Embedded COMPUTING DESIGN

www.embedded-computing.com

JULY 2007

VOLUME 5 NUMBER 5

Solutions advance to Defend and Protect

SPECIAL

INCLUDED WITH THIS ISSUE:

MOXA

Industrial Embedded Computers

OpenSystems Publishing

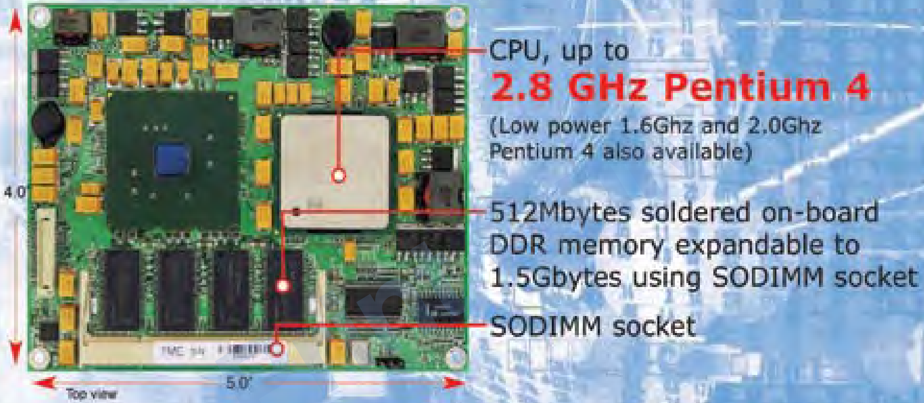
Embedded Computer Solutions For Harsh Environments

-40°C to +85°C Operating Temperature

Five Year Product Availability Guarantee

ECM401

World's Fastest Embedded Computer Module



Features:

- (6) Serial ports
- (4) USB 2.0 ports
- (1) 10/100Base-T
- Compact Flash Socket
- E-IDE supports 2 devices
- Video I/F (1600X1200, 32 Mb)
- AC'97 2.2 Audio
- Less than 5 seconds boot up time
- Intelligent thermal management with independent microcontroller
- Power requirement: +12V @ 3A (2.0Ghz P4, 256MB)
- Over 200,000 hours MTBF

Over 15 years in business of designing and manufacturing embedded computer products for OEMs and System Integrators

We can design your Embedded Computer Board in 30 days.

Time-to-market is very critical to a company's success.
TME has a proven development and manufacturing process that allows new embedded computer products, using TME's core technologies, to be developed in 30 days.
OEMs and System Integrators can now bring their products to the market without compromising cost and features at the expense of time.

Typical Applications

- ▲ Robotic
- ▲ Medical
- ▲ Avionics
- ▲ e-Kiosks
- ▲ Transportation
- ▲ Military/Aerospace
- ▲ Industrial Automation
- ▲ Inventory management
- ▲ Point Of Sale Terminal
- ▲ Test & Measurement

ECM401 Embedded Computer Module provides all functions and features of a high performance computer on a very small Module.

Embedded Computer Designers can easily design an I/O board with proper connectors and form factor that is most suitable for their applications.

The ECM401 supports up to 1.5Gbytes DDR memory, 2.8GHz CPU, with built-in Audio, Video, USB, Network, serial, LPT interfaces and PCI BUS extension capability.

tme

Toronto MicroElectronics Inc.
5149 Bradco Boulevard, Mississauga, ON., Canada L4W 2A6
Tel: (905) 625 - 3203 ~ **Fax:** (905) 625 - 3717
sales@tme-inc.com ~ www.tme-inc.com

www.embedded-computing.com/search

Embedded COMPUTING DESIGN

www.embedded-computing.com VOLUME 5 • NUMBER 5 JULY 2007

COLUMNS

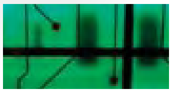
DEPARTMENTS

COVER
Much like Secret Service personnel, electronic devices must identify weaknesses, assess threats, and determine appropriate security measures. Read how new technologies and strategies are evolving to protect today's increasingly vulnerable embedded systems starting on page 12.

Published by: OpenSystems Publishing™

FEATURES

SPECIAL: Security in embedded applications



HARDWARE TECHNOLOGY: Thermal- and power-management techniques for embedded systems

E-CASTS

IMS and IP network
August 15, 2 p.m. EDT

Software-defined radio: what you need to know
August 21, 2 p.m. EDT

www.opensystems-publishing.com/ecast

E-LETTER

July: **www.embedded-computing.com/eletter**
The heat is on
By George Meyer, Celsia Technologies

EVENTS

ESC Boston
September 18-21 • Hynes Convention Center, Boston, MA
www.embedded.com/esc/boston

WEB RESOURCES

Subscribe to the magazine or E-letter:
www.opensystems-publishing.com/subscriptions

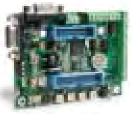
Industry news:
Read: www.embedded-computing.com/news
Submit: www.opensystems-publishing.com/news/submit

Submit new products:
www.opensystems-publishing.com/vendors/submissions/np

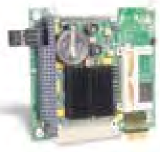
We've Slashed Slow Boot-Up Times

We don't pussyfoot around. Your embedded application needs to come up and execute quickly. Micro/sys CPU boards are optimized to cut through the boot code, which slashes the time from start-up to application readiness for maximum performance over a wide range of hardware platforms.

When you use Micro/sys boards, you gain the value of more than 30 years experience in embedded applications. Our sales team will help you match your boot time requirements with the best board, BIOS, and operating system combination. If you have a tough spec, give us a call.... We welcome the challenge.

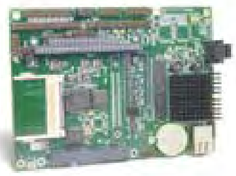


MCB58: Compact microcontroller with CAN, 32 DIO, 4PWM D/A, Temp. Sensor, RTC, 16K Serial EEPROM, 60K Flash, and 4K RAM. *Boots in 160 microseconds.*



SBC1586: Headless, Low-Power PC/104 Pentium with Compact Flash, 4 COM ports, USB, and Ethernet. *Boots in under 4 seconds.*

SBC1625: Low-Power ARM processor with Dual Ethernet, 4 COM ports and 24 Digital I/O on PC/104. *Boots in under 14 seconds to Linux Prompt.*



SBC4495: 486/586 EPIC CPU with GPS, Ethernet, 24 bit I/O, 14 bit A/D and D/A. *Boots in under 4 seconds.*

MICRO/SYS

3730 Park Place, Montrose, CA 91020
Voice (818) 244-4600 Fax (818) 244-4246
info@embeddedsys.com

www.embeddedsys.com

©2006 Micro/sys. All brand and/or product names listed are registered trademarks of their respective owners.

Editor's Choice • Embedded Computing Design • PRODUCTS

www.embedded-computing.com/search

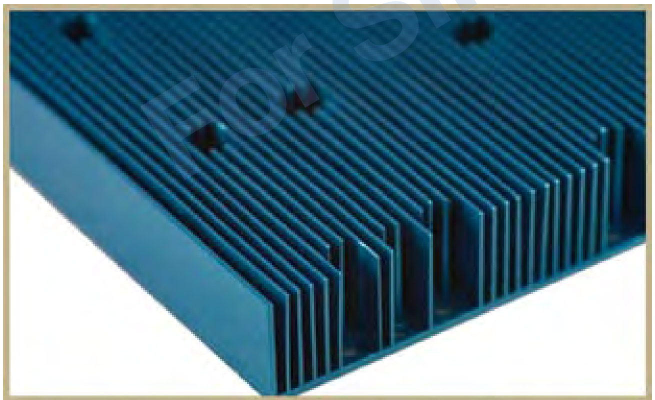
A USB hub you can count on

Industrial USB users are demanding. They need dependable connections that won't be knocked loose and isolation from electrical faults that can disrupt an embedded system.

Though USB has not always been the best choice in many industrial applications, Sealevel Systems, Inc. is focused on making USB the ubiquitous Universal Serial Bus for industrial systems. The company's Seal/O-270U is a seven-port optically isolated USB 1.1/2.0-compatible hub that protects computers from damaging power surges, spikes, and ground loops commonly found in industrial and OEM applications. The Seal/O-270U offers system designers an effective tool for interfacing USB peripherals in virtually any environment. In addition to protection from electrical damage, the Seal/O-270U includes Sealevel's patent-pending SeaLATCH locking USB connector to prevent accidental cable disconnection of both upstream and downstream USB ports.

The Seal/O-270U provides up to 1,500 Vac protection from harmful voltages injected on USB peripheral cabling. Status LEDs on the hub indicate external power, connection to the host, and fault conditions. The hub is housed in a rugged metal enclosure, and each of the seven USB downstream connections provides a full 500 mA of power suitable for all USB peripherals.

Sealevel Systems, Inc. • Seal/O-270U



www.embedded-computing.com/search

Embedded COMPUTING DESIGN
AN OPENSYSTEMS PUBLICATION

Embedded and Test & Analysis Group

- Embedded Computing Design
- Embedded Computing Design E-letter
- Embedded Computing Design Resource Guide
- Industrial Embedded Systems
- Industrial Embedded Systems E-letter
- Industrial Embedded Systems Resource Guide
- PXI, Test & Technology
- PXI, Test & Technology E-letter
- PXI, Test & Technology Resource Guide

Editorial Director Jerry Gipper
jgipper@opensystems-publishing.com
Contributing Editor Don Dingee
Technical Editor Chad Lumsden
clumsden@opensystems-publishing.com
Associate Editor Jennifer Hesse
jhesse@opensystems-publishing.com
Copy Editor Robin DiPerna
European Representative Hermann Strass
hstrass@opensystems-publishing.com
Special Projects Editor Bob Stasonis
Senior Designer Joann Toth
Senior Web Developer Konrad Witte
Graphic Specialist David Diomede
Circulation/Office Manager Phyllis Thompson
subscriptions@opensystems-publishing.com

OpenSystems Publishing

Editorial/Production office:
16872 E. Avenue of the Fountains, Ste 203, Fountain Hills, AZ 85268
Tel: 480-967-5581 ■ Fax: 480-837-6466
Website: www.opensystems-publishing.com

Publishers John Black, Michael Hopper, Wayne Kristoff
Vice President Editorial Rosemary Kristoff

Communications Group

Editorial Director Joe Pavlat
Assistant Managing Editor Anne Fisher
Senior Editor (columns) Terri Thorson
Technology Editor Curt Schwaderer
Associate Editor Jennifer Hesse
European Representative Hermann Strass

Military & Aerospace Group

Group Editorial Director Chris Ciufo
Assistant Editor Sharon Schnakenburg
Senior Editor (columns) Terri Thorson
European Representative Hermann Strass

ISSN: Print 1542-6408, Online 1542-6459

Embedded Computing Design is published 8 times a year by OpenSystems Publishing LLC., 30233 Jefferson Ave., St. Clair Shores, MI 48082.

Subscriptions are free to persons interested in the design or promotion of embedded computing systems. For others inside the US and Canada, subscriptions are $56/year. For 1st class delivery outside the US and Canada, subscriptions are $80/year (advance payment in US funds required).

Canada: Publication agreement number 40048627
Return address: WDS, Station A, PO Box 54, Windsor, ON N9A 615

POSTMASTER: Send address changes to ***Embedded Computing Design***
16872 E. Avenue of the Fountains, Ste 203, Fountain Hills, AZ 85268

Thank embedded for your TiVo

Jerry Gipper

USA Today recently published a list of what it considered were the top 25 inventions in the past 25 years, what the paper referred to as 25 years of "eureka" moments that have changed our lives. While perusing this list, I quickly noticed a trend in these inventions – most involve or are related to embedded computing. It is amazing to see how much our society has become dependent on the feats embedded designers have accomplished in the last quarter-century.

Here's the list of inventions, ranked in order of importance according to *USA Today's* estimations, with some of my comments:

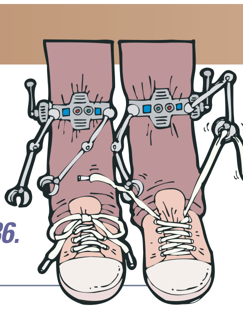
Cell phones: *Star Trek* fans have to be proud. Today's cell phones nearly rival the capabilities of Starfleet communicators. Now if only we could work out the bugs on transporters and replicators.
Laptops: Though laptops themselves are not usually considered embedded, they are full of devices that are intelligent, such as intelligent disk drives, wireless communications, thermal-management systems, and attached peripherals.
BlackBerries: See cell phones. All PDAs can be categorized in this class, but BlackBerries have caught on with business users in particular. They can be addictive and a great tool (most of the time).
Debit cards: Even some debit cards have embedded processors and memory. No cards work without card readers full of embedded electronics that connect them to financial networks for transactions.
Caller ID: Would not be possible without embedded electronics. The next enhancement is to efficiently eliminate unwanted calls.
DVDs: The drives are embedded systems. Embedded technology helps overcome some of the standards issues by enabling one drive to handle many different standards.
Lithium rechargeable batteries: Mobile embedded systems could not exist without this battery technology.
iPods: From tiny Shuffles to video iPods, they are changing the way we manage and listen to music.
Pay at the pump: It seems as if we cannot carry enough cash today (that is, any cash). Innovation at the gas station is on the increase as pumps become more like multipurpose kiosks.
Lettuce in a bag: I couldn't come up with a great connection here, but I'm sure that many embedded systems are involved between the fields and your dinner table.
Digital cameras: Another great device that is changing the way we "capture the moment." Expect much more innovation here in the future. The phone/camera combo still doesn't quite meet expectations as it takes marginal-quality images and lacks flash and zoom capabilities.
Doppler radar: Embedded technology is all over radar systems. Computing power is what makes them so versatile, from weather monitoring and forecasting to traffic control.
Flat-panel TVs: These hit the market hard and have made finding a good TV a cinch because they all provide outstanding pictures. Just think: when was the last time you had to adjust the color? If the products exhibited at the Consumer Electronics Show are any indication, embedded electronics are going to make it possible to do some pretty incredible things with television.
Electronic tolls: Not a big fan of tolls, but at least embedded systems speed up the process.
PowerPoint: How could the marketing folks tell everyone about these great technological advancements without PowerPoint? For better or worse, it has become the business world's main communications tool.
Microwavable popcorn: Wouldn't be microwavable without embedded computing to run the microwave.
High-tech footwear: Putting embedded computers in shoes to measure distance, stress, and gather data enhances the wearing experience. This extends to artificial limbs, which use embedded systems to make them more lifelike.
Online stock trading: Stock trading has long been a stronghold for embedded computing. A lot of embedded computing is going into the background to make trading possible.
Big Bertha golf clubs: Would have been impossible to design without electronics to assist in gathering data on club swings.
Disposable contacts: Made with the aid of machinery controlled by embedded systems.
StairMaster: Electronics make these easier to use and more functional, giving you a variety of workout experiences to meet your conditioning needs.
TiVo: Major embedded systems are used to change the way we view television. How did I survive without one?
Purell: OK, so they got me here, but I know that embedded systems are needed to bottle this stuff.
Home satellite TV: See TiVo. Need both to gain the full home entertainment experience.
Karaoke: Live bands couldn't put up with "I Got You Babe"-belting amateurs, so embedded systems took on the task.

These are all devices that did not exist 25 years ago, which makes me wonder what the next 25 years has in store. It never ceases to amaze me how important embedded computing has become in our lives, and I know the impact is only going to become greater in the future.

Jerry

Jerry Gipper
Editorial Director
jgipper@opensystems-publishing.com

Think any life-changing gadgets should be added to (or axed from) this list? Share your thoughts at ***www.embedded-computing.com/b/?p=36.***



jgipper@opensystems-publishing.com

By Don Dingee

Lean outsourcing may drown supply chain

"Dearly beloved, we are gathered here today to bury our lean outsourcing supply chain partners, drowned at sea …"

That's a sobering thought. The breaking news as I went to deadline was Flextronics' acquisition of Solectron (for the scoop, see www.embedded-computing.com/b/?p=39). On the surface, this seems like a good thing. Flextronics gets bigger, taps into more markets and customers, passes on lower costs … that sound you just heard was the needle screeching across the turntable of my mind.

Trying to achieve even lower costs spells almost certain death for Electronic Manufacturing Services (EMSs) as we know them. They are already at the limits of margin and profitability. There must be something else going on here.

Dig a bit deeper into this acquisition and it becomes apparent that the firm really pulling the levers creating the conditions is Cisco Systems. One company's lean results can quickly turn into another's inventory-filled shoes.

In the ocean, trying to swim

Cisco's lean outsourcing initiative seems to make sense. Working with four EMS providers – Foxconn, Celestica, Jabil Circuit, and Solectron – the idea is to set up tight coordination and move major chunks of inventory from Cisco into the EMS firms over a two-year period.

Angel Mendez, Senior VP of worldwide manufacturing at Cisco Systems, was quoted in a March 2007 interview with *EMSNow* saying, "The long-term benefit of Cisco Lean to our contract manufacturers and suppliers is a decrease in the amount of inventory in the overall supply chain."

But Adam Pick of iSuppli painted a different picture on May 3 in *EMSNow*, remarking that "While Solectron Corp. has increased its revenues for five consecutive quarters, the Milpitas-based EMS provider also has increased its inventory levels for the past five quarters. Since August 2005, Solectron's inventory level has surged by 44 percent. To make things worse, it's expected that Solectron could add an additional $250 to $300 million in inventory as Cisco Systems Inc. shifts stockpiles to the EMS provider in 2007 as part of its Lean initiative."

