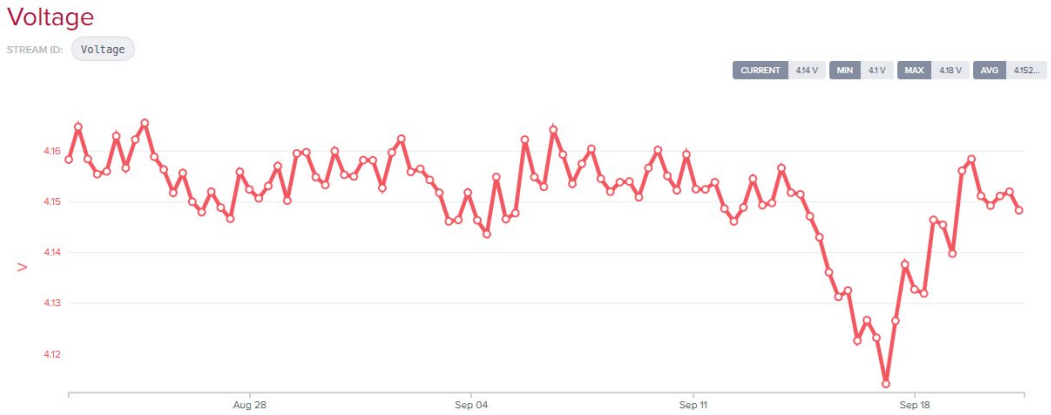


Figure 3. *Battery Voltage over a time period of 1 month*

ABOUT THE AUTHOR

After studying communications engineering in Cologne, Hans-Guenter Kremser worked for several years as a development engineer and in various semiconductor manufacturers as an FAE. Today he works as a Principal-FAE (Field Application Engineer) for analogue products at Texas Instruments.

References

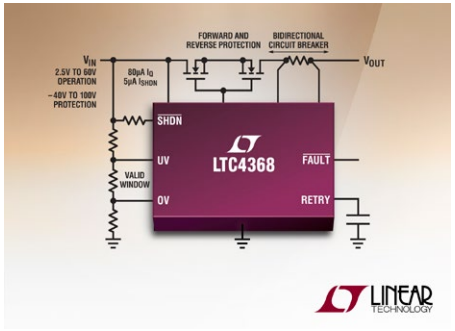
1. https://de.wikipedia.org/wiki/Sonnenenergie
2. http://processors.wiki.ti.com/index.php/CC3200_DEMOS#AT.26T_M2X
3. http://energia.nu/pin-maps/guide_cc3200launchpad/
4. https://e2e.ti.com/support/wireless_connectivity/simplelink_wifi_cc31xx_cc32xx/f/968/t/543241
5. http://www.ti.com/ww/en/internet_of_things/iot-cloudsolution.html

productroundup

productroundup

Bidirectional electronic circuit breaker

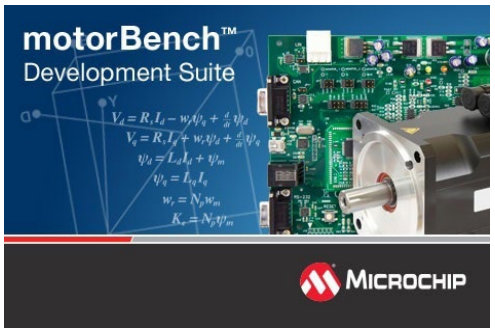
LTC4368 is a circuit protection controller ensuring safe voltage and current levels for 2.5V to 60V electronics in battery-powered automotive, industrial and portable systems. It replaces fuses, transient voltage suppressors and discrete circuitry, enabling a compact and comprehensive solution for shielding electronics from damaging overcurrent and over-, under- and reverse-voltage conditions. The LTC4368 controls back-to-back N-channel MOSFETs to provide a low loss current path during normal operation, turning them off for overcurrent faults in the forward or reverse direction.



Complete article, here

Motor-control tool suite features auto-tuning

Microchip has released an advanced motor-control software plug-in for the MPLAB X integrated development environment (IDE) with auto-tuning and self-commissioning capability. The free plug-in motorBench Development Suite comes with an initial board and motor GUI-based tool that measures critical motor parameters and auto-tunes control algorithm gains. Within the system, software generates editable MPLAB X IDE project code for Microchip's dsPIC33EP DSCs (digital signal controllers), for permanent magnet synchronous motor development.



