PRODUCTS IN FOCUS

• SENSOR TECHNOLOGY
• INTERNET OF THINGS
• ROBOTICS
• INTERCONNECTIONS
• MACHINE VISION
• WIRELESS TECHNOLOGY
• EMBEDDED SOFTWARE
• SECURITY
Design With The Best

FREE SHIPPING
ON $50+ USD

0800 587 0991
DIGIKEY.CO.UK

6.8 MILLION+ PRODUCTS ONLINE | 750+ INDUSTRY-LEADING SUPPLIERS | 100% FRANCHISED DISTRIBUTOR

* A shipping charge of £12.00 will be billed on all orders of less than £33.00. A shipping charge of $18.00 USD will be billed on all orders of less than $50.00 USD. All orders are shipped via UPS, Federal Express, or DHL for delivery within 1-3 days (dependent on final destination). No handling fees. All prices are in British pound sterling or United States dollar. Digi-Key is a franchised distributor for all supplier partners. New products added daily. Digi-Key and Digi-Key Electronics are registered trademarks of Digi-Key Electronics in the U.S. and other countries. © 2018 Digi-Key Electronics, 701 Brooks Ave. South, Thief River Falls, MN 56701, USA.
Comment

Embedded World, Embedded Vision

Machine vision looks set to open up new areas of application as it migrates from PC-based to embedded systems.

At this year’s Embedded World one area of real interest appears to be in embedded vision. Images can now be processed on compact, very powerful computer platforms that consume very little energy and, as a result, the technology is opening up new areas of application that could not be covered previously by either PC-based or intelligent image processing (machine vision) systems.

At this year’s Embedded World the topic takes centre stage with Bosch, Qualcomm and Arrow, among others, coming together to discuss the migration from PC-based to embedded systems and the potential of this technology as well as its uses and challenges.

“Autonomous driving is currently one of the major trends. Self-driving cars and many other innovations are being made possible thanks to camera-based security systems. The opportunities offered by these “embedded vision” systems are many and various,” says Dr Olaf Munkelt, Chairman of the Board of the VDMA Machine Vision Group.

Beyond self-driving embedded vision is seen as opening up new areas of application for the machine vision industry, whether in the factory of the future, in retail trade or the consumer or medical sectors.

While it may have been used in industrial automation systems to improve production quality and throughput for some time, it’s true to say that the biggest advancement in machine vision has been in processing power.

At a time when processor performance is doubling every two years and there is a continued focus on parallel processing technologies like multicore CPUs and FPGAs, vision system designers are now able to apply highly sophisticated algorithms to create more intelligent systems.

This increase in performance is helping designers not only to acquire images faster but also process and make decisions based on visual data faster than ever before.

As more vision systems look to use the latest generations of multicore CPUs and powerful FPGAs, designer engineers will need to be able to better understand the benefits and trade-offs of using these processing elements.

Neil Tyler
Editor, New Electronics
WHAT.
6.8 MILLION+ PRODUCTS ONLINE
WHEN.
99% OF ORDERS SHIPPED SAME DAY
WHERE.
WHEREVER YOU NEED IT

*A shipping charge of £12.00 will be billed on all orders of less than £33.00. A shipping charge of $19.00 USD will be billed on all orders of less than $50.00 USD. All orders are shipped via UPS, Federal Express, or DHL, for delivery within 1–3 days (dependent on final destination). No handling fees. All prices are in British pound sterling or United States dollar. Digi-Key is a franchised distributor for all supplier partners. New products added daily. Digi-Key and Digi-Key Electronics are registered trademarks of Digi-Key Electronics in the U.S. and other countries. © 2018 Digi-Key Electronics, 701 Brooks Ave. South, Thief River Falls, MN 56701, USA.
Mentor, a Siemens Business, is a technology leader in electronic design automation (EDA), providing software and hardware design solutions that enable companies to develop better electronic and mechanical products faster and more cost-effectively.