Now, the motive behind the acquisition is clear. Solectron, drowning from the weight of inventory already in its system with more coming from Cisco, had little choice but to partner with someone like Flextronics just to survive.

I'm not suggesting this is Cisco's fault. They've even admitted that during the transition period to Lean, inventory levels in the supply chain could actually increase until stabilization is reached. It looks like that was the case with Solectron.

Getting lean tough, staying lean tougher

The real issue may be shortcomings in Solectron's inventory processes. Inventory is a funny thing. Too little, and you can't build goods to meet demand, and have to deal with lead times and pricing that's out of control. Too much, and you end up drowning in costs to maintain it.

You then have to resort to fast footwork to slough off inventory – fire sales for excess goods, moving inventory farther back into the supply chain with just-in-time practices and vendor-managed inventory strategies. These steps can make your balance sheet look better – for a while. But if your underlying process keeps building inventory, you've got a problem that just keeps putting the weight back on.

> Inventory is a funny thing. Too little, and you can't build goods to meet demand, and have to deal with lead times and pricing that's out of control. Too much, and you end up drowning in costs to maintain it.

Cisco is trying to create the right model to permanently reduce inventory, creating better processes for real-time demand prediction and communication up and down the supply chain. But they can diet and toss off a lot of inventory very quickly, far too much to handle in some cases. It's not the supply side of the equation that usually gets messed up – it's the demand side, where things and costs pile up quickly.

And Cisco isn't the only big company driving for this model, which doesn't bode well for EMS firms that can't handle the processes needed.

Pushed to the edge

Solectron took a bold step to partner with Flextronics before slipping under the waves. Flextronics is big enough to take on some risk and survive. I'm wondering how many more EMS firms are out there, quietly but desperately treading cold water against the weight of inventory passed from their customers.

How are things at the EMS firms that supply you? This acquisition seems like it could be a tipping point for the EMS industry and the companies that depend on them. I'd like to hear your thoughts and ideas on this and other ongoing developments in embedded technology – e-mail me at ddingee@opensystems-publishing.com.

Embedded gets behind the wheel

By Hermann Strass

An accelerating market

Car electronics is the fastest-growing electronic market segment in Germany. Most microprocessors and supporting electronics in production there are being used in embedded automotive applications. This is evidenced by the increasing number of PCBs made in Germany in 2006 that became baseboards for embedded car electronics. While PCB production lost market share in many parts of Europe (-13.5 percent in Spain), it rose by 7.4 percent in Germany, 4.8 percent in Switzerland, and 4.6 percent in Austria. Industry experts expect moderate growth in Germany this year, partly because production previously outsourced to Asia is shifting back to Germany to achieve better quality and faster results.

Driverless car stays on track

The Golf GTI 53^{+1} (Figure 1) from Volkswagen, Germany, is the latest automobile that can drive autonomously along a known road. This experimental vehicle is being used to test and verify antilock braking, electronic skid prevention, engine drag torque control, and other electronic subsystems in cars. A laser scanner and differential GPS navigation system guide the car, which can follow a prescribed driving pattern on a test track marked with traffic cones at maximum cornering speeds. The digital GPS system measures the car's position with a precision of 2 cm (0.8").

Figure 1

The MicroAutoBox from dSPACE GmbH, Germany, a leading producer of engineering tools for developing and testing mechatronic control systems, automatically controls the power steering, accelerator pedal, and brake booster. A standard VW Golf equipped with a MicroAutoBox acts as an electronic control unit, conducting repetitive tests under normal road conditions. Calculation software from the University of Hamburg determines the ideal line for attaining minimized steering wheel movement and maximum driving speed/acceleration. This software also determines the optimum braking points, maximum cornering speeds, and other parameters. MATLAB/Simulink is used to develop simulated models of driving situations. The Golf GTI 53^{+1} is used to test electronic components in a prescribed driving pattern and does not function like a driving robot that can find its own way.

A compact stand-alone box measuring 220 mm x 225 mm x 95 mm (8.7" x 8.9" x 3.8"), the MicroAutoBox uses an embedded IBM PowerPC 750FX at 800 MHz and runs real-time applications like chassis control, power train, body control, X-by-Wire, and other applications. Its many interfaces include CAN, LIN, FlexRay (optional), serial RS-232/K-line/L-Line and others, analog in and out, and lots of digital channels. This allows for easy integration into a wide variety of cars.

> [The Golf GTI 53^{+1}] can follow a prescribed driving pattern on a test track marked with traffic cones at maximum cornering speeds.

Feels like real gear

Porsche has closed the gap between virtual simulation and the actual drivetrain by developing a shift force simulator, which is controlled by electronics from dSPACE running a Porsche simulation model to provide a realistic gear shift feel. This manual transmission sensation is a brand-specific feature with a high recognition factor intended to differentiate the car from the competition, just like the brand-specific engine sound. Static and dynamic effects must be considered in the simulation model. Determining what the shifting quality will be without having any real parts available is possible at various stages of development.

MATLAB/Simulink is used to develop a simulated Porsche model with virtual transmission. The model runs on a dSPACE DS1104 Controller board using a Freescale Power Architecture MPC8240. This board runs the complex Porsche model software and controls the sensors and actors. An enhanced future system will include visualization and sound.

The shift force simulator evaluates the gear stick position, movement speed, and pedal inputs (clutch, brake, and accelerator) and calculates the reaction forces to produce a realistic feel. Independent of real prototype parts, the shift force simulator can be deployed in many configurations. Even ergonomic aspects, like the driver's position relative to the gear stick, can be adjusted. Porsche uses this simulator to custom develop products for other companies.

Ford is implementing a Ford Fiesta car as a development vehicle for a Micro Hybrid Drive. Ford uses the Fiesta at its research center in Aachen, Germany, to test energy-saving hybrid drives that can reload the battery when braking. A MicroAutoBox loaded with control software (ControlDesk) and application software (CalDesk) also from dSPACE helps achieve optimized results from the Ford Fiesta development car.


AMD
Smarter Choice
Automation
Medical
Network Security

Embedded confidential: keeping electronic systems safe

By Jerry Gipper

Computing technology has evolved from huge, bulky mainframes to the desktop to being embedded in common consumer devices. At the same time, the need for a secure computing environment has risen considerably. So what do we mean when we talk about security in an embedded computing environment? When most people hear the word *security*, it brings to mind images of data encryption, secret codes, and passwords. But security is about much more than that; it is a matter of risk management.

Examine a typical Secret Service security detail. Secret Service personnel assess various threats to their charge, vulnerabilities of their defenses, and actual attacks. Electronic devices resemble this type of security detail in that they face the same concerns. What can harm your cell phone, iPod, HDTV, or automobile? Where is it vulnerable? What do you do when it's attacked? To address these concerns and determine the right level of security for the device, you must estimate total security costs, make trade-offs, analyze potential threats, consider the probability of attack given your particular set of vulnerabilities, and identify effective and appropriate defenses. Then you can implement certain strategies depending on costs and your ability to manage risks.

"Customers don't know what they want in security," says Scott Robertson, product line manager at Analog Devices, Inc. "They are interested but don't quite understand what security is all about. They often jump to the issue of encryption." But simply encrypting everything may not always be the right solution or even practical in some applications. Robertson remarks, "Open processors and open operating systems cannot by definition be secure." From the outset, something has to serve as what he calls the *root of trust* that cannot be altered or compromised.

Security is of paramount importance in embedded electronic systems as more and more personal and financial data is transmitted and stored electronically. Exposures exist anywhere data resides, which is increasingly moving from secure data centers to less secure PCs, cell phones, and PDAs attached to equally vulnerable wireless networks.

Threats itemized

In his book, *Security for Ubiquitous Computing*, John Wiley & Sons, Inc., Frank Stajano uses a well-established taxonomy to subdivide computer security threats into three categories: *confidentiality*, *integrity*, and *availability*. Breaking down security into these elements makes evaluating potential solutions easier and more effective (see Figure 1).

Safeguarding wireless devices

By John Asahina, VP of marketing, Connectivity and Wireless Division, Silex Technology America

Wireless embedded computing devices are actually small computer systems, so they are potentially as vulnerable to security threats as Windows PCs. In fact, several viruses that have already been created specifically target cell phones, which are a type of embedded computing device. Although it is fairly unlikely that a hacker would write a virus for a device that is not a mass-produced product, some major security issues still arise when embedded computing devices are connected to enterprise or small and medium-size businesses' networks using Wireless LAN (WLAN) protocols.

The problem is that wireless embedded computing devices are transmitting radio signals, and nothing can prevent a hacker from intercepting these signals with a wireless laptop. This is a particularly crucial issue because these devices often transmit sensitive data. For example, an embedded computing device connected to a medical instrument could be sending confidential patient information to a server. To prevent a hacker from "sniffing" this information from a wireless laptop, the device must encrypt the information. The hacker can still capture the radio signals, but they will appear as garbage unless the necessary decryption key is available.

WLAN networks also use authentication services to ensure unauthorized users cannot connect to the network. Authentication is critical because a hacker connected to the network could potentially take control of a computer to access databases, delete files, and so on. The ability to monitor the authentication procedure and credentials of a wireless embedded computing device with weak security would allow a hacker to "spoof" that device and gain access to the network.

Not all WLAN security protocols are created equal. In particular, the original Wired Equivalent Privacy (WEP) security has major flaws that enable hackers to easily crack its encryption and authentication. Wi-Fi Protected Access (WPA) is much better, but is more prone to fail from denial of service attacks than other methods. In addition, tools for cracking PreShared Key (PSK) authentication are now readily available. The best security today is WPA2 with one of the 802.1X authentication protocols (for example, EAP-TLS or PEAP; PSK is not sufficient) now widely used on enterprise networks.

The single most important requirement for a wireless embedded computing device's security is compatibility with whichever type of security is used on the network. Most large networks have a standard for WLAN security, so the network manager may not even allow noncompliant devices to be used. This is because network security is only as strong as its weakest link. For example, if a WEP device is added to a WPA2 network, a hacker could easily crack the WEP security to gain access to the network.

The bottom line is wireless embedded computing devices should ideally support all major WLAN security methods. Failure to do so could create unnecessary security holes in networks and consequently limit the market potential for these devices.

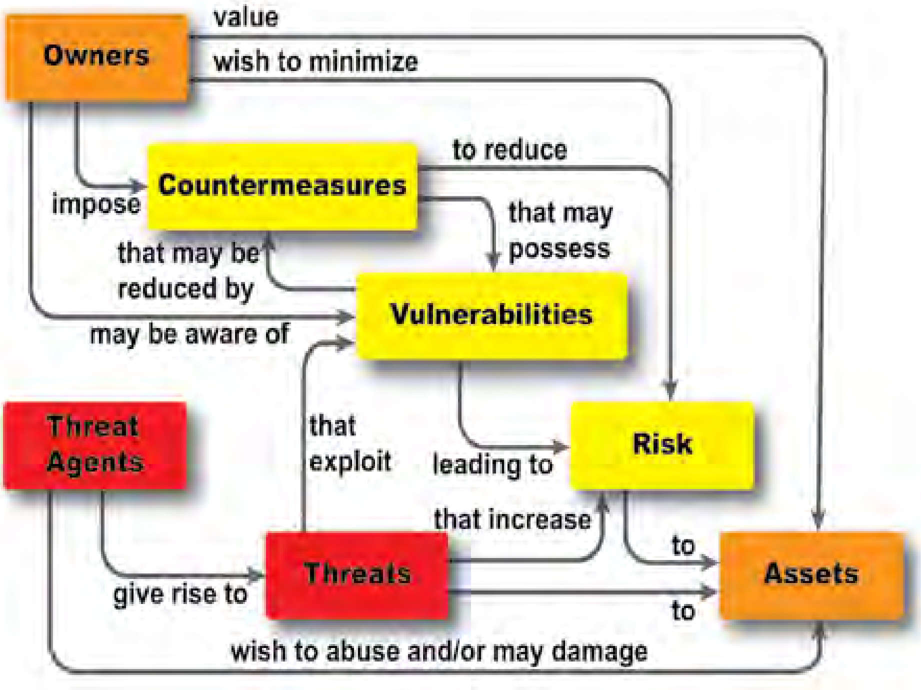


Figure 1

Stajano describes *confidentiality* as the property that is violated whenever information is disclosed to an unauthorized principal, which could be a person or another computing device. *Integrity* is violated whenever the information is altered in an unauthorized way. It may be altered at a host or in transit between devices. *Availability* is the property of a system that always honors any legitimate requests by authorized principals. It is violated when an attacker succeeds in denying service to legitimate users, typically by using up all the available resources.

Encryption adapts to embedded

Computer security is not a new problem. Many of today's security issues have proven solutions rooted in mainframe computer technology, but they must be adapted and applied to embedded computing applications and consumer devices.

Even traditional mainframe companies have undertaken research for embedded applications. Last year, IBM announced a project called SecureBlue to develop a technology the company claimed would greatly increase the security of consumer products, medical devices, defense systems, and digital media. IBM declared the new technology would enable mainframe-inspired security typically only available in data centers and protect the confidentiality and integrity of information on a device through encryption. This would prevent unauthorized use even by an adversary with physical access to or control of the device.

As various digital devices are becoming increasingly widespread and essential, information is becoming more distributed and thus more vulnerable, making strong security all the more important, especially given that devices can be easily lost or stolen. Encryption techniques have long been employed on high-end systems, but the technologies are traditionally expensive and have considerable impact on system performance, making them impractical for consumer products. Today, new technologies are making encryption practical even for low-cost, relatively low-performance electronics.

Seal(s) of approval

Industries such as consumer, medical, government/defense, and digital media need a security seal of approval to address security and assure compliance and compatibility. Several organizations are involved in establishing security recommendations. The National Institute of Standards and Technologies (NIST, http://csrc.nist.gov) has developed the Federal Information Processing Standards 140-2 (FIPS 140-2, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf) for federal departments and agencies to use when implementing cryptographic-based security systems to protect sensitive or valuable data.

Protecting a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. The standard provides four qualitative levels of security intended to cover a wide range of potential applications and environments. FIPS 140-2 is not just for government agencies; it is also used by cable TV companies, the banking industry, and just about anyone who wants security.

"Users encounter multiple levels of security as data gets transferred from point to point," says Mark Moran, senior strategic marketing manager at Xilinx. "This adds a new level of concern. As data gets to the user, both the data and the device must be secure." His customers often want to pay for the level of security they need and prefer designs that can be altered by the developer to handle attacks in various ways depending on the device and the situation.

Another familiar standard is the Common Criteria (CC), an international standard (ISO/IEC 15408) for computer security. CC describes a framework where computer system users denote their security requirements. Vendors then implement and/or make claims about the security attributes of their products, and testing laboratories evaluate the products to ascertain if they meet the claims. In short, CC ensures that the process of specification, implementation, and evaluation of a computer security product is conducted in a rigorous and standard manner.

Unlike FIPS 140-2, CC does not provide a list of mandatory product security requirements or features. CC evaluations are performed on computer security products and systems. The evaluation validates claims made about the target, and, for practical reasons, verifies the target's security features.

The evaluation process also tries to establish how much confidence should be placed in the product's security features through quality assurance processes. Each Evaluation Assurance Level (EAL) corresponds to a package of assurance requirements that covers complete product development with a specified level of strictness. As shown in Table 1, CC lists seven levels, with EAL1 as the most basic (and therefore cheapest to implement and evaluate) and EAL7 as the most stringent (and most expensive). Higher EAL levels do not necessarily mean better security; they only indicate more extensive validation of the claimed security assurance.

> Protecting a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module.

Common Criteria Assurance Level	Process Rigor Required for Product Development
EAL1	Functionally tested
EAL2	Structurally tested
EAL3	Methodically tested and checked
EAL4	Methodically designed, tested, and reviewed
EAL5	Semiformally designed and tested
EAL6	Semiformally verified, designed, and tested
EAL7	Formally verified, designed, and tested

Table 1

The rise of Common Criteria

Common Criteria (CC) is the result of integrating information technology and computer security criteria. In 1983, the United States issued the Trusted Computer Security Evaluation Criteria (TCSEC), which became a standard two years later. Criteria developments in Canada and European Information Technology Security Evaluation Criteria countries followed the original U.S. TCSEC work.

The U.S. Federal Criteria development, an early attempt to combine these other criteria with the TCSEC, eventually led to the current pooling of resources to produce CC, which is based on the infamous Orange Book issued by the DoD. The watchdog for the CC Project is the CC Portal, www.commoncriteriaportal.org, which displays listings of products that have passed CC evaluation and offers development documents available for download.

Even the National Security Agency (NSA) is involved. The NSA operates the National Information Assurance Partnership (NIAP, www.niap-ccevs.org), a federal initiative established to meet the security testing needs of both Information Technology (IT) consumers and producers.

NIAP's long-term objective is to help increase the level of trust consumers have in their information systems and networks through cost-effective security testing, evaluation, and validation programs. In meeting this goal, NIAP seeks to:

- Promote the development and use of evaluated IT products and systems
- Champion the development and use of national and international standards for IT security
- Foster research and development in IT security requirements definition, test methods, tools, techniques, and assurance metrics
- Support a framework for international recognition and acceptance of IT security testing and evaluation results
- Facilitate the development and growth of a commercial security testing industry within the United States

The type of certification achieved varies by application and type of device. It is important to understand these security requirements and apply the right type of certification. And, as Moran points out, the ability to handle changes in protocols and standards should be considered. Security devices that can handle a variety of security protocols and standards allow different data or media streams to be transmitted as the application warrants.