Complete article, here

Check out LoRa connectivity on STM32 eval boards

Two prototype boards available from STMicroelectronics enable evaluating the LoRaWAN and other Low-Power Wide Area Network (LPWAN) technologies including 6LoWPAN. The boards are based on the smallest and lowest-power LoRaWAN modules that exist on the market today, with a footprint not larger than 13 x 12 mm and power consumption in the range of 1.2 µA in standby mode. The B-L072Z-LRWAN1 STM32 LoRa Discovery kit ($46.50) builds on the all-in-one open module from Murata that integrates a STM32L072CZ microcontroller and Semtech SX1276 transceivers.

Complete article, here

Sub-1-mΩ, 40V/45V N-ch power MOSFET

Toshiba Electronics has expanded its U-MOS IX-H series of low-voltage N-channel power MOSFETs; nine 40V and five 45V devices are intended for industrial and consumer applications, including high-efficiency DC-DC converters, high-efficiency AC-DC converters, power supplies and motor drives. They use Toshiba's low-voltage trench structure U-MOS IX-H process to combine minimum on-resistance with low output charge. Depending on the device, maximum RDS(ON) (@VGS=10V) ranges from 0.80 mΩ to 7.5 mΩ.

Complete article, here

productroundup

Microscanner for interactive laser projection

Transforming any surface into a virtual user interface, Bosch Sensortec's BML050 is an optical MEMS based scanner that promises improved image quality and focus-free projection, creating flexible and intuitive virtual user interfaces. With the BML050, a precise on-demand UI can be created. The BML050 is offered for embedded projectors and augmented reality applications such as games, infotainment and in-car head-up displays. The scanner includes two tiny MEMS mirrors to project an RGB colour laser onto any surface to create a projected image.

Complete article, here

SPICE library for inductors, with parasitics and saturation

Schurter is making available sophisticated simulation models for its entire range of magnetic chokes (compensated and linear types) taking into account magnetic saturation, parasitic effects and thermally induced deratings, which requires more complex simulation models of the individual components and accordingly leads to more accurate simulation results. Detailed SPICE simulation models of current compensated or linear chokes include damping curves: SPICE models as well as mechanical CAD models are available for all Schurter's chokes.

Complete article, here

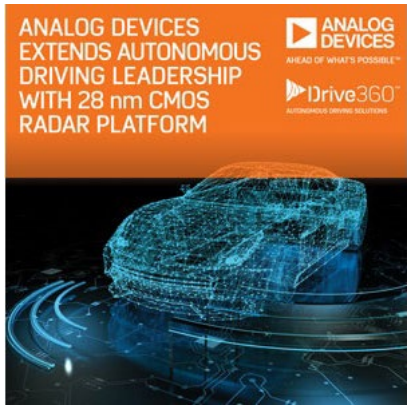
Pico's USB scope software now decodes CAN FD

Pico Technology, maker of PC oscilloscopes and data loggers, has added CAN FD decoding to its PicoScope 6 software. This software, available free of charge for all PicoScope oscilloscopes, delivers features such as serial decoding, channel math, mask limit testing and spectrum analysis, while maintaining a clear, uncluttered display with easy-to-use controls. Serial decoding allows the user to see the the decoded data on the same timebase as the analogue waveforms. Bit fields within frames are colour-code for easier identification, with errors highlighted in red.

Complete article, here

Automotive radar chips in 28nm CMOS

Analog Devices' Drive360 28nm CMOS RADAR technology platform is a development of its ADAS (Advanced Driver Assistance Systems), MEMS, and RADAR technology portfolio. ADI says it is the first to offer automotive RADAR technology based on an advanced 28nm CMOS process, with higher levels of RF performance to advanced safety and autonomous driving applications. This performance, ADI adds, exceeds current best-in-class SiGe (silicon-germanium technology) implementations and will create radars that see smaller objects further away.



Complete article, here

productroundup

8-bit PIC MCU comes with Memory Access Partition

Microchip's PIC16F15386 family is the company's "most powerful launching point" into the 8-bit PIC MCU portfolio. In addition to Microchip's current Core Independent Peripherals (CIPs), this family includes a high-accuracy 32 MHz internal oscillator and memory features such as Memory Access Partition (MAP) with bootloader-friendly write-protection to prevent accidental over-write. Device Information Area (DIA) offers protected storage for unique device identification and calibration values. It is the first 8-bit PIC MCU family to offer the 48-pin package, adding more ADC channels and I/Os. The family offers high levels of CIP integration to perform system functions, such as signal generation, motor control, safety monitoring, system communications, and human interface, outside the core while minimising power consumption. The new MCUs offer IDLE and DOZE modes as well as Peripheral Module Disable power-management features.

Complete article, here

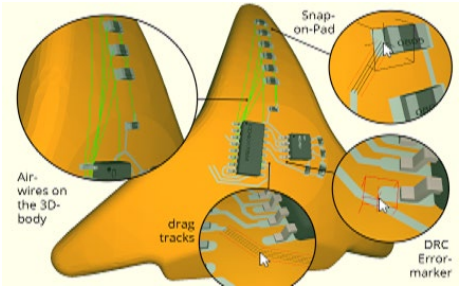
Ultra-compact 86 x 81 mm embedded PC

ADL Embedded Solutions' ultra-compact ADLEPC-1500, at 3.4 x 3.2 in., is a full-feature embedded PC targeted for unmanned, industrial controls, robotics, traffic management and surveillance, with wide voltage and temperature range. It is based on the compact ADLE3800SEC E3800-series Atom SBC with onboard DisplayPort, USB3.0, USB2.0, M.2 KeyB 2242 SATA and two LAN ports. Quad and dual-core E3800 processor options also support DirectX 11, Open GL 4.0, and full HD video playback.

Complete article, here

Free-download software to create 3D-PCB design files

Beta Layout (Eire & Germany) has released the latest version of its TARGET 3001! V18 PCB-POOL software, a free download. This version includes support for prototyping of 3D-MIDs – mechatronic interconnect devices. The underlying PCB-Pool offering is a prototyping service where multiple different PCB designs are amalgamated on to a single panel to reduce costs. Now, the company has added the option to create "3D PCBs". 3D Mechatronic Integrated Devices are three-dimensional bodies with integrated circuit structures. A metallized thermoplastic part (MID) replaces the PCB.



Complete article, here

CAD/CAM-software enables browser-hosted PCB design optimization

EasyLogix (Regensburg, Germany), developer of software for circuit board design and PCB quality assurance, has released PCB-Investigator version 8.0. The upgraded version of the CAD/ CAM software developed for review processes during the development of electronic assemblies, can, for the first time, be accessed via a browser interface without the need for local installation. By using the ODB++ data format, PCB-Investigator creates a common database, which documents every change, and is accessible to everyone involved in the development, quality assurance and production process.

Complete article, here

productroundup

Low-cost FPGAs to support 10G traffic

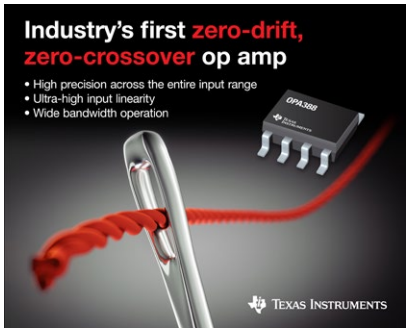
The Intel Cyclone 10 family of FPGAs – Cyclone 10 GX and Cyclone 10 LP – is differentiated by support for 10G transceivers and hard floating point DSP (digital signal processing). It offers doubled performance over the previous generation of Cyclone. The architectural innovation in the implementation of IEEE 754 single-precision hardened floating-point

DSP blocks can enable processing rates up to 134 GFLOPs (giga floating-point operations per second). This is important for engineers needing higher performance using the FPGA for applications such as motion or motor control systems.

Complete article, here

Zero-drift, zero-crossover op amp: precision & linearity

With precision and high input linearity in a single high-performance device, Texas Instruments says it has the first operational amplifier (op amp) to offer both zero-drift and zero-crossover technology. The OPA388 op amp maintains high precision across the entire input range for



test and measurement, medical and safety equipment, and data-acquisition systems. The amp provides high DC precision: low maximum offset voltage of 5 µV, a typical offset voltage drift of 0.005 µV/°C and a maximum input bias current of 700 pA over the extended industrial temperature range of -40°C to 125°C.

Complete article, here

Handheld scope bundles 8 test functions

Rohde & Schwarz' handheld R&S Scope Rider now offers a total of eight instrument functions. Added features include a spectrum analyzer, a frequency meter and a harmonic analyzer for evaluating the quality of power supplies. The fully insulated, handheld instrument meets measurement category CAT IV requirements, and can be used to perform measurements at the source of low-voltage installations up to 600V. With dedicated modes for XY operation, roll mode and mask testing, the Scope Rider comes as a 2- or 4-channel instrument for bandwidths up to 500 MHz.