Right to digital protection

One application area related to security that is getting a lot of attention is Digital Rights Management (DRM). Devices have keys that allow them to access server content. Though very specific, access rules are vague on key implementation details. Platforms that manage digital content are different and proprietary.

The Internet has brought DRM to the forefront. DRM is important to content providers because it enables revenue to be generated by content. Without security and DRM, there is no profit.

Content management on the Internet has undergone three waves since its introduction. The first wave was the posting of previously print-only material. When the Internet emerged, everyone started throwing print content onto websites to drive traffic to their sites. This content was loaded for free and distributed for free with very little rights management or protection. The expectation that everything was free soon became the normal mode of operation.

The second wave was digital music. While early attempts to load content on the Internet used the free model of distribution established for print material, music producers began efforts to preserve their rights to the digital content and collect their royalties. These producers engaged the legal process to help restrict and manage content distribution. Today, DRM is designed into most devices that touch music content. Though not entirely effective, DRM has emerged to give the music industry some semblance of protection.

Video is the third wave. Video content providers are studying more effective DRM methods, including streaming video for pay, streaming with ads, and delayed downloads of live or first-run events. Television content producers have perhaps the best shot at actually making some money with their content. Services like YouTube have challenged this to some extent while the DRM battle continues. Time and experience are allowing protection schemes to evolve.

Advanced solutions manage risk

Security solutions in both hardware and software for embedded applications are maturing as the challenge of security has risen to the top of the priority list for system designers. Excellent solutions to the most challenging problems are becoming more practical for embedded devices as they increase in performance and capability. Standards developed by government agencies will influence how consumer devices manage security risks as other new standards address specific needs of these devices. Innovation in security solutions will continue as designers look for solutions that effectively manage risk at an affordable cost point. **ECD**

SPECIAL FEATURE

DRM extends mobile content

By Edo Ganot, Executive VP of business development, Discretix

Digital Rights Management (DRM) is the ultimate mobile content enabler. With robust, interoperable DRM schemes in place, mobile users can enjoy a wide range of benefits, including choice, interoperability, and flexible pricing models.

- ***Choice:*** Handset manufacturers are constantly bringing new and exciting models to market, offering additional features and improved functionality. The average replacement cycle for a mobile device is 18-24 months. Moreover, the adoption of number portability is increasing the frequency with which the mobile user moves between various service providers. Ideally, the mobile user should be able to upgrade a device and freely select a service provider without risking content already purchased and downloaded onto the device.
- ***Interoperability:*** According to Strategy Analytics, by 2010, 75 percent of the mobile phones shipped will include a removable memory expansion slot. The expansion slots used on mobile phones are fully compatible with a broad range of Consumer Electronic (CE) devices, including MP3 players and home and car stereos. Currently, there is no technical barrier limiting music purchased on a mobile phone from being transferred to any other CE device.
- ***Flexible pricing models:*** Several business models are now being used in the world of digital music. Yahoo, Napster, and Real Networks offer an "all you can eat" subscription model, while Apple, Microsoft, and eMusic offer tracks for individual purchase. Other models may be more applicable to the mobile subscriber; for example, purchasing or renting content for a limited time or a limited number of plays. Other options include variations in sound quality, limited number of copies, and the ability to share content among multiple subscribers (superdistribution).

Without a DRM scheme in place, content will be limited to certain formats and devices. For the consumer, this means being locked into one device manufacturer and one service provider. DRM allows the service provider to establish user rights for multiple devices rather than a single mobile phone, thereby eliminating the need for consumers to repurchase the same content. DRM also provides the capability to support multiple pricing models ranging from outright purchase to time-based rental, giving the consumer a broader selection of choices.

Editor's Choice • Embedded Computing Design • PRODUCTS

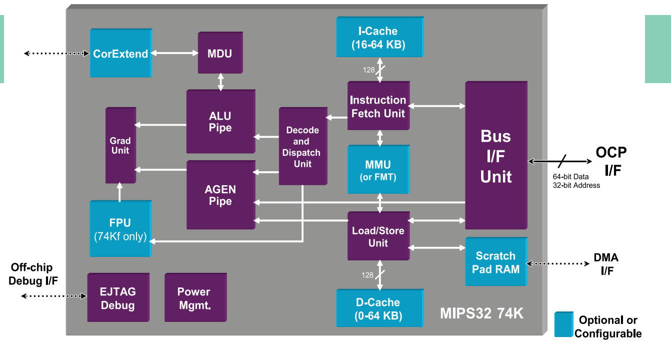
www.embedded-computing.com/search

Performance beyond 1 GHz

It's hard to imagine all the processing power packed into the smallest of today's embedded computing systems. New applications force designers to seek out more from their processors. MIPS Technologies, Inc. has unveiled the MIPS32 74K cores, touted as the industry's first fully synthesizable 32-bit processors to achieve operating frequencies greater than 1 GHz in a 65 nm GP process.

"The rapid convergence of digital devices and the emergence of new consumer applications, PON, WiMAX, and H.264 are driving the demand for superior performance, lower system costs, and low power consumption," said Jack Browne, VP of marketing at MIPS Technologies.

74K Core Architecture

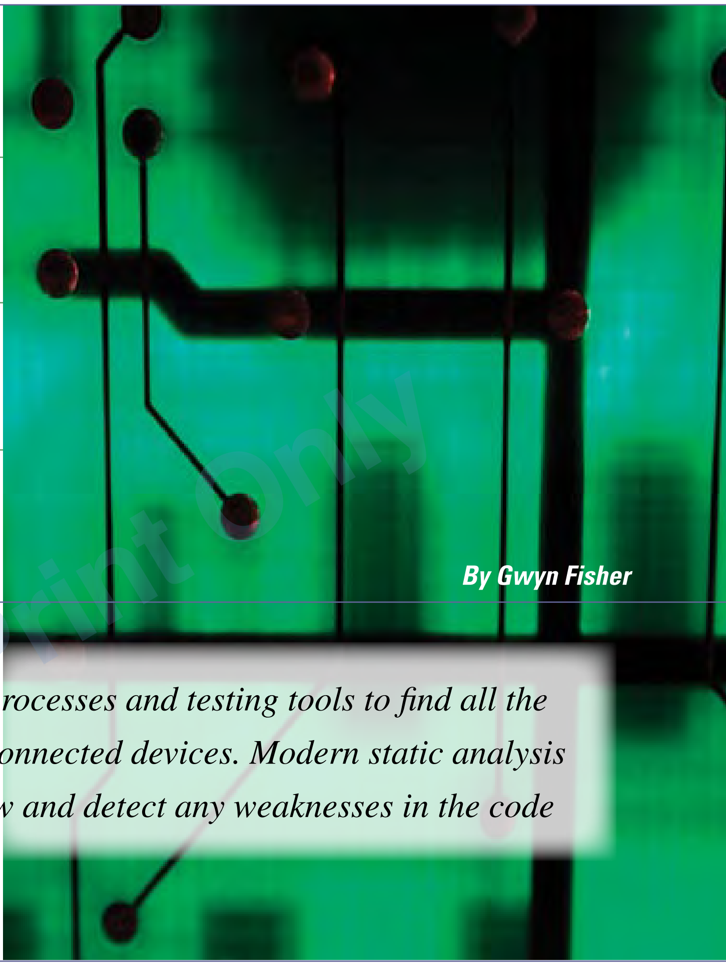


The 74K cores are uniquely designed for high-volume applications throughout the digital home, including HD-DVD, DTV, set-top boxes, DVD players/recorders, broadband access, PON, residential gateways, and VoIP. The microarchitecture features a 17-stage asymmetric limited dual-issue pipeline. Out-of-order instruction dispatch enables execution of multiple instructions more often than an in-order processor, resulting in significantly improved performance and efficiency.

MIPS Technologies, Inc. • MIPS32 74K cores


intel
Leap ahead
Intel. Igniting Innovation.

New threats demand new code analysis tools



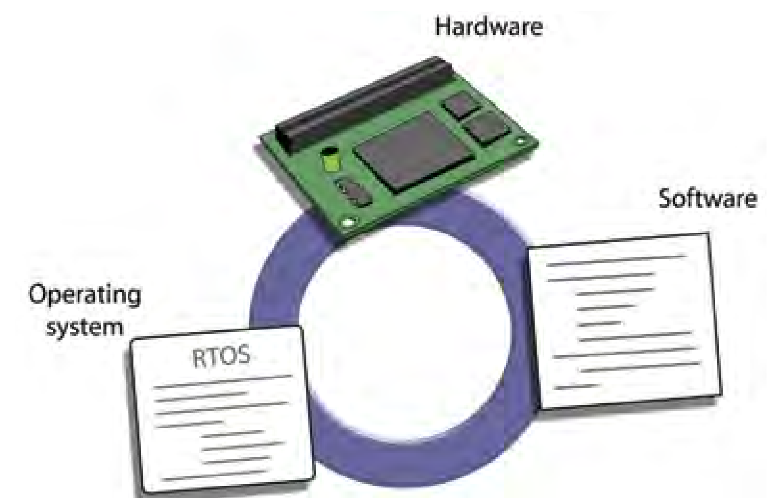
By Gwyn Fisher

Developers cannot depend on old code review processes and testing tools to find all the bugs and potential vulnerabilities in today's connected devices. Modern static analysis tools, however, provide a complete system view and detect any weaknesses in the code that could lead to a malicious attack.

Whether it's a Net-savvy, grocery-ordering super fridge or a wireless-capable, life-saving defibrillator, devices powered by embedded software are not only adding amazing new capabilities, they are also increasingly plugged into the global, public network. But by gaining connectivity and exposing – if not broadcasting – their presence to the world, these devices are becoming enticing targets for nefarious troublemakers.

Just because it's a seemingly innocuous fridge doesn't mean that a black hat with the time, motivation, and misplaced talent won't exploit the latent vulnerabilities an embedded developer unwittingly left in the device's software. The bad guys might turn the Web-enabled appliance into a slave processor or, worse, have the device appear to operate as intended while performing a variety of aggravating or illegal tasks behind the scenes.

Embedded developers have always had to worry about coding defects more than most mainstream developers. Embedded software powers devices that, upon failing or even so much as hiccupping, can cost millions of dollars, ruin a company's reputation, or put lives at risk. But with built-in connectivity becoming common for many devices, embedded developers now have a whole new set of design and coding constraints to add to their already exhaustive checklist. As illustrated in Figure 1, the interaction of embedded device components makes code quality critical.



Point of failure can be a single component or the interaction of components.

Figure 1

What makes it so hard to ensure embedded solutions are secure? The answer is that at least three components – the hardware and its connectivity to the outside world, a real-time or hardened operating system, and the software running on it – must be secure and stable and not crash or enable external exploits when interacting. While each component may be relatively defect-free and resistant to attack, the entire package may not be.

Automated code analysis tools needed

Embedded developers usually rely on their own coding skills, manual code reviews, unit tests, and post-build testing and quality assurance to hunt down software defects. However, with relatively small embedded software solutions consisting of 100,000 lines of code and larger projects containing millions of lines of code, the old code review processes and testing tools can't possibly be expected to find all the bugs and potential vulnerabilities. Neither can developers rely on these processes and tools to uncover the subtle issues that arise from the interplay of the various subsystems that make up a typical modern device.

It's already common practice to rigorously peer review only the main threads of execution within a code base, leaving the quality and security of many ancillary code paths up to the talent of the individual developer. But in the world of online devices, manufacturers can't be confident in their product's lack of vulnerability if the developers haven't applied rigor to every possible code path.

Faced with this type of challenge, it makes sense to look to automated tools for help. In the past, however, source code analysis tools have been very inaccurate, resulting in developers spending additional time combing through lengthy defect reports to determine if the issues the tool reported are even valid. The good news is that code analysis technology has advanced.

Not your father's lint

We've all done it. We've run lint – the open source static analysis tool and its variants – on that new module we're so proud of and watched the ensuing avalanche of warning messages fill our monitors. It's not pretty and, more importantly, not useful. Yet hidden in all that noise is real information – information about errors that developers need to know about. These errors could transform a new device from a state-of-the-art, revenue-generating, must-have product into a financial and public relations disaster that would fuel the development blogs for weeks.

Because lint and its offspring lack fairly basic capabilities and deliver high numbers of false positives, the tools' effectiveness in highlighting real concerns and thus ability to save developers' time is limited. What's worse, the poor-performing lint family tree has sullied the reputation of the entire concept of source code analysis.

Embedded developers need to know that lint does not represent the state of modern static analysis tools. Advances in technology and the thinking behind how the tools work have given rise to more useful, effective solutions. These modern tools are much more than lint with a pretty graphical shell. The best are capable of parsing millions of lines of code and delivering accurate, human-readable results. The tools not only make automated analysis useful, but also will soon make it an essential part of any embedded development process. In other words, modern automated static analysis tools no longer demonstrate their own shortcomings; they now efficiently tell developers what's wrong with the code. Figure 2 shows the new embedded development process with integrated static analysis.

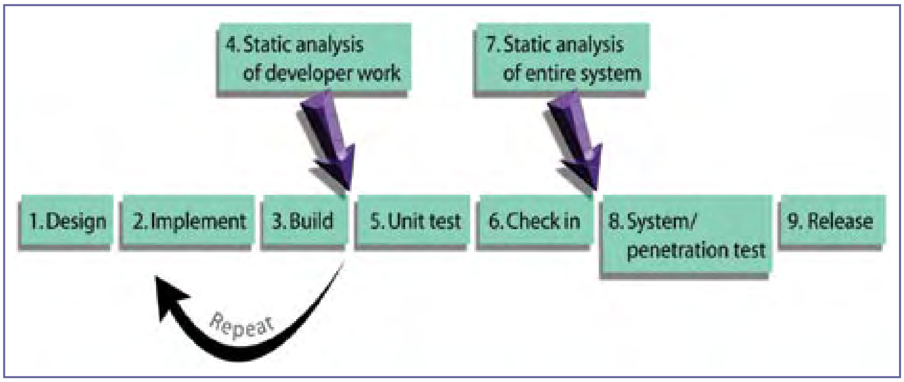


Figure 2

Static analysis solutions deliver more insight

Modern source code analysis tools provide a wide variety of bug and vulnerability detection capabilities. They highlight issues that have a real and measurable impact on the security and quality of an end product, including NULL pointer detection, memory management problems, array bounds violations, concurrency validation and deadlocks, buffer overflows, and tainted data propagation.

Using advanced code path analysis that leverages a complete system view, invalid code paths, inaccessible boundary conditions, and unlikely execution scenarios can all be disqualified from consideration, leaving developers with a scrubbed, viable, and accurate picture of what's actually wrong with the code. Consider the simplified example in Listing 1:

```
void f(int x, int y) {
   int value, *p, *q;
   p = (x & 1) ? NULL : &value;
   if( p ) *p = 1;
   q = p;
   if (y & 1) *q = 1;
}
```

Code path analysis can easily follow the NULL assignment, aliasing, and subsequent invalid dereferencing that occurs here whenever both x and y contain odd values. But split this into several functions over several modules, and though code path analysis can still spot the problem, traditional methods and low functionality analysis tools may fail to spot the dependency, as shown in Listing 2.

```
File: m1.c

static int value;
int* f(int x) {
   return (x & 1) ? NULL : &value;
}

File: m2.c

void g(int* ptr, int y) {
   if (y & 1) *ptr = 1;
}

File: m3.c

int main() {
   g(f(3), 1);
}
```

Now consider that the problems being isolated are not just quality defects of this type but rather subtle security vulnerabilities that could leave the device open to an external attack. Passing maliciously constructed incoming data to an operating

> Modern automated static analysis tools no longer demonstrate their own shortcomings; they now efficiently tell developers what's wrong with the code.

system function that causes stack frame corruption because of invalid assumptions is not something that can necessarily be caught in quality assurance. Since most development organizations cannot emulate a motivated hacker's devious mind, automated code analysis tools provide a safety net that will catch problems current tools and processes fail to uncover.

Steps to safer and secure code

To achieve heightened security, developers first must make a fundamental shift in mentality. They must embrace the assumption that software will be under constant attack from malicious systems and hackers. Having a healthy fear of software being compromised – not because of malfunctions or crashes but as a result of coherent, intensive attacks – should be the norm. Remember, the bad guys aren't necessarily out to crash a device. The talented ones want to hijack the system and turn it into an insecure conduit for illegal pursuits.

Building on this healthy and necessary paranoia, developers should complement manual code reviews and other testing activities with automated source code analysis. There simply is not enough time or available resources to manually validate each possible code execution thread. Only automated tools can map the dependencies, plot the execution paths and data flow, and flag anything that might potentially cause a problem in the software or among the various device components.

The chosen code analysis solution must be accurate, fast, and, most importantly, must work the way each individual developer works. For example, a command line tool isn't going to mesh with an integrated development environment user's process. Likewise an Emacs devotee is going to have a hard time with a Visual Studio plug-in. But with the proper tool in hand, the solution can be fully integrated into the development process, allowing developers to analyze and uncover a significant percentage of vulnerabilities and defects before checking in the code.

As soon as a system is connected, it's under attack. But with a new mindset and a modern tool firmly in place, developers will be ready to deliver safer and more secure code than ever thought possible. **ECD**

Gwyn Fisher *is Klocwork's CTO. Prior to joining Klocwork, Gwyn served as Senior VP of R&D for LumaPath, where he led the creation of LumaPath's Active Integration product suite, and as Senior VP of R&D for Hummingbird Ltd., where he was responsible for more than 350 employees and five product lines within 11 different locations across the United States, Canada, and Europe. In addition to working as a strategy consultant for many international software firms, Gwyn also held positions at PC DOCS, Inc., Fulcrum Technologies, Ltd., TRIP Systems International, and Paralog Ltd. He has a BS in Computer Science from Royal Holloway, University of London in the United Kingdom.*

To learn more, contact Gwyn at:

Klocwork
35 Corporate Drive • Burlington, MA 01803
866-556-2967
gwyn@klocwork.com • www.klocwork.com

Highly efficient cooling in low-airspeed environments

By Barry Dagan

The physical dimensions of embedded applications are continuing to shrink as users attempt to compress as many functions as possible into a given space. Selecting thermal-management products for these power-hungry miniaturized embedded applications has become a highly complex process. Because embedded applications are placed in a wide array of systems and applications, the thermal-management specification process must be based on a worst-case scenario, both in terms of the magnitude of available airspeeds and the direction from which airflows originate. Designers can choose from a handful of heat-sink options to cool devices efficiently in a low-airspeed environment.

Selecting a heat-sink configuration

When selecting heat sinks for embedded applications placed within low-airspeed environments, designers must consider two important conceptual issues: the density of the pin or fin array and the orientation of the fins.

The first factor that should be addressed is the density of the heat sink. When searching for cooling solutions, engineers often look for heat sinks that possess the largest possible surface area. The common belief is that the more surface area a heat sink has, the more powerful it will be. While this may be true for high-airspeed environments, in low-airspeed environments and the natural convection mode, heat sinks with sparse configurations are generally more efficient.

When densely packed pin arrays are placed in low-airspeed environments, friction forces prevent slow-moving air from breaking the stagnant boundary layers around pins. As a result, surrounding airflows cannot flush through the heat sink, leading to poor convective heat transfer. On the other hand, when sparsely configured heat sinks are placed in low-airspeed environments, the large spacing between the pins presents less resistance to slow-moving airstreams and allows them to penetrate the array of pins, resulting in a more efficient convective heat transfer.

The second factor that should be addressed is fin orientation. Choosing an omnidirectional heat sink is essential for low-airspeed environments, specifically in cases where it is impossible to control the location of the heat sink in relation to the fans in the system. An omnidirectional heat sink ensures the orientation of the air source does not affect performance. Conversely, selecting a unidirectional heat sink introduces significant uncertainty as the orientation of the fan has a substantial impact on performance. For example, in a

pin-fin design (see Figure 1), the direction from which the air is approaching does not affect the performance of the heat sink.

Increased demand for highly efficient heat sinks in low-airspeed environments has driven thermal-management vendors to offer new and more efficient heat-sink designs. One of the more innovative heat-sink technologies introduced in recent years is splayed pin-fin heat-sink technology (see Figure 2).

Splayed pin-fin heat sinks contain an array of round pins bent outward in a gradual fashion. The splayed design offers a breakthrough in thermal management as the heat sinks are sparsely configured yet still contain a large surface area. This rare combination stems from the unique splayed design, which takes advantage of generally unused space in the box.

Heat-sink optimization

Cooling power generated in low-airspeed environments is limited, even if the most suitable heat sinks are selected. A common rule of thumb states that a heat sink will be five times more powerful in a high-airspeed environment than if placed in a low-airspeed environment.

Considering the heavy loads of heat being dissipated by today's leading-edge embedded computing systems and the limited space allocated for cooling purposes, the heat-sink specification process has become a challenging task. The following methodologies can help designers improve cooling in low-airspeed environments.

Custom heat sinks

Selecting an off-the-shelf heat sink is always a preferable solution; however, it is not always a feasible one. In cases where

Figure 1

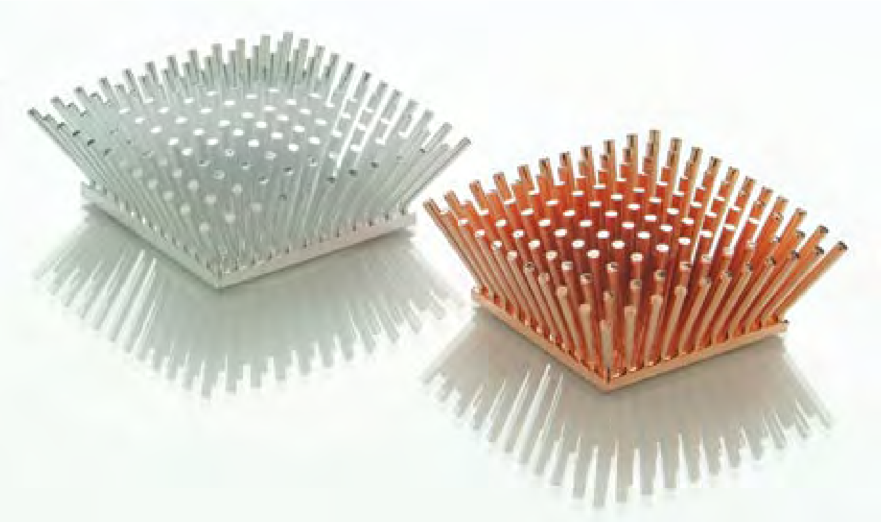


Figure 2

The splayed design offers a break-through in thermal management as the heat sinks are sparsely configured yet still contain a large surface area.

standard heat sinks do not provide the desired thermal resistance, a custom heat sink may be required. Selecting a custom heat sink that fills all the available space around the device achieves a significantly more efficient solution because of two factors: the increase in total surface area and the elimination of air bypass.

It is evident that a larger heat sink will offer more surface area, which in turn will increase the cooling power. However, the low pin density of the heat sink should be maintained and the additional surface area should be generated by a larger footprint or from taller pins.

The second less obvious but highly important factor is that maximizing the size of the heat sink can reduce the bypass air typical to low-airspeed environments. Eliminating possible air bypass forces the moving air to flush through the pins, thus improving the air convection throughout the entire heat sink.

Switching to copper

Copper is a significantly more conductive element than aluminum, and as a result, copper heat sinks provide a cooling premium over identically structured aluminum heat sinks. One of the attractive aspects of switching to copper from aluminum is that additional cooling can be derived without more application space.

Copper heat sinks generally outperform identically structured aluminum heat sinks by 5 to 25 percent. The extent of the cooling premium is a factor of several variables. However, the larger the difference between the footprint of the heat sink and the footprint of the device, the larger the performance boost derived by switching to a copper heat sink. This is because copper's highly conductive nature enables it to spread heat along the heat sink's base much faster than aluminum. An additional advantage of using copper in such instances is the prevention of hot spots at the chip's junction.

To demonstrate how switching to copper can provide a substantial cooling premium, consider the process of cooling a powerful, exposed, silicon flip-chip CPU. A typical high-end CPU has a 0.5" x 0.5" exposed silicon heat source and dissipates between 20 to 50 W. Power levels of this magnitude require a relatively large heat sink. Using copper in this case would enable the heat to spread efficiently across the heat sink. In addition to providing approximately 25 percent more cooling power, copper would prevent excessive peak of the junction temperatures.

Fan sinks

As previously discussed, low-airspeed cooling is limited by nature, and in certain situations, cooling hot devices may be impossible without the aid of additional air sources. One of the simplest ways to approach situations in which heat sinks cannot provide the required cooling power is using fan sinks.

Fan sinks are a combination of a heat sink and a fan, with the fan mounted on top of the device in the impingement-cooling mode. Though fan sinks provide substantial cooling premiums, several factors can limit the adoption of a fan-sink solution. First, a current source is not always available. Cost and mean time between failure also can be prohibitive.

To illustrate the performance advantage of a typical fan sink, compare the thermal resistance of a fan sink to a sparsely configured pin-fin heat sink, both placed in a 200 LFM low-airspeed environment. In this example, the overall dimensions of the heat sink are comparable to the overall dimensions of the fan sink. The footprint of the pin-fin heat sink is 1.5" x 1.5" with a height of 0.6", and the fan sink measures 1.5" x 1.5" x 0.3" with a 1.6" x 1.6" x 0.3" fan on top, resulting in an overall height of 0.55". The thermal resistance of the pin-fin heat sink is 2.2 °C/W, while the thermal resistance of the fan sink is 1.35 °C/W, illustrating the clear advantage of adding fan airflow.

Addressing cooling challenges

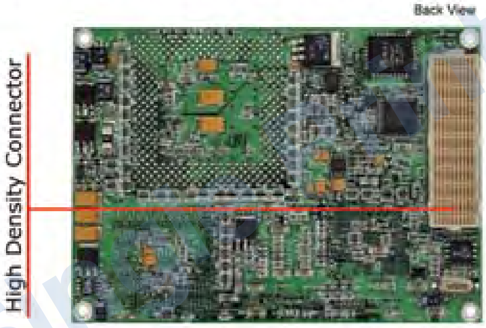
As the devices used in embedded applications continue to heat up, the need for

Embedded Computer Solutions
For Harsh Environments
-40°C to 85°C Operating Temperature
Five year product availability guarantee

Micro-P3
1.26GHz Pentium III
System On Module

$US 275.00/each
(OEM Qty. 900Mhz CPU,
256K L2 cache)

- Choice of ultra low power Tualatin Pentium III / Celeron CPU from 500MHz to 1.26GHz with 256/512 KB L2 cache
- Up to 512MB SDRAM
- Intelligent thermal management with independent microcontroller
- Over 200,000 hours MTBF
- 5V @ 2.2A, 3.3V @ .7A with 900 MHz CPU and 256 MB memory



PCI/LPC/SMB Bus •
CRT/LCD video •
Dual channel enhanced IDE •
10/100Base-T •
AC'97 2.2 Audio •
2 RS232 Ports •
1 LPT Port •
4 USB 1.1 Ports •
8 GPIO Ports •
Keyboard and Mouse •
+3.3V •

5831
Pentium III EBX SBC designed for
Mobile and Outdoor Applications

- 500MHz to 1.26GHz Pentium III CPU
- Ultra low power
- Passive Heat Sink for CPU up to 900MHz
- 14W (using 900Mhz CPU, 256K L2 cache)
- -40°C to +85°C operating temperature

- Soldered Onboard 256MB SDRAM (Optional 768MB with SODIMM)
- CompactFlash Disk (up to 6 Gbytes)
- LCD/CRT Video, 10/100Base-T Ethernet interface, AC'97 Audio, TV Out
- 6 serial ports, dual USB, 256 Bytes EEPROM, 64-bit unique electronic ID
- 128/512Kbytes battery backed SRAM with 10 years data retention
- Intelligent thermal management with independent microcontroller
- Less than 4 seconds boot up time
- 8" x 5.75" standard EBX form factor
- Supports DOS, Windows 98, NT, 2000, XP, CE, QNX, pSOS, Linux, VxWorks

tme
Toronto MicroElectronics Inc.
5149 Bradco Boulevard, Mississauga, ON., Canada L4W 2A6
Tel: (905) 625 - 3203 ~ Fax: (905) 625 - 3717
sales@tme-inc.com ~ www.tme-inc.com

www.embedded-computing.com/search

cooling power will continue to escalate. Engineers designing embedded computing systems will undoubtedly face increasingly more complex cooling challenges, which will lead to the proliferation of copper heat sinks as well as fan sinks. **ECD**

***Barry Dagan** is technical director of the chief technology office at Cool Innovations, Inc. Barry has been involved in thermal management for more than 25 years in a variety of positions and industries. He holds multiple patents and designed a number of breakthrough thermal-management products. Barry earned his BSC in Mechanical Engineering at the Technion Institute of Technology.*

To learn more, contact Barry at:

Cool Innovations, Inc.
141 Cidermill Avenue, #2
Concord, ON, L4K 4G5
Canada
905-760-1992
barryd@coolinnovations.com
www.coolinnovations.com

Mesa
5I21
SERIAL
ANYTHING
I/O CARD

- 400K FPGA for Serial Logic
- 12 RS-422/RS-485 Channels
- Bus Master Capability
- Up to 10 Mbps Bit Rate Standard
- On card selectable Termination
- Fail Safe Input Biasing
- Price in 100's $153

Mesa Electronics
www.mesanet.com
PH: 510.223.9272 Fax: 510.223.9585
sales@mesanet.com
tech@mesanet.com

www.embedded-computing.com/search

IEI Provides You Complete Core 2 Duo Platform

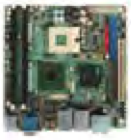
We maximize every application for you.

Based on revolutionary Intel® Core™ 2 Duo processors, IEI's single board computer products are ready to bring you with energy-efficient and multitasking performance. More unique functions like HDTV Out, HD Audio, PCIe Mini Card, ASF 2.0 and TPM 1.2 are integrated in IEI's innovative single board computer solution.

RoHS Lead Free

Power-Saving Solution

Industrial Motherboard



KINO-9452
Mini-ITX
Intel® Core™ 2 Duo, Core Duo/ Core Solo Processor, Dual PCIe GbE, HDTV output & Two independent stream Audio

KINO-9453
Mini-ITX
Intel® Core™ 2 Duo CPU with VGA/DVI, Dual GbE, USB 2.0, SATA II and Audio

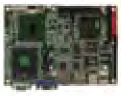
IMB-9452
microATX
Intel® Core™ 2 Duo, Core® Duo/Solo 667MHz FSB CPU, VGA, Dual PCIe GbE, SATA II, USB 2.0, 6 COM and Audio

Full-Size SBC

PCIE-9452
PICMG 1.3
Socket 479 Intel® Core™ 2 Duo CPU Card With VGA, Dual PCIe GbE, SATA II and USB 2.0

WSB-9452
PICMG 1.0
Intel® Core™ 2 Duo CPU with VGA / DVI/HDTV, Dual PCIe GbE, and SATA II

EPIC SBC



NANO-9452
Intel® Core™ 2 Duo/ Solo Processor, SATA II, Dual PCIe GbE, CF Type II, IDE, USB 2.0 and Audio

PICOe SBC

PICOe-9452
Intel® Core™ 2 Duo CPU with VGA/LVDS, Dual GbE, USB 2.0, SATA II and Audio

High-Performance Solution

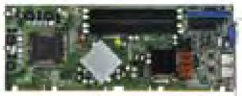
Industrial Motherboard

KINO-9454
Mini-ITX
Intel® Core™ 2 Duo, Pentium® 4/ Pentium® D 1066/800/533MHz CPU, SATA II, Dual PCIe GbE, USB 2.0 and Audio

IMB-9454
microATX
Intel® Core™ 2 Duo, Pentium® 4/ Pentium® D/ Celeron® D FSB 533/800/1066MHz CPU, VGA, Dual PCIe GbE, SATA II, USB 2.0, 6 COM, & Audio

IMBA-9454
ATX
Intel® Core™ 2 Duo, Pentium® D/ Pentium® 4/ Celeron® D CPU FSB 533/800/1066MHz,, VGA, Dual Channel DDR2, FDD, LPT, 4 x SATA II, 8 x USB 2.0 and 6 COM

Full-Size SBC



PCIE-9450 PICMG 1.3
LGA 775 Intel® Core™ 2 Duo™ Pentium® D/4 CPU Card with VGA, Dual PCIe GbE and SATA II

WSB-9454 PICMG 1.0
LGA775 Intel® Core™ 2 Duo, Pentium® D/4, Celeron ® D CPU with VGA/ DVI, Dual PCIe GbE, SATA II

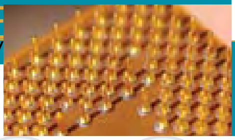
www.embedded-computing.com/search

America
IEI Technology USA Corp.
168 University Parkway, Pomona, CA 91768
Tel: +1-909-595-2819 Fax: +1-909-595-2816
sales@usa.ieiworld.com www.usa.ieiworld.com

Headquarters
IEI Technology Corp.
No. 29, Jhongsing Rd.,Sijhih City,Taipei County, 221, Taiwan
TEL : +886-2-86916798 FAX : +886-2-66160028
sales@ieiworld.com www.ieiworld.com

China
IEI Technology SH Corp.
515 Shen Fu RD. XinZhuang Industrial Develop Zone
TEL :+86-21-5442 9000 FAX : +86-21-5442 9100
sales@ieiworld.com.cn www.ieiworld.com.cn


ARM



Innovative band engineering techniques target CMOS gate leakage dilemma

By Robert J. Mears, PhD

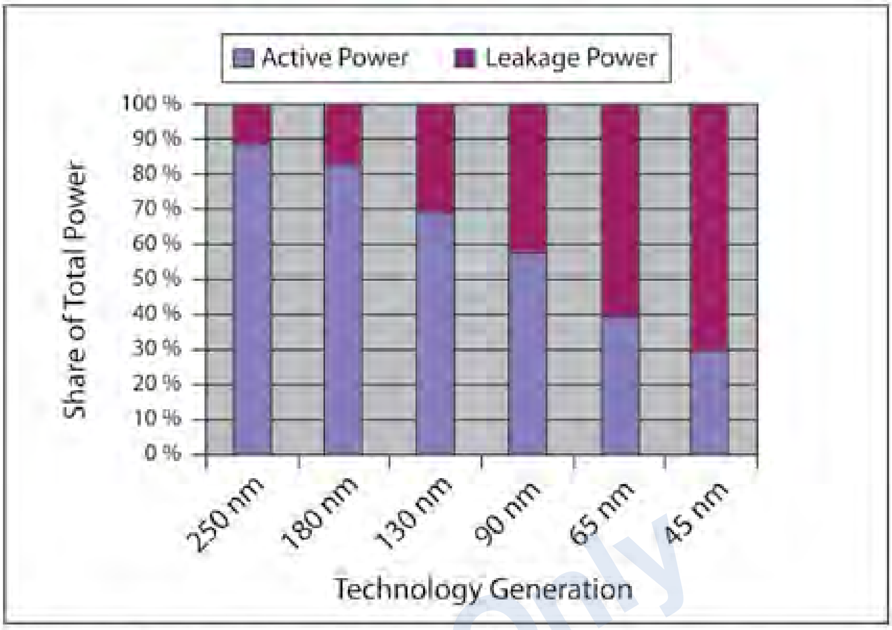
Semiconductor performance has gained enormous benefits from continuing advances in transistor scaling. While drive current enhancement techniques such as strain engineering and hybrid orientation have extended Moore's Law, one of the biggest barriers to device scaling beyond 45 nm is gate leakage, which accounts for significant static power dissipation in high-performance devices. A new platform addresses this pressing manufacturing and design challenge by reengineering silicon.