Complete article, here

3400F ultracapacitors for power hold-over

Distributor Rutronik (Ispringen, Germany) has Nesscap's N60 series, 3.0V/3400F capacitors that increase ratings for power, energy and overall performance while conforming to the industry-standard 60 mm cylindrical form factor. Compared to Nesscap's standard 2.7V 3000F cells, the N60 ultracapacitors deliver 42% greater power density and store

40% more energy. Their cell design and rugged mechanical construction ensure cycle life of 1million cycles as well as a high shock and vibration performance. Performance is guaranteed in a wide temperature range from -40°C to +65°C.

Complete article, here

SECURITY IN THE IOT DEMANDS MORE FOCUS FROM OEMS

BY ANTHONY PELLERIN, DIRECTOR OF TECHNOLOGY, WITEKIO

The trend towards connecting everything to the Internet presents an increased threat to the IT infrastructure; one they can't fix themselves. OEMs need to understand the risks and the security measures available to mitigate them.

In simple terms, what really separated the embedded and enterprise sectors in the past wasn't the type of devices they featured, but the services those devices provided. Not so long ago, deeply embedded devices presented a very small (if any) profile to the wider world, but the IoT will ask those devices to increase that presence, by becoming an active part of the Network and contributing to it in more ways than simply providing data. Rather than just connecting disparate devices together, the Internet of Things (IoT) is about extending the reach of the IT infrastructure.

With that increased profile comes a security threat; if things are easier to detect on a network they will naturally become a target. For OEMs unfamiliar with the kind of security measures routinely found in the IT infrastructure, that may present new challenges. Adding IT-like security to IoT devices isn't simple, but it is becoming more relevant and more important with every new device that gets connected.

WHERE TO START?

An obvious place to start is, perhaps, the technology that will actually connect the devices. Communication interfaces, both wired and wireless, can be an open door (or window) to the criminal element, but they invariably come with a level of protection that should be exercised. Who hasn't heard accounts of Wi-Fi networks being accessed because the password hadn't been changed from the manufacturer's default? It may seem obvious, but it can also be easily overlooked.

Wireless interfaces continue to displace wired alternatives thanks to their convenience. However, that convenience shouldn't extend to making the network open to all devices within range, yet if the security features aren't applied appropriately the result is just that; an unsecured network (Figure 1).

This is true for many wireless protocols but is perhaps more apparent in the IoT due to the widespread use of Personal Area Networks (WPANs). Since their inception, WPANs have suffered from security issues, possibly because the close proximity of the devices implies a secure environment. In fact, the reach of WPANs means anyone in the immediate vicinity, such as a public area or even the building next door, could access a network through an unsecured device.

A good example is Bluetooth; the specification implements four security modes, but any device operating in Mode 1 is not considered to be secure at all, as it doesn't implement any authentication or encryption. Mode 4, on the other hand, is an enforced security mode which uses encrypted key exchange. OEMs should also be aware that paired devices can be either Trusted or Untrusted with respect to accessing the host's services. Trusted devices have full, unrestricted access to all services, while untrusted devices could require further authentication. Applying the right security modes and trust levels will help ensure a more secure network.

Setting an indecipherable password is good practice for managing access to a network, but if the device accessing that network has no

screen, keyboard or user interface with which to enter the password, it needs to be shared securely. It is possible (but not advisable) to share passwords and keys over an established connection without any encryption. This has been demonstrated by various 'unplugged' events in the WPAN arena.

The so-called Man in the Middle attack takes advantage of this, once access to a network is established patterns on the network traffic can be analysed to identify regular exchanges. If these are sent unencrypted it is relatively simple to replace them with instructions that could, for example, initiate an over-the-air update and thereby take control of a device or its services.

LET'S GET PHYSICAL

It should be noted that securing a wireless interface doesn't guarantee security if a physical attack is still possible. Many wired buses, such as CAN, are prone to attack if physical access is available and no security measures have been taken. Some serial interfaces, such as USB Type C, now offer security features such as cryptographic based authentication. Many more, older, protocols will not have considered security when conceived, such 'legacy' protocols are still widely used in embedded devices and for those that aren't connected to a larger network they may present little or no security threat. But the trends towards total connectivity could even make legacy devices a weak link.

One major threat from unauthorised access to a system comes in the form of a software update, introducing functions that simply shouldn't be present. These could be subtle changes, such as pushing data out over a CAN bus, making them difficult to detect. The answer is to protect the system from unauthorised software updates.