In the past 40 years, the semiconductor industry has reaped the benefits of silicon scaling to create a market where enormous and predictable advances in transistor performance are occurring concurrently with enormous and predictable reductions in transistor cost, size, and power consumption. Abiding by Moore's Law, the industry has continually doubled semiconductor performance approximately every two years while driving significant advances in areas such as portable electronics by lowering power requirements to extend battery life. Bulk silicon lies at the heart of this transformational industry and today accounts for up to 95 percent of the $250 billion semiconductor market.

Silicon's electrical properties, high-quality native oxide, low-defect density, and ability to scale to large wafer sizes have combined to make Complementary Metal Oxide Semiconductor (CMOS) silicon the industry's dominant design medium. Continual advances in the process roadmap have not come easily, however. As semiconductor manufacturers have migrated to finer process lithographies, silicon's fundamental physical properties and native oxide have been put to the test.

Perhaps the most imposing problem facing circuit designers today is current leakage, especially transistor gate leakage. As the industry moves from 90 nm manufacturing process geometries to 65 nm and below, serious degradation of IC power efficiency is becoming a dominant consideration. At 90 nm, static power consumption from leakage mechanisms, particularly gate leakage across increasingly thin gate oxides, accounts for more than 40 percent of the power dissipation of a microprocessor. At 65 nm, the problem worsens to about 60 percent. By the time the industry reaches 45 nm, the benefits of scaling will fail to boost performance in the face of imposing leakage, power dissipation, and

Perhaps the most imposing problem facing circuit designers today is current leakage, especially transistor gate leakage.



*Source: IC Insights, Intel; 45 nm extrapolation based on internal estimates

Figure 1

tunneling effects. Figure 1 illustrates how leakage is becoming a more significant concern than active power for MPUs.

No new materials

The semiconductor industry has attempted to address these scaling issues by investing in a number of innovative process improvements. The challenge has been determining how to extend the capabilities of silicon and lower power dissipation without requiring major changes in proven semiconductor materials.

At the 130 nm node, manufacturers began introducing commercially viable Silicon-On-Insulator (SOI) enhancements. This technology places a thin layer of insulation such as silicon oxide between the silicon surface and the substrate. SOI lowers parasitic capacitance and junction leakage, and in the process, boosts performance by 20-35 percent. It can also be used to lower power consumption compared to devices running at the same frequency in bulk CMOS. However, manufacturers using SOI technology face significantly higher substrate costs and yield challenges as the technology scales to finer process nodes and thermal-resistance issues arise.

At the 90 nm node, manufacturers turned to strained silicon techniques to address these scaling limitations. These technologies increase or decrease the normal inter-atomic distance between silicon atoms in the wafer plane. The small distortion of the crystal lattice alters the electronic band structure of the silicon. If the inter-atomic distance is increased (tensile strain), electrons travel more freely, but holes are impeded. The reverse is true if the inter-atomic distance is decreased (compressive strain). By combining tensile and compressive strain approaches, the mobility of both electrons and holes can be significantly improved, which in turn boosts chip operating speeds.

But as channel lengths shrink, the benefits of strained silicon approaches diminish. Regardless of which strained silicon approach is used, for instance, drain current enhancement in strained Negative-channel Metal Oxide Semiconductor (NMOS) devices saturates at 25 percent. And as manufacturers move to smaller geometries and scale up stresses, the technology becomes increasingly difficult to implement.

Intel and IBM recently announced advances in high-k dielectric oxides, which deliver better insulation than conventional silicon dioxide to reduce gate leakage. But problems persist with Fermi-level pinning and the generation of higher-threshold voltages, mobility degradation, and reliability issues. Despite these efforts, scalability issues remain. Furthermore, new high-k techniques introduce exotic materials such as hafnium to the manufacturing process, adding complexity and cost to the process flow.

Reexamining band engineering

In the past few years, researchers at MEARS Technologies have developed a new platform that addresses the fundamental obstacles to CMOS scaling by significantly reducing gate leakage while simultaneously enhancing drive current. This cost-neutral process does not use new materials in the fabrication process and is compatible with existing manufacturing infrastructure, including bulk CMOS, SOI, strained silicon, and high-k approaches.

Two well-known observations drove the search for this new methodology. The first was that the electronic properties of any material are primarily governed by its electronic band structure or the relationship between the energy and the momentum (speed) of electrons and holes in the material. The band structure of a material is a function of the arrangement of the atoms, or the lattice, and the electronic nature of the atoms themselves. The curvature of a material's band minima and maxima in turn determines how easily an electron or hole is accelerated. The larger the curvature, the more easily electrons are accelerated with an applied electric field – in other words, the electrons have a reduced effective mass.

The team determined that to improve performance, the lattice of the atoms had to be modified. Normally one would assume that altering the design of the lattice in the plane of the device would improve performance. Instead, the researchers discovered they could manipulate the bands in a planar silicon device by intermittently breaking the silicon periodicity in the vertical direction (see Figure 2). Furthermore, by leveraging their ability to build up the silicon by individual atom layers and taking advantage of recent advances in manufacturing equipment, they could complete this enhancement with a conventional silicon epitaxial step.

The additional silicon layer is fully crystalline but has a strongly anisotropic electronic band structure. Silicon atoms are intermittently spaced apart slightly more in the vertical than the horizontal plane of the device. That distribution supports the creation of *channels* for electrons and holes to travel parallel to the surface more freely in the wafer plane, improving electron mobility for both NMOS and Positive-channel Metal Oxide Semiconductor (PMOS) devices. This effect is in distinct contrast to strain techniques, for example, which require separate tensile strain for NMOS and compressive strain for PMOS.

In contrast, electron flow in the vertical direction is impeded. In this direction, effective mass can be increased and band curvature reduced by up to an order of magnitude. This unique property results in a significant reduction in gate leakage even while the additional silicon layer enhances drive current in the horizontal plane of the device.

Multiple benefits

This innovative approach to reengineering silicon, known as the *MST Platform*, or simply *silicon-on-silicon*, offers semiconductor manufacturers a variety of benefits. In-plane mobility increases drive current and can be used to improve transistor performance in microprocessors, DRAM, SRAM, flash and other memory ICs, as well as RF and mixed-signal devices. Some of this increased drive current capability can also be traded for higher-threshold voltages and lower-subthreshold leakage power. At the same time, the technology reduces gate leakage by up to 80 percent, far outperforming strained silicon or SOI technologies, while remaining completely compatible with these existing industry approaches. Early tests indicate that the silicon-on-silicon platform delivers up to 30 percent enhancement in drive current.

The MST Platform is the result of a five-year design effort conducted in partnership with International Sematech's Advanced Technology Development Facility and Lawrence Semiconductor Research Laboratory and has been tested on more than 1,000 wafers. Validated by industry-standard E-test and bench measurements, the new platform has been successfully applied to sub-90 nm processes and is compatible with industry-standard

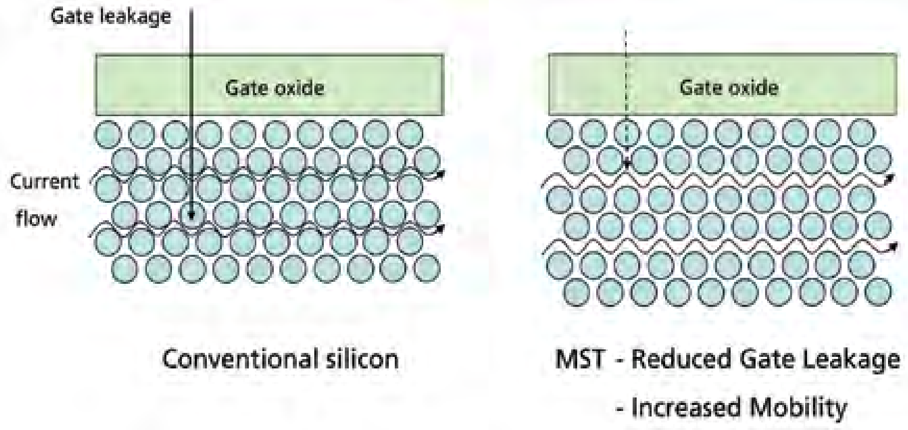


Figure 2

manufacturing equipment. Given its adaptability to existing CMOS infrastructure, the MST Platform is expected to be adaptable to next-generation 32 nm and 22 nm flows. MEARS Technologies' MST integration is shown in Figure 3.

From a semiconductor manufacturer's perspective, this technology offers a number of advantages. It reduces risk by relying on established CMOS manufacturing techniques and requiring no new materials or complex architectures. The technology also simplifies implementation because it can be easily inserted into existing manufacturing processes. It only requires the addition of a few simple steps to a standard CMOS flow used to construct the transistor channel. And it relies on standard equipment. In most cases, manufacturers can implement the technology in six months or less.

The MST Platform is also attractive from a cost standpoint. Given potential die real estate savings (from reducing the widths of non-minimum-geometry devices) and the technology's ability to use existing manufacturing tooling, implementing the technology is practically a cost-neutral exercise. Manufacturers using this technology simply insert the special expitially grown silicon into their standard CMOS flow as a channel replacement layer.

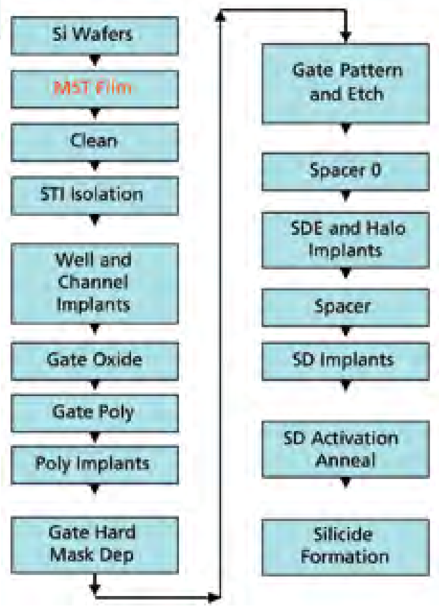


Figure 3

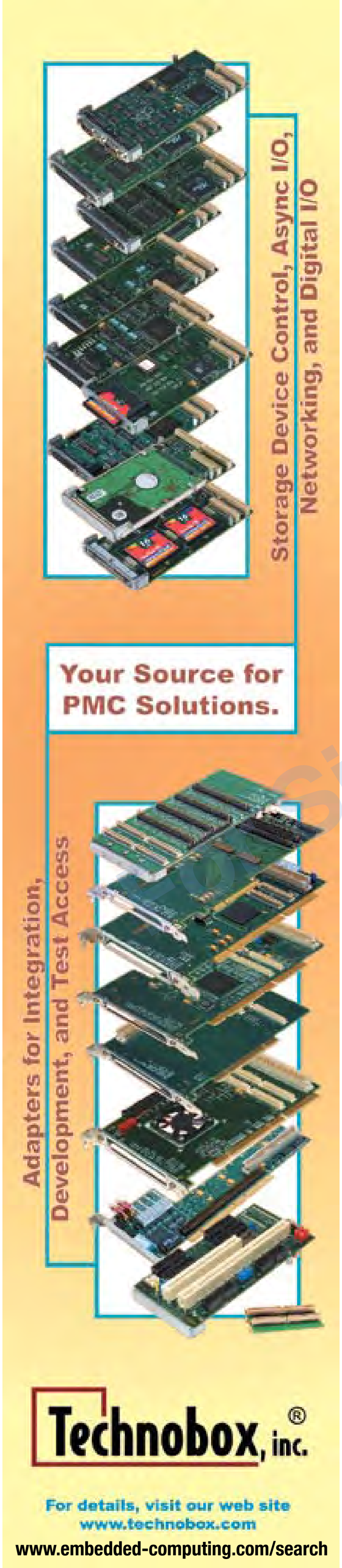
Perhaps the greatest cost impact of this new technology is the investments it allows semiconductor manufacturers to forgo. By increasing drive current and reducing gate leakage, the silicon-on-silicon approach allows semiconductor manufacturers to implement 65 nm and 45 nm CMOS generations without resorting to the added expense associated with alternative technologies. **ECD**

***Robert J. Mears**, PhD, is MEARS Technologies' founder, president, and CTO. Robert has 25 years of research experience in electronics and photonics and is the inventor of the erbium-doped fiber amplifier, which helped enable broadband Internet. He has authored or coauthored approximately 150 publications and numerous patents and is an Emeritus Fellow of Pembroke College, Cambridge.*

To learn more, contact Robert at:

MEARS Technologies
1100 Winter Street, Suite 4700
Waltham, MA 02451
617-219-0600
info@MEARStechnologies.com
www.MEARStechnologies.com


Industrial pqi
TURBO
2.5" SATA Flash Disk
64GB

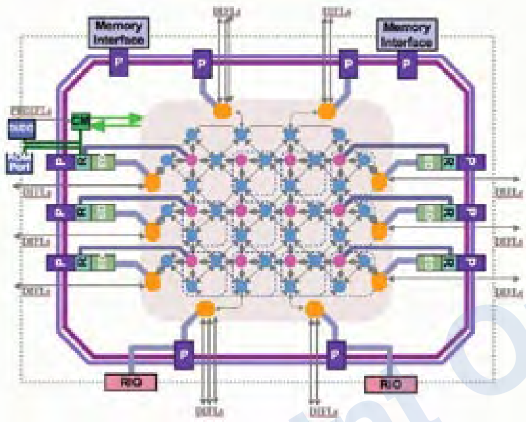


Editor's Choice • Embedded Computing Design •

PRODUCTS

Polymorphic processor

We're all familiar with configurable processors, but what about a processor that is adaptable and can morph to meet changing processing requirements? The University of Southern California Information Sciences Institute and Raytheon teamed under a contract with DARPA to create what they say is the world's first computer architecture that can adopt different forms depending on the application. Dubbed MONARCH (Morphable Networked MicroArchitecture) and developed to address the large data volume of sensor systems and their signal and data processing throughput requirements, it is the most adaptable processor ever built for the DoD. It performs as a single System-on-Chip (SoC) in an array of chips for teraflop throughput.



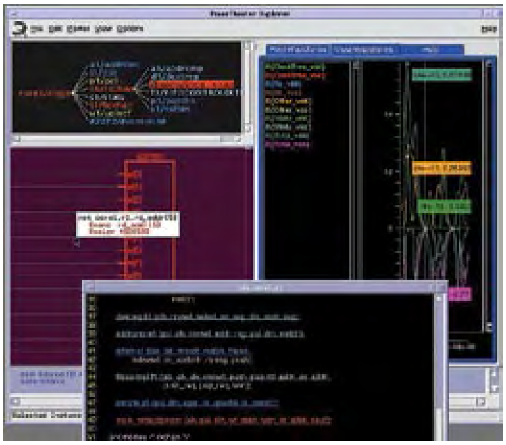
With this flexibility, MONARCH can significantly reduce the amount of hardware (and therefore power) required for computing systems while still achieving extremely high (teraflop) throughput. Because of the memory integrated on the chip, very small systems may be implemented with a single MONARCH device. For larger implementations, MONARCH's ability to "morph" devices so they can perform downstream tasks instead of sitting idle while waiting for fresh input further reduces hardware demand.

MONARCH, which contains six microprocessors and a highly interconnected reconfigurable computing array, provides 64 GFLOPS with more than 60 GBps of memory bandwidth and more than 43 GBps of off-chip data bandwidth. Each device has input/output ports to enable seamless data movement among multiple chips. The device has two off-chip memory interfaces for large problems. Every chip is equipped with two RapidIO interfaces for connecting to industry-standard equipment.

Raytheon Company • MONARCH

The power of visualization/debugging

A viewer that allows System-on-Chip (SoC) designers to find hot spots in a design and visualize, debug, and interactively determine ways to reduce a design's power could go a long way toward improving SoC power management.