One way of doing this is to make the memory where the application code is stored write-protected during the production phase. Many modern MCUs offer this in the form of write-protect fuses for the on-chip Flash memory. Once the Flash has been programmed and the fuses blown, the on-chip Flash can no longer be (re)programmed. Of course, this also makes in-service upgrades impossible, so should be used with care.

For systems based on MCUs using off-chip memory, the solution may be to use some form of secure boot technology. NXP offers one such solution, called High Assurance Boot, or HAB. This is a software library executed from ROM (so it can't be modified) at boot time. This then uses a digital signature to authenticate the code stored in Flash. It uses cryptography based on the Public Key Infrastructure (PKI), which involves signing the firmware using a private key during production and verifying it using a public key at runtime. Successful verification at boot time establishes a root of trust.

HARDWARE TO THE RESCUE?

Many MCU manufacturers, and IP providers such as ARM, now offer hardware-based security features that support and accelerate encryption and authentication. For example, the ARMv8-M architecture offers ARM's TrustZone technology for manufacturers of ARM Cortex-M based microcontrollers. This has the effect of separating a system in to two distinct areas; a trusted zone and an untrusted zone. When this is used in conjunction with a secure operating system and secure boot technology it creates what ARM calls a Trusted Execution Environment. Some licensees have taken this a step further by adding their own security hardware features, so adding security to even the smallest and lowest power IoT nodes should now be possible.

The Internet of Things will increase the footprint of the enterprise infrastructure and that's really where the threat lies. It won't be enough to rely on the Internet's 'backbone' to keep edge nodes secure from attack. The volumes involved with the IoT are staggering, so getting it right will be challenging. But taking the right steps, such as adopting encryption and authentication, will help make the task more manageable.

Anthony Pellerin *is Director of Technology at software systems integrator Witekio, (formerly Adeno Embedded);* *www.witekio.com*

EDN europe

EDN-EUROPE is published 11 times in 2017 by
European Business Press SA,
533 Chaussée de Louvain, 1380 Lasne, Belgium
Tel: +32-2-740 00 50 Fax: +32-2-740 00 59
email: info@eetimes.be.
VAT Registration: BE 461.357.437.
RPM: Nivelles.
It is is free to qualified engineers and managers involved in engineering decisions – see:
http://www.edn-europe.com/subscribe

CONTACTS

PUBLISHER

André Rousselot
+32 27400053
andre.rousselot@eetimes.be

EDITOR-IN-CHIEF

Graham Prophet
+44 7733 457432
edn-editor@eetimes.be

Patrick Mannion
Brand Director EDN Worldwide

european business press

CIRCULATION & FINANCE

Luc Desimpel
luc.desimpel@eetimes.be

ADVERTISING PRODUCTION & REPRINTS

Lydia Gijsegom
lydia.gijsegom@eetimes.be

ART MANAGER

Jean-Paul Speliers

ACCOUNTING

Ricardo Pinto Ferreira

SALES CONTACTS

Europe

France, Spain, Portugal
Daniel Cardon
+33 688 27 06 35
cardon.d@gmail.com

Belgium
Nadia Liefsoens
+32-11-224 397
n.liefsoens@fivemedia.be

UK, Ireland, Israel
Nick Walker
The Netherlands
+44 (0) 1442 864191
nickjwalker@btinternet.com

Germany,
Eastern Europe
Victoria & Norbert Hufmann
+49 911 93 97 64 42
sales@hufmann.info

Switzerland, Austria
Monika Ailinger
+41-41-850 4424
m.ailinger@marcomedia.ch

Italy
Andrea Rancati
+02 70 30 00 88
arancati@rancatinet.it

Scandinavia
Colm Barry & Jeff Draycott
+46-40-41 41 78
jeff.draycott@womp-int.com
colm.barry@telia.com

USA & Canada

West
Todd A. Bria
+1 831 477 2075
tbria@globalmediasales.com

PA, NJ & NY
Jim Lees
+1-610-626 0540
jim@leesmedia.com

East, Midwest, South Central & Canada
Steve Priessman
+1-352 325-4100
steve@stevenpriessman.com

East, Midwest, South Central & Canada
Lesley Harmoning
+1-218.686.6438
lesleyharmoning@gmail.com

Asia

Japan
Keita Sato
+81-3-6824-9386
ksato@mx.itmedia.co.jp