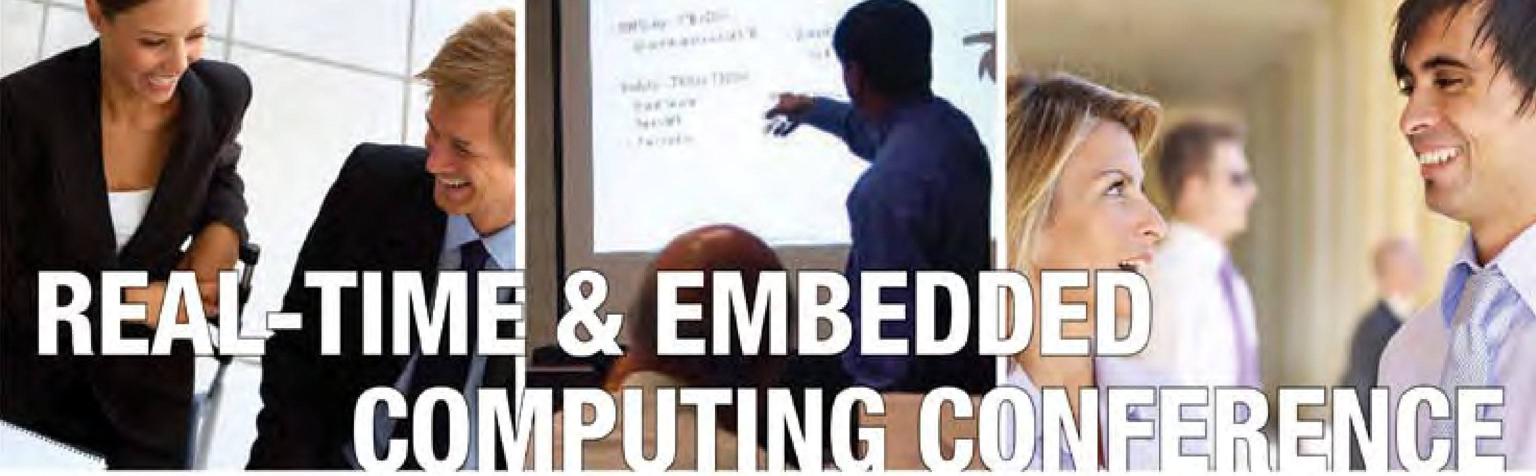
Sequence Design has added such a viewer to their PowerTheater analysis tools. This new analysis environment lets large design groups employ PowerTheater engines for power estimation and multiple PowerTheater-Explorer visualization and debugging tools.

"Users will experience immediate productivity gains when using PowerTheater-Explorer," said Sequence president and CEO Vic Kulkarni. "It provides access to more power data that can be manipulated at both the RTL and gate levels of abstraction than any other solution."

The hierarchical RTL power tree display shows hot spots that can be cross-probed to schematics, indicating how activity is moving through the design and how instances affect one another. The integrated waveform viewer in PowerTheater-Explorer can input qualified vectors for all modes of operation and report average modal power for package selection or worst-case for preventing dynamic voltage drop. Waveforms can be viewed simultaneously to debug power problems, including power over time, peak power, and comparisons between logic and power waveforms.

Sequence Design, Inc. • PowerTheater-Explorer

Editor's Choice Products are drawn from OSP's product database and press releases. Vendors may add their new products to our website at www.opensystems-publishing.com/vendors/submissions/np/ and submit press releases at www.opensystems-publishing.com/news/submit. OSP reserves the right to publish products based on editors' discretion alone, and does not guarantee publication of any product entries.



Real-Time & Embedded
computing conference

NEW TRAINING WORKSHOPS & SEMINARS

Register Today at www.rtecc.com

Enter a World of Embedded Computing Solutions

Attend open-door technical seminars and workshops especially designed for those developing computer systems and time-critical applications. Get ahead with sessions on Multi-Core, Embedded Linux, VME, PCI Express, ATCA, FPGA, Java, RTOS, SwitchFabric Interconnects, Windows, Wireless Connectivity, and much more.

Meet the Experts

Exhibits arranged in a unique setting to talk face-to-face with technical experts. Table-top exhibits make it easy to compare technologies, ask probing questions and discover insights that will make a big difference in your embedded computing world. Join us for this complimentary event!

Be sure to enter the drawing on-site for an iPod Video

AAEON ADVANTECH ELMA Green Hills intel
LYNUXWORKS NATIONAL INSTRUMENTS PENTEK QNX WIND RIVER

Join Us In...

January
Copenhagen, Denmark
Santa Clara, CA

February
Melbourne, FL

March
Huntsville, AL
Atlanta, GA
Phoenix, AZ
Albuquerque, NM

April
Boston, MA
Bethesda, MD

May
Milan, Rome Italy
Dallas, Austin, Houston, TX

June
Chicago, IL
Minneapolis, MN

July

August
Longmont, CO
Colorado Springs, CO

September
Beijing, Shanghai, China
Ottawa, ON
Montreal, PQ
Shenzhen, Xi'an, China
San Diego, Long Beach, CA

October
Tyson's Corner, VA

November
Detroit, MI
Toronto, ON
Vancouver, BC

December
Seattle, WA
Portland, OR

www.rtecc.com

For Single Print Only

www.embedded-computing.com/search

Check out data sheets and more

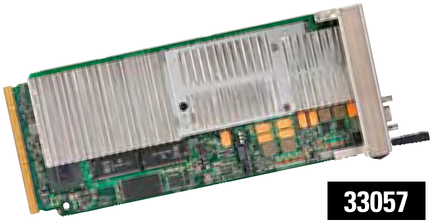
Special Services and Events: New Products at www.embedded-computing.com/search

AdvancedMC module

Motorola

Model: PrAMC-7201 **RSC No:** 33057

Processor AdvancedMC module • Intel Pentium M processor, E7520 memory controller hub, and 6300ESB I/O controller hub • Dual GbE interfaces based on Intel 82571ED PCI Express to dual GbE controller • Memory configurations possible up to 2 GB with ECC support • MontaVista CGE 4.0 for the Centellis and Avantellis 3000 series platforms • Wind River PNE Linux operating environment for the Centellis 1000 platform • AMC.1 PCI Express, AMC.2 GbE, and AMC.3 SATA support • Module management controller implementing IPMI v1.5



33057

Data acquisition

Advantech eAutomation Group

Model: PCI-1742U **RSC No:** 32973

One MSps, 16-bit, 16-channel high-resolution multifunction data acquisition card • Fast sampling rate for PCI bus • 16x single-ended or 8x differential analog input channels, 1.0 MSps single-channel sampling rate (800 KSps multichannel), 2x 16-bit D/A output channels, 16x digital I/O channels, and 1x 10 MHz 16-bit counter channel • 1K analog input FIFO • Autocalibration function • Universal PCI bus support (3.3 V and 5 V PCI bus signaling) • Board identification switch • Comes with Windows DLL drivers and ActiveX controls for programming with VB, VC, or Delphi • LabVIEW drivers are included for easy integration into LabVIEW applications

32973

GE Fanuc Embedded Systems

Model: daqNet **RSC No:** 33036

A fully integrated acoustic data acquisition/conversion system • Fully integrated acoustic server in a compact rack-mount 1U chassis • Up to 192 channels of acoustic I/O or 240 channels of digital I/O • Dual GbE interfaces for data I/O and control • Choice of up to four analog input, analog output, and digital I/O modules • Precise sampling synchronization across multiple servers • User configuration digital I/O module with immediate, external signal, or time-based trigger

33036

Display controller

Matrox Graphics

Model: TripleHead2Go Digital **RSC No:** 33019

Part of Matrox's series of Graphics eXpansion Modules • Supports a stretched desktop of up to 3840 x 1024 (triple 1280 x 1024) across three monitors • Upgrade a workstation, desktop computer, or notebook to use three monitors (four including notebook screen) at a time • Features a dual-link digital I/O for high-end workstations and DVI monitors • Provides support for systems with analog (VGA) output and analog (VGA) monitors • Support for a dual-monitor configuration for a maximum resolution of 3840 x 1200 (dual 1920 x 1200) stretched across two displays • No parts to insert in a computer and no hardware or software replacement • Harness existing graphics hardware's full capabilities for 2D, 3D, and video • Compact box suitable for travel • Easy-to-use Matrox PowerDesk software for multidisplay controls

DSP algorithm

IntegrIT

Model: NatureDSP Signal **RSC No:** 33004

A library of signal processing routines needed for implementing typical algorithms for advanced signal processing • Real-time, accurate LPF/HPF/notch/peak filter synthesis • A set of predefined filters/interpolators for standard voice/audio sample rates (8,000, 11,025, 14,400, 16,000, 22,050, 44,100, 48,000 Hz) • Wide variety of windowing functions • Envelope detection, adaptive averaging, RSSI • True fixed-point implementation with saturation; no floating point • Free library for MS Visual Studio – enables development under PC

Enclosure

Hybricon

Model: DT-XC VPX REDI **RSC No:** 32996

Desktop chassis • Supports six-slot VITA 48.1 VPX-REDI backplane with 1.0" pitch • Five-slot full-mesh backplane with uncommitted six-slot 1,900 W power supply supports a wide range of 12 V and 5 V powered VPX • VPX-REDI desktop development platform • Side-to-side cooling • 6U x 160 mm subrack supporting six 1.0" pitch positions • Subrack supports 6U x 80 mm rear-transition modules • Front panel includes a DC ENABLE switch, a system reset button, and power indication LEDs • VPX-REDI backplane with 1.0" pitch per VITA 46.0, 46.3, 46.10, 48.0, and 48.1 • DC power: +12 V at 75 A (VITA 46 VS1 and VS2 supply), +5 V at 100 A (VITA 46 VS3 supply), +3.3 V at 40 A (VITA 46 3.3 V AUX), +12 V at 17 A (VITA 46 +12 V AUX), and 12 V at 17 A (VITA 46 -12 V AUX) • Cooling: provides 18 CFM per slot with high-pressure boards • Fan monitor speed control • Width: 17.18" (436.4 mm) • Height: 10.47" (265.9 mm) 6U • Depth: 16.00" (406.4 mm) • Weight: 28 lbs • Two top handles • Standard desktop feet

Fieldbus: CAN

PEAK-System

Model: PCAN-PC/104-Plus **RSC No:** 32971

Baud rate settings up to 1 Mbaud • CAN bus connection via Sub-D, 9-pin (to CiA DS102-1) • Two can be configured totally independently • SJA1000 CAN controller with 16 MHz clock frequency • Four PCAN-PC/104-Plus cards in a single PC/104 stack possible • Operation in 5 V and 3.3 V PC/104-*Plus* systems • Support for operating systems Windows 2000, XP, Embedded XP, Vista, and Linux (including XENOMAI support) • Works 100 percent with CANfestival (free CANopen master/slave SW stack for Windows and Linux)

FPGA resource boards

Acromag

Model: PMC-CX **RSC No:** 33064

User-configurable FPGA modules feature conduction cooling and differential digital I/O • Cost/performance mix suitable for many mid-level computing functions • 32 bidirectional RS-422/485 differential I/O lines or 16 bidirectional CMOS I/O lines • Rear I/O connection • Customizable FPGA with 11,500 or 24,192 logic cells (Xilinx Virtex-II XC2V1000 or XC2V2000) • FPGA code loads from PCI bus or flash memory • 256K x 36-bit dual-ported SRAM memory • Supports dual DMA channel data transfer to CPU • Supports both 5 V and 3.3 V signaling • Extended temperature operation (-40 °C to +85 °C)

33064

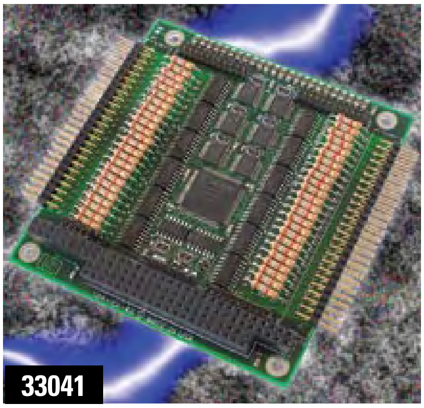
NEW PRODUCTS

I/O: digital

ACCES I/O Products

Model: 104-IDI-48 Series **RSC No:** 33041

A family of 48-channel optically isolated digital input boards • PC/104 form factor • 48 individually optically isolated AC/DC inputs • Polarity-insensitive AC/DC inputs accept up to 60 Vdc or AC rms • Change-of-state detection (IRQ) on selected inputs (certain models) • AC or voltage transient filtering • Optically isolated channel-to-channel and channel-to-ground • -40 °C to +85 °C operating temperature



33041

I/O: multifunction

Lyrtech

Model: Quad Dual-Band RF **RSC No:** 33066

The Quad Dual-Band RF transceiver is a four-channel MIMO RF analog front end, as part of a development solution for MIMO and 2.4-5 GHz RF multichannel advanced base stations • Rack-mount four-channel 2.4-5 GHz MIMO RF to Zero-IF analog front-end – MAX2829 (4x) • Plug-and-play with Lyrtech DSP and FPGA advanced development platforms • Fully controllable RF and baseband receiver gains • 30 dB power control range on transmitters • Antenna polarization switching capability • Coherent locked phase of all RX/TX transceivers, enabling beam-forming prototyping

33066

Integrated Development Environment

Applied Informatics

Model: Rapide++ **RSC No:** 32985

Rapide is Applied Informatics' Integrated Development Environment (IDE) for embedded Linux application development under both Windows and Linux host systems • Based on Eclipse CDT, the open source industry-standard IDE for embedded and enterprise software development • Automatic discovery of development boards connected via Ethernet (TCP/IP) • No need to configure IP addresses manually • Plug-and-play development • A variety of target tools: terminal, file system browser, editor, system viewer, and process and thread viewer • Development tools readily available • POCO C++ class libraries and wizards for new project creation and the import of GNU Autoconf-based open source projects • Comfortable remote debugging • Powerful, cross-platform build system

RoweBots

Model: iZoom! v3 **RSC No:** 33062

Eclipse-based C/C++ IDE with compiler, debugger, and libraries • Single-click install • Integrated compiler • Integrated debugger • Open source • Includes support and textbooks to facilitate programming proficiency

Memory

Varisys

Model: VMS1 **RSC No:** 32974

An IEEE P1386.1-compliant PMC module that allows one or two standard CompactFlash memory cards to be used as a mass storage solution for embedded systems • Measures 149 mm x 74 mm • Supports single or dual CompactFlash memory cards (Type I or Type II) • PCI rev 2.2-compliant 32-bit 33 MHz bus master with DMA • SFF-8038i-compliant ATA host controller • Supports all PIO and UDMA modes up to ATA/100 • Optional external connection to one IDE channel via PMC P14 user I/O • Commercial and rugged variants, with options including conformal coating, industrial temperature operation, and conduction cooling • Compatible with Windows, Linux, VxWorks, and many other operating systems

PC/104 module

Arbor Technology

Model: Em104-a5362 **RSC No:** 32969

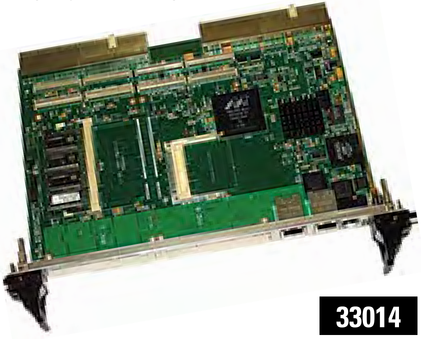
Low-power PC/104 CPU module • AMD Geode LX series processor • 1x 200 pin • DDR SODIMM up to 1 GB SDRAM • Supports CRT and 18/24-bit TTL • 2x USB 2.0 ports and 2x serial ports • Supports PC/104 interface

Processor: PowerPC

Orion Technologies

Model: CPC7510 **RSC No:** 33014

PowerPC 6U SBC • IBM 750FX or 750GX • CompactPCI host or peripheral controller • Marvell Discovery II system controller • Two 64-bit 66 MHz PMC slots • Two 10/100 Ethernet ports • Hot swap/high availability



33014

Processor: Xeon

WIN Enterprises

Model: PL-01033 **RSC No:** 32990

2U rack-mount dual Intel Xeon network appliance with 10 GbE, two SATA HDD, Mini PCI, LCM • High-performance network appliance for the enterprise market • Supports dual Intel Xeon processors with 800 MHz FSB • 10 GbE SFP or copper connectors • Bypass function in four GbE ports • Two 64-bit PCI-X 100 MHz slots and one Mini PCI slot

System boards

North Atlantic Industries

Model: 75C2 **RSC No:** 32986

Improved single-slot, multifunction, 3U CompactPCI card • Synchro measurement, A/D, D/A, function generator, discrete I/O, TTL I/O, transceiver I/O, and RTD available • Interchangeable multifunction design provides extensive diagnostics • Available in both commercial temperature range and severe environment/industrial temperature range • For increased flexibility, each of the 75C2's functions is highly programmable at the channel level • Continuous BIT testing is performed on all functions and channels

32986

Technobox

Model: 4978 **RSC No:** 32975

RoHS-compliant adapter • Supports up to eight lanes for SAS or SATA devices (four per connector) • Rates up to 3 Gbps per lane • PCI-X compatible • LSI SAS1068 controller • Dual SFF-8470 front-panel interface • Storage of user-defined parameters, BIOS, and mirroring data

32975

NEW PRODUCTS

Check out data sheets and more
Special Services and Events: New Products at www.embedded-computing.com/search

Telecom

MEN Micro

Model: F210 Interface Card **RSC No:** 33056

A 3U, single-slot CompactPCI interface card with a highly sensitive, 12-channel parallel GPS receiver and a GSM device for communications in very low signal strength applications • GSM-R (Rail) EGSM 900/GSM 1800 and GPS according to NMEA 0183 • GPS and GSM are optically isolated • 4 HP 32-bit/33 MHz CompactPCI • Two UARTs via SA-Adapters • FPGA for further customized functions • Two reverse SMA connectors to external antennae • Extended temperature ranges • Conformal coating

Tracking: RFID

ThingMagic

Model: Mercury5e **RSC No:** 33032

An embedded RFID reader utilizing the Intel RFID Transceiver R1000 chip, which integrates a number of components into a single RFID circuit • Combines multiregion capability into a single RFID module, enabling immediate, locally compliant deployment of any Mercury5e in Europe, North America, or South Korea • Utilizes an embedded version of the latest ThingMagic "Yagi" MercuryOS, for 100 percent tag reads and simultaneous reads • Provides the ability to identify and filter interference from other RFID readers, fluorescent lighting, and wireless networks and telephones • Optimized for Generation 2 RFID tags • Supports Generation 2 dense reader mode and advanced filtering to reject multiple interference sources • Consumes very little power, facilitating maximum battery life and a broader range of mobile and embedded RFID applications

NEW PRODUCTS

Check out data sheets and more

Special Services and Events: New Products at www.embedded-computing.com/search

ADVERTISER INFORMATION

Page #	Advertiser	Category
15	Advantech Corporation	Single board computers and blades
11	AMAX	Embedded Systems/Solutions
22	Annapolis Micro Systems, Inc.	FPGAs, reconfigurable computing
28	ARM Developers' Conference	Industry tradeshow
21	Fastwel Co. Ltd.	MIL-Spec/Industrial Solutions
8	Harting Technology Group	Connectors and adapters
32	Harting Technology Group	Connectors and adapters
27	IEI Technology USA Corp.	High-performance computing
18	Intel	High-performance computing
31	MEN Micro Elektronik GmbH	MIL-Spec/Industrial Solutions
16	Mesa Electronics	Mezzanines and I/O modules
26	Mesa Electronics	Mezzanines and I/O modules
5	Micro/sys, Inc.	Single board computers and blades
1	MOXA	MIL-Spec/Industrial Solutions
33	PQI Europe	Storage solutions
6	Radian Heatsinks	High-performance computing
35	Real-Time & Embedded Computing	Industry tradeshow
34	Technobox, Inc.	Mezzanines and I/O modules
25	Technologic Systems	FPGAs, reconfigurable computing
2	Toronto MicroElectronics, Inc.	Embedded Systems/Solutions
14	Toronto MicroElectronics, Inc.	Embedded Systems/Solutions
26	Toronto MicroElectronics, Inc.	Embedded Systems/Solutions
24	Tri-M Systems Inc.	High-performance computing
30	Tri-M Systems Inc.	High-performance computing
39	Ultimate Solutions, Inc.	Embedded Systems/Solutions
40	VersaLogic Corp.	High-performance computing
3	WinSystems, Inc.	Single board computers and blades

www.embedded-computing.com/search

OpenSystems Publishing

Advertising/Business Office

30233 Jefferson Avenue
St. Clair Shores, MI 48082
Tel: 586-415-6500 ■ Fax: 586-415-4882

Vice President Marketing & Sales
Patrick Hopper
phopper@opensystems-publishing.com

Business Manager
Karen Layman

Sales Group

Dennis Doyle
Senior Account Manager
ddoyle@opensystems-publishing.com

Tom Varcie
Senior Account Manager
tvarcie@opensystems-publishing.com

Doug Cordier
Account Manager
dcordier@opensystems-publishing.com

Andrea Stabile
Advertising/Marketing Coordinator
astabile@opensystems-publishing.com

Christine Long
E-marketing Manager
clong@opensystems-publishing.com

Regional Sales Managers

Jerry Bleich
New England
jbleich@opensystems-publishing.com

Richard Ayer
West Coast
rayer@opensystems-publishing.com

Barbara Quinlan
Midwest/Southwest
bquinlan@opensystems-publishing.com

Ron Taylor
East Coast/Mid Atlantic
rtaylor@opensystems-publishing.com

Ernest Godsey
Central and Mountain States
egodsey@opensystems-publishing.com

International Sales

Dan Aronovic
Account Manager – Israel
daronovic@opensystems-publishing.com

Reprints and PDFs

Becky Mullaney: 717-399-1900 ext 166
ecdreprints@opensystems-publishing.com

www.opensystems-publishing.com

BDI2000
BDI1000

What Do These Embedded Applications Have In Common?

Each embedded application is unique. That's why VersaLogic offers an extensive line of embedded products with choices of size, performance, and features. That's also why **VersaLogic works closely with customers** to tailor standard products to meet their needs. **Product customization** is available in quantities as low as 100 pieces!

More importantly, embedded customers have many **common needs**. Meticulous quality standards, dedicated customer support, and reliable product delivery are just a few that VersaLogic provides. That's why customers from a wide range of industries **rely on VersaLogic** for their embedded computer needs.

Could you use **uncommonly-good support**? Call today to see if your unique application is a good match with VersaLogic's unique approach to service and support. We may have more in common than you think!

Call 800-824-3163. Visit www.VersaLogic.com.

30 YEARS
1976 - 2006
VERSALOGIC CORPORATION

VDC
2006
PLATINUM
VENDOR

Rated a **"Platinum Vendor"**
by Venture Development
Corporation (2002-2006) for
excellence in customer service.

VERSALOGIC
CORPORATION
(800) 824-3163 • info@VersaLogic.com

www.embedded-computing.com/search

MOXA®

Moxa Systems Co., Ltd.
Tel: +886-2-2910-1230
Fax: +886-2-2910-1231
www.moxa.com
info.sys@moxa.com

USA

Moxa Technologies, Inc.
Toll-free: 1-888-MOXA-USA (1-888-669-2872)
Tel: +1-714-528-6777
Fax: +1-714-528-6778
www.moxaUSA.com
usa@moxa.com

Taiwan

Moxa Technologies, Inc.
Tel: +886-2-8919-1230
Fax: +886-2-8912-1231
www.moxa.com
taiwan@moxa.com

China

Moxa Technologies Shanghai, Inc.
Tel: +86-21-5298-8618
Fax: +86-21-5298-8643
www.moxa.com
china@moxa.com

Moxa Technologies Beijing, Inc.
Tel: +86-10-6872-3959/60/61
Fax: +86-10-6872-3958
china@moxa.com

Moxa Technologies Shenzhen, Inc.
Tel: +86-755-8368-4084/94
Fax: +86-755-8368-4148
www.moxa.com
china@moxa.com

Europe

Moxa Europe GmbH
Tel: +49 (0) 89 3 70 03 99-0
Fax: +49 (0) 89 3 70 03 99-99
www.moxa.com
europe@moxa.com

P/N: 1900000009810 Vol. 7.1

MOXA®

Embedded Computers

Ready-to-Run, Reliable, Wide Temperature

Microsoft® Windows® Embedded Partner

-40°C 75°C

Warranty 5 Year

www.moxa.com

ThinkCore W341/321/311

RISC-based Ready-to-Run Wireless Embedded Computers with WLAN, 4/2/1 Serial Ports, LAN, SD, USB, Linux OS

- MOXA ART ARM9 32-bit 192 MHz processor
- On-board 64/32 MB RAM, 16 MB flash disk
- 802.11a/b/g wireless LAN
- WEP, WPA, and WPA2 encryption
- Infrastructure Mode and Ad-Hoc Mode supported
- WLAN Repeater function supported
- 4/2/1 software-selectable RS-232/422/485 serial ports
- 10/100 Mbps Ethernet for network redundancy
- Designed to withstand continuous 5G vibration and 50G shock
- SD socket for storage expansion supported
- Ready-to-run Linux Kernel 2.6 platform
- DIN-rail or wall-mount installation
- Robust, fanless design

ThinkCore W345/325/315

RISC-based Ready-to-Run Wireless Embedded Computers with GSM/GPRS, 4/2/1 Serial Ports, LAN, SD, USB, Linux OS

- MOXA ART ARM9 32-bit 192 MHz processor
- On-board 64/32 MB RAM, 16 MB flash disk
- Built-in quad band GSM/GPRS 850/900/1800/1900 MHz
- GPRS Class 10, Coding Scheme from CS1 to CS4 supported
- 4/2/1 software-selectable RS-232/422/485 serial ports
- 10/100 Mbps Ethernet for network redundancy
- Designed to withstand continuous 5G vibration and 50G shock
- SD socket for storage expansion supported
- Ready-to-run Linux Kernel 2.6 platform
- DIN-rail or wall-mount installation
- Robust, fanless design

ThinkCore V481

X86 Ready-to-Run Embedded Computer with VGA, Dual LANs, 8 Serial Ports, CompactFlash, USB, Audio, WinCE 5.0 OS

- Intel Celeron M 1 GHz CPU, 400 MHz FSB
- On-board 256 MB DDR SRAM, 128 MB CompactFlash
- 8 software-selectable RS-232/422/485 serial ports
- Serial port speed from 50 bps to 921.6 Kbps, supporting ANY BAUDRATE
- Dual 10/100 Mbps Ethernet for network redundancy
- Supports 2nd CompactFlash socket for storage expansion
- 2 USB 2.0 Hosts support system bootup
- LED indicators for System Ready and Storage
- Ready-to-run WinCE 5.0 platform
- DIN-rail or wall-mount installtion
- Robust, fanless design

EM-1220

RISC-based Ready-to-Run Embedded Core Module with 2 Serial Ports, Dual LANs, SD, µClinux

- MOXA ART ARM9 32-bit 192 MHz processor
- On-board 16 MB RAM, 8 MB flash disk
- 2 software-selectable RS-232/422/485 serial ports
- Dual 10/100 Mbps Ethernet for network redundancy
- RS-232 serial console port supports PPP
- Ready-to-run µClinux Kernel 2.6 platform
- SD signals supported for external SD socket connection
- Built-in RTC, buzzer
- 8 GPIOs reserved for system integration
- Credit card size design for easy integration at any field site
- Full-function development kit for quick evaluation and application development
- -40 to 75°C wide temperature model available

EM-1240

RISC-based Ready-to-Run Embedded Core Module with 4 Serial Ports, Dual LANs, SD, µClinux

- MOXA ART ARM9 32-bit 192 MHz processor
- On-board 16 MB RAM, 8 MB flash disk
- 4 software-selectable RS-232/422/485 serial ports
- Dual 10/100 Mbps Ethernet for network redundancy
- RS-232 serial console port supports PPP
- Ready-to-run µClinux Kernel 2.6 platform
- SD signals supported for external SD socket connection
- Built-in RTC, buzzer
- 10 GPIOs reserved for system integration
- Full-function development kit for quick evaluation and application development

UC-7124/UC-7122

Mini RISC-based Ready-to-Run Embedded Computers with 4/2 Serial Ports, Dual LANs, SD, USB, WinCE 5.0 OS

- Cirrus Logic EP9302 ARM9 32-bit 192 MHz processor
- On-board 16 MB RAM, 16 MB flash disk
- 4/2 software-selectable RS-232/422/485 serial ports
- Serial port speed from 50 bpsto 921.6Kbps, supporting ANY BAUDRATE
- Dual 10/100 Mbps Ethernet for network redundancy
- SD socket for storage expansion supported
- Built-in RTC, buzzer, Watchdog Timer
- Ready-to-run WinCE 5.0 platform
- -40 to 75°C wide temperature model available

UC-7420/UC-7410

RISC-based Ready-to-Run Embedded Computer with 8 Serial Ports, Dual LANs, USB, PCMCIA, CompactFlash

- Intel XScale IXP-422/425, 266/533 MHz processor
- On-board 128 MB RAM, 32 MB flash disk
- 8 RS-232/422/485 serial ports
- Dual 10/100 Mbps Ethernet for network redundancy
- USB 2.0 Host
- CompactFlash socket for storage expanion
- PCMCIA supports WLAN, GPRS, UMTS, HSDPA
- LCM display and keypad for HMI
- Ready-to-run Linux / WinCE 5.0 platform
- DIN-rail or wall-mount installation
- Robust, fanless design

UC-7408

RISC-based Data Acquisition Embedded Computer with 8 Serial Ports, 8 DI Channels, 8 DO Channels, Dual LANs, PCMCIA, CompactFlash

- Intel XScale IXP-422/425, 266/533 MHz processor
- On-board128 MB RAM, 32 MB flash disk
- 8 RS-232/422/485 serial ports
- 8-ch digital input and 8-ch digital output
- Dual 10/100 Mbps Ethernet for network redundancy
- CompactFlash socket for storage expanion
- PCMCIA supports WLAN, GPRS, UMTS, HSDPA
- Ready-to-run Linux / WinCE 5.0 platform
- DIN-rail or wall-mount installation
- Robust, fanless design

UC-7402

RISC-based Ready-to-Run Embedded Network Computer with Dual LANs, PCMCIA, CompactFlash

- Intel XScale IXP-422/425, 266/533 MHz processor
- On-board 128 MB RAM, 32 MB flash disk
- Dual 10/100 Mbps Ethernet for network redundancy
- CompactFlash socket for storage expanion
- PCMCIA supports WLAN, GPRS, UMTS, HSDPA
- Ready-to-run Linux platform
- Hardware level data encryption engine supports AES, DES, and 3DES
- SSL, SSH, TLS security function
- Built-in firewall and VPN function
- Apache web server supports PHP and XML
- DIN-rail or wall-mount installation

ThinkCore DA-660 Series

RISC-based 19-inch Rackmount Data Acquisition Embedded Computers with 8/16 Serial Ports, LANs/Fiber Ports, PCMCIA, CompactFlash, USB

- Intel XScale IXP-422/425, 266/533 MHz processor
- On-board 128 MB RAM, 32 MB flash disk
- 8/16 RS-232/422/485 serial ports
- Dual/quad 10/100 Mbps Ethernet for network redundancy
- Standard 19-inch rackmount installation, 1U height
- Wide range of power input voltages from 100 to 240V, both AC and DC
- LCM display and keypad for HMI
- Ready-to-run Linux / WinCE 5.0 platform
- Robust, fanless design

ThinkCore IA241/IA240

RISC-based Industrial Ready-to-Run Embedded Computers with 4 Serial Ports, 4 DI Channels, 4 DO Channels, Dual LANs, PCMCIA, SD

Wide Temperature

TAIWAN EXCELLENCE 2006

- MOXA ART 32-bit ARM9 industrial processor
- On-board 64 MB RAM, 16 MB flash disk
- 4 RS-232/422/485 serial ports
- 4-ch digital input and 4-ch digital output
- Dual 10/100 Mbps Ethernet for network redudancy
- PCMCIA supports wireless expansion (802.11b/g, GPRS/ UMTS/HSDPA)
- SD socket for storage expansion supported
- Ready-to-run Linux platform
- Unique patented Software Encryption Lock
- Industrial DIN-rail installation, wall-mount is also possible
- Robust, fanless design, IP30 protection mechanism
- -40 to 75°C wide temperature model available

UC-7112/UC-7110

Mini RISC-based Ready-to-Run Embedded Computers with 2 Serial Ports, Dual LANs, SD

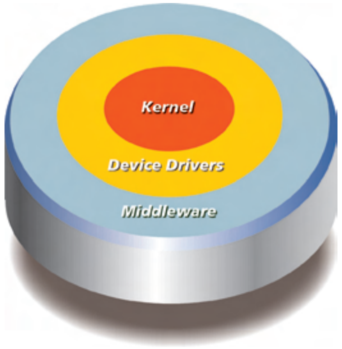
Wide Temperature

- Mini controller with ready-to-run platform for customized applications
- MOXA ART ARM9 32-bit 192 MHz processor
- 16 MB RAM (about 12 MB of user programmable space)
- 8 MB Flash ROM (about 4 MB of user programmable space)
- Dual 10/100 Mbps Ethernet for network redundancy
- 2 software-selectable RS-232/422/485 serial ports
- SD socket for storage expansion supported
- Built-in RTC, buzzer
- Ready-to-run µClinux platform
- GNU GCC cross-compiler
- -40 to 75°C wide temperature model available (UC-7110 only)

MOXA Ready-to-Run Software Environment

Kernel Ready
- Linux
- Windows CE 5.0

Device Drivers
- Ethernet
- 802.11a/b/g
- GPRS, UMTS, HSDPA
- RS232/RS422/RS485
- USB 1.1/2.0
- CompactFlash, SD
- PCMCIA/CardBus
- Watchdog
- LCM, Keypad, Buzzer,...



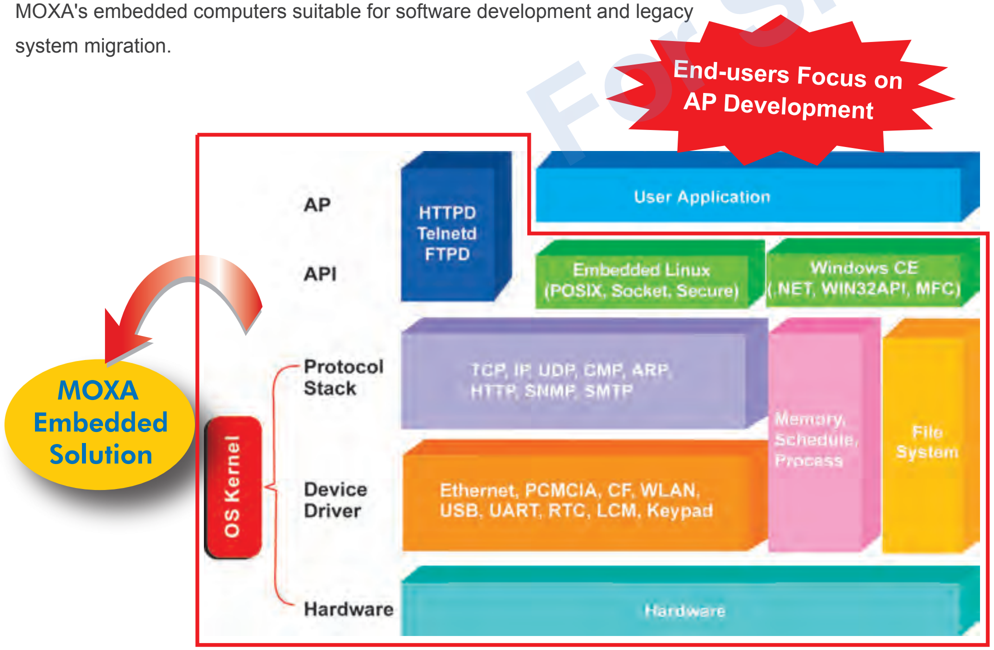
File Systems
- JFFS2 (Linux)
- TFAT (WinCE)

Services
- Telnetd
- FTPD
- HTTPD
- SSHD
- Firewall

Middleware
- OpenVPN
- MySQL
- Web Service

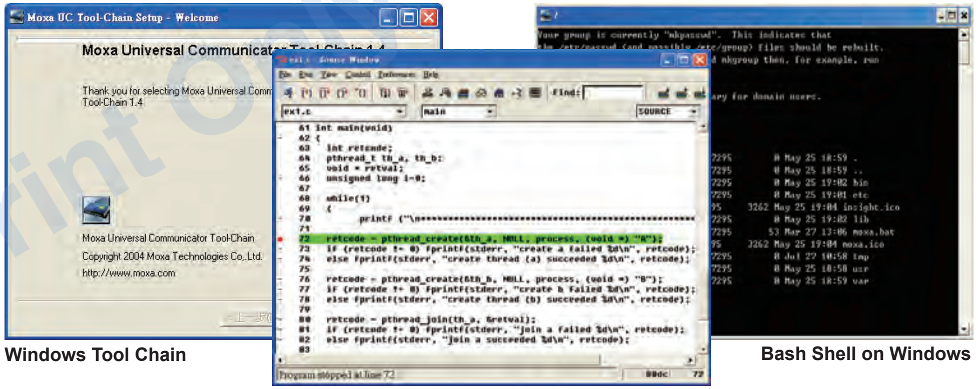
Open yet Reliable Operating System for Easy Development

MOXA embedded computers are built on either the Linux or Microsoft® Windows® CE 5.0 operation system. Building on an open operating environment makes MOXA's embedded computers suitable for software development and legacy system migration.



Linux Application Development

MOXA Linux C/C++ APIs	Software Encryption Lock (Patented)
Linux PC Tool Chain	MOXA 2G NPort Real TTY Driver
Windows Tool Chain	UC-Finder: IP Broadcast Search
PHP/CGI/Perl	On-Line Source Code Debugging



Moxa Universal Communicator Tool-Chain 1.4

Thank you for selecting Moxa Universal Comm
Tool-Chain 1.4

Moxa Universal Communicator Tool-Chain

Copyright 2004 Moxa Technologies Co.,Ltd.

http://www.moxa.com

```
int main(void)
{
  int retcode;
  pthread_t th_a, th_b;
  void * retval;
  unsigned long i=0;

  while(1)
  {
        printf ("\n*****************************************************

  retcode = pthread_create(&th_a, NULL, process, (void *) "A");
  if (retcode != 0) fprintf(stderr, "create a failed %d\n", retcode);
  else fprintf(stderr, "create thread (a) succeeded %d\n", retcode);

  retcode = pthread_create(&th_b, NULL, process, (void *) "B");
  if (retcode != 0) fprintf(stderr, "create b failed %d\n", retcode);
  else fprintf(stderr, "create thread (b) succeeded %d\n", retcode);

  retcode = pthread_join(th_a, &retval);
  if (retcode != 0) fprintf(stderr, "join a failed %d\n", retcode);
  else fprintf(stderr, "join a succeeded %d\n", retcode);
```

Program stopped at line 72

```
Your group is currently "mkpasswd".  This indicates that
the /etc/passwd (and possibly /etc/group) files should be rebuilt.
d mkgroup then, for example, run

ary for domain users.

7295          0 May 25 18:59 .
7295          0 May 25 18:59 ..
7295          0 May 25 19:02 bin
7295          0 May 25 19:01 etc
95         3262 May 25 19:04 insight.ico
7295          0 May 25 19:02 lib
7295         53 Mar 27 13:06 moxa.bat
95         3262 May 25 19:04 moxa.ico
7295          0 Jul 27 10:58 tmp
7295          0 May 25 18:58 usr
7295          0 May 25 18:59 var
```

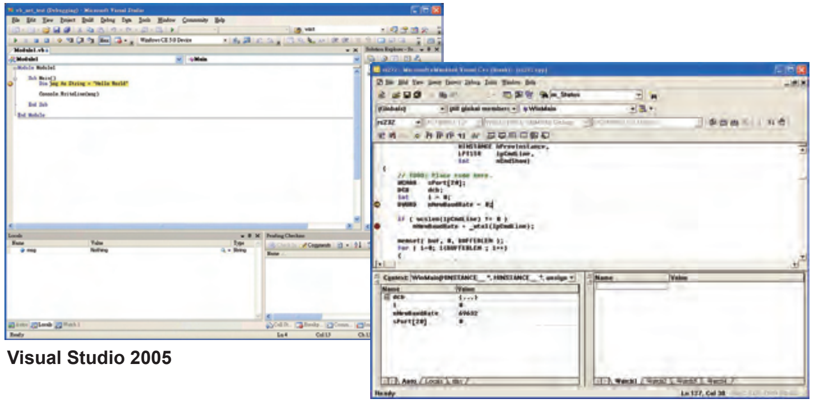
Windows Tool Chain

Insight Debugger

Bash Shell on Windows

Windows CE 5.0 Application Development

MOXA WinCE 5.0 C/C++ APIs	Microsoft Foundation Classes (MFC)
Libraries and Run-Times	Microsoft .NET Compact Framework 2.0
OM/DCOM, and ATL	XML and SOAP Toolkit
Winsock 2.2	On-Line Source Code Debugging



Visual Studio 2005

Embedded Visual C++ 4.0

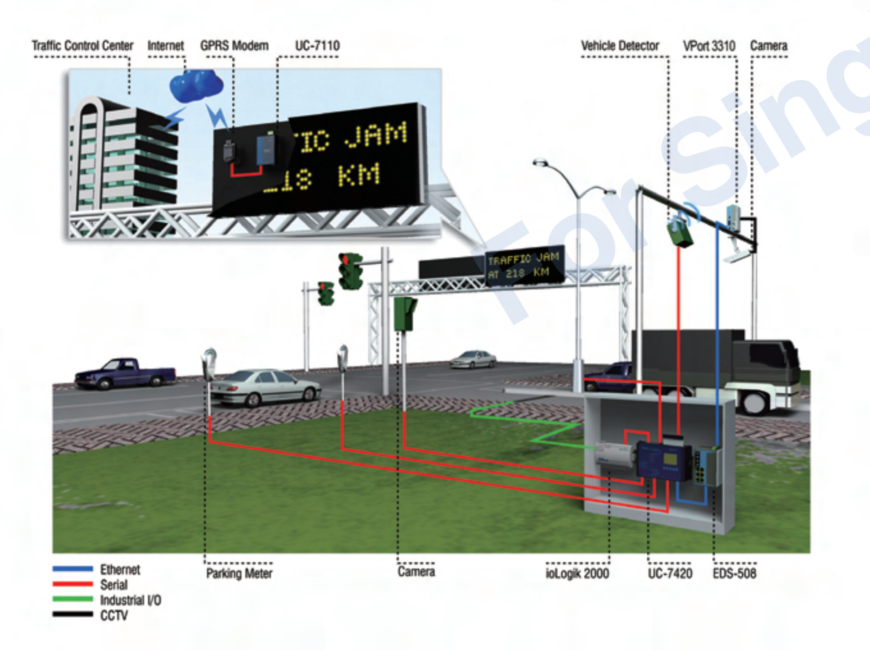
Intelligent Transportation System

Automatic Monitoring and Control of Traffic

Overview

Intelligent Transportation Systems (ITS) are designed to improve both safety and efficiency. For example, it is becoming more common to use automatic surveillance and network communication to reduce traffic jams at busy intersections. IP cameras are used to allow human operators to gauge the number of cars waiting at the intersection, and then UC-7420, MOXA's 8-port embedded computer, transmits the images over the Internet from the intersection to a remote monitoring center. The UC-7420 can also be used to transmit signals that control the status of each traffic light to the central command center.

Another option is to use sensors that automatically detect which parking spaces are occupied and which spaces are empty. Connecting the sensors to a UC-7420 through an RS-485 network and then programming the UC-7420 to monitor the sensors continuously gives parking lot managers the ability keep track of which spaces are unoccupied. When a car leaves a space, this information is relayed to a central computer over an Ethernet LAN or 802.11 wireless LAN. More sophisticated systems use LED displays, which can be connected to the UC-7420, to notify drivers which parking spaces are empty.



Benefits

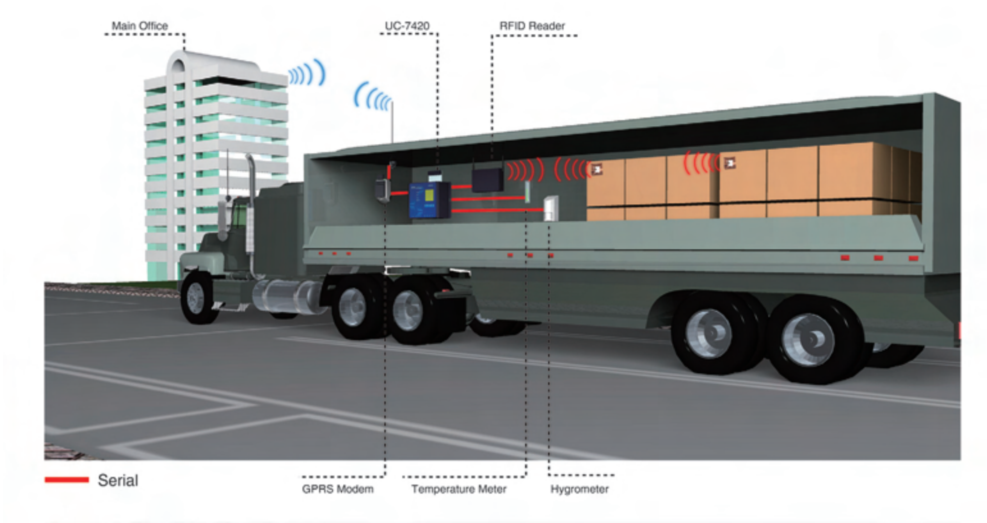
1. CompactFlash slot for data logging
2. Multiple connection options for greater networking versatility
3. PCMCIA slot for wireless network card
4. OpenVPN feature for a secure system

RFID for Logistics System

Instant Tracking System for Logistics Management

Overview

Inventory management is an important aspect of express delivery systems. In the past, human beings were the main tool used to collect and disperse inventory data. The introduction of the barcode helped make inventory management more accurate, but human beings were still needed to operate the barcode readers. As a result, inventory management was still very time-consuming. The UC-7420 can be used as a front-end controller in an RFID logistics system. In this case, an RFID reader, the UC-7420 embedded computer, and a satellite modem are installed in each delivery truck. The RFID reader and satellite modem are both connected to the UC-7420, and an RFID tag is attached to each package. This type of system can be used to send real-time information of the location of each package back to the main office. This type of RFID logistics system is very powerful, since the location of a package can be tracked, even if the package is transferred from one truck to another.



Benefits

1. Reliable and compact
2. Data buffering and logging
3. Low power consumption
4. Programmability facilitates RFID tracking system

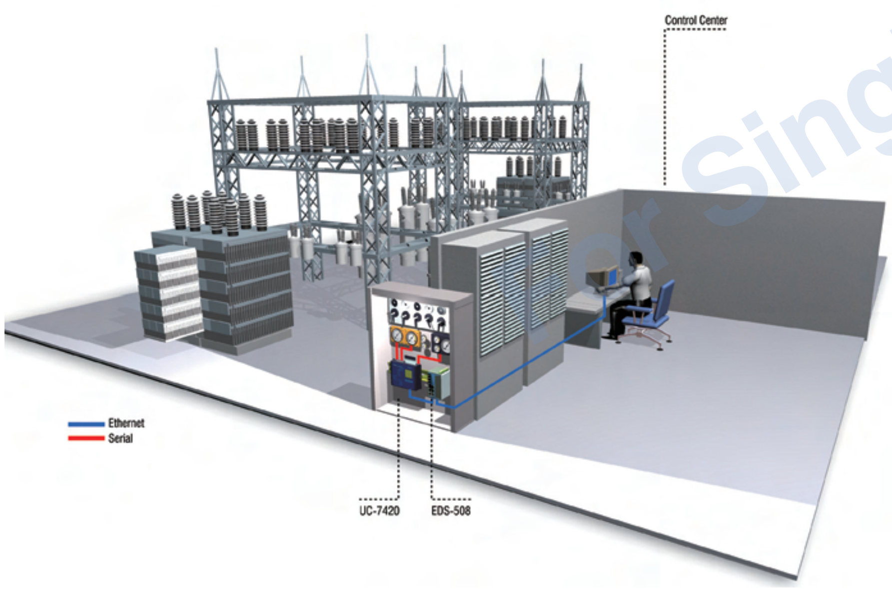
Power Management System

Bringing Reliability and Localized Computing Power to Substation Monitoring

Overview

High-tech power companies around the world are conducting research to identify economical ways to simplify a power plant's automatic protection and warning system, but without sacrificing reliability. One of the main requirements of such a system is a computing device that can handle protocol conversion, data acquisition, monitoring, and control. MOXA's embedded computers are front-end embedded computers that come with 8 RS-232/422/485 serial ports, dual Ethernet ports, wireless LAN capability, and an industrial strength no fan, no hard drive design that suit these requirements exactly.

The built-in operating system makes it easy to install software, and the Flash expansion slot lets users add additional memory space as needed. The dual Ethernet ports of MOXA's embedded computers provide redundancy for critical systems, ensuring that the embedded computer will still be able to communicate with each protection device and with the backup host if the network fails.



Benefits

1. No fan, no hard drive design for longer MTBF
2. CompactFlash for data logging
3. Dual-LAN ports for setting up super-redundant system
4. Programmability facilitates protocol conversion

Power Management System

Remote Monitoring of Solar Power Meters Over the Internet

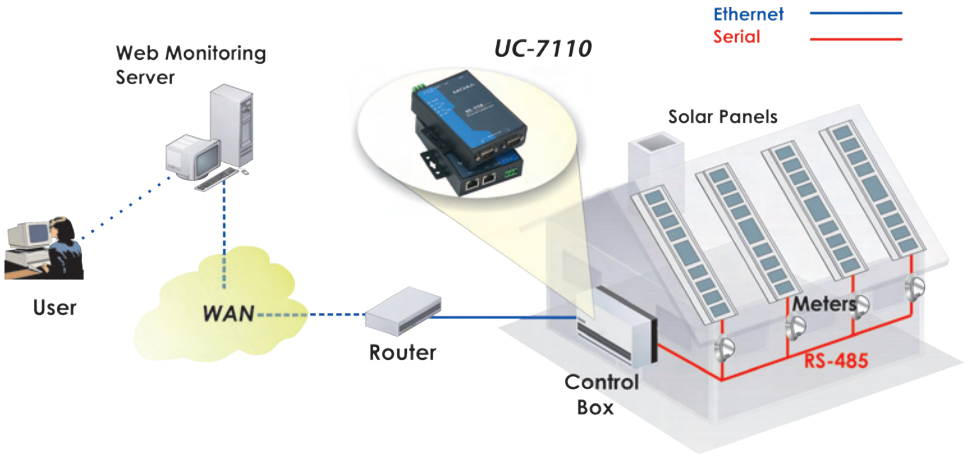
Overview

As the world's population continues to grow and more factories are built, it becomes more and more important to provide sufficient power in an environmentally sustainable way. The solar power solution has received much publicity and backing from environmental enthusiasts, and is beginning to enter the mainstream.

In solar power systems, rooftop solar panels are used to absorb the Sun's energy and convert it into electrical energy. The electrical energy is sent to a control box using RS-485 serial wires and is monitored by a power meter. Energy providers are looking for an Internet solution for more efficient and flexible management and monitoring of their renewable energy systems. For this type of application, a programmable serial-to-Ethernet communication gateway is needed to convert RS-485 serial data into a format suitable for transmission over the Ethernet.

MOXA's UC-7110 offers an economical and resourceful solution for routing serial data to an existing Ethernet network. Solution providers can embed their own monitoring and protocol conversion software into the UC-7110 to monitor power generation and consumption data.

As a front-end controller, the UC-7110 is conveniently sized and includes customized programming options to convert power meter data into Ethernet packet format. The UC-7110 can be used in place of a PC, significantly reducing costs for solution providers, and its small size gives system managers added installation flexibility.



Benefits

1. Adapts easily to an RS-485 network without requiring cabling of existing structure
2. Includes intuitive BSD-style API for easier programming
3. Replaces front-end PC for significant reduction in maintenance costs
4. Shortens application development time through rich API library support
5. Enables fast time to market by using existing hardware and software design