The company offers innovative products and solutions that help engineers overcome the design challenges they face in the increasingly complex worlds of board and chip design.

Mentor, a Siemens Business has the broadest industry portfolio of best-in-class products and is the only EDA company with an embedded software solution.

Services
Design-Through-Manufacturing PCB Systems Development Mechanical Analysis Functional Verification Design to Silicon

New and Emerging Products
Electrical System and Harness Engineering Electronic System Level (ESL) Design Embedded Systems Design

Contact details
Mentor, a Siemens Business Rivergate Newbury Business Park London Road Berkshire RG14 2QB tel: +44 (0)1635 811411

www.mentor.com

Embedded Software

IoT framework breakthrough
Mentor announces an Industry 4.0 breakthrough with new IoT framework

Manufacturers building Industry 4.0 smart devices are realising a harsh reality: implementing cloud backend services down to the end node is a complex and expensive endeavour. Further, Industry 4.0 implementations, to be cost effective, must offer a high degree of device interoperability, scalability and portability across changing or unknown cloud backends.

To address these challenges, Mentor has introduced the Mentor Embedded IoT Framework (MEIF) — the industry’s first comprehensive, cloud vendor-agnostic embedded software framework (see Figure 1). Featuring well-defined interfaces engineered to extend a cloud vendor software development kit (SDK), MEIF streamlines the integration of Industry 4.0 networks by complementing leading cloud providers such as Amazon Web Services (AWS), Eclipse IoT, Microsoft Azure, and Siemens MindSphere. MEIF is OS-agnostic, which means it supports any processor architecture and scales from resource-constrained end nodes up to IoT gateways/devices powered by multicore processors.

Enhanced communications from cloud backend to end node, Mentor’s offering supports a breadth of services to enable successful device management (Figure 2). This includes authentication and provisioning; configuration and control; monitoring and diagnostics; and software updates and maintenance. The framework also features advanced capabilities to help manufacturers manage the reliability and overall quality of Industry 4.0 devices. MEIF is extensible so manufacturers can integrate and enable their own diagnostics as well.

Security from the bottom up
MEIF incorporates the Mentor Embedded runtime platforms, which support security from device power-on with a hardware-based root of trust and a complete software chain of trust. Additionally, MEIF includes a GUI-based utility to sign, encrypt, and package artefacts which are then delivered to the devices where they can be securely validated and authenticated.

The new Mentor Embedded IoT Framework for Industry 4.0 addresses a host of common challenges associated with security, portability, inter-operability, and cloud vendor lock-in.

• For more information on this complete solution, visit https://www.mentor.com/embedded-software/iot-framework

www.newelectronics.co.uk

www.digikey.co.uk
Modular connectivity

Pluggable spring clamp terminal blocks for DIN rail-mounted devices in the manufacturing sector

Process flows in the manufacturing sector often use controllers which mount on a DIN rail. These configurable control systems are designed to carry out multiple safety or monitoring measurements at machine or system level. Often, the controls allow a modular upgrade so they can be adjusted to the requirements and the size of the machine. This requires a modular connectivity that METZ CONNECT is providing with its U-Contact range of PCB level connectors.

Connection technology

For decades, screw type terminal blocks have been the connection of choice for rail-mounted devices in building and industrial automation applications. Nowadays, device manufacturers are moving towards spring clamp technology connectors. The push-in technology of these connectors is user-friendly, offering a fast and tool-free cable connection. Installer experience in the field has shown that wiring installation times can be reduced by up to 50% when using Spring connectors with Push-in Technology in comparison to the traditional screw-type technology. Furthermore, the Spring clamp technology offers permanent contact security to the conductor particularly in environments where vibration is present. The solution: the SP99 by METZ CONNECT.

The perfect spring clamp terminal block

Besides the general benefits of this terminal block such as contact security (maintenance free connection), permanent conductor contact, rapid connection by push-in technology, SP99 offers additional benefits for the manufacturing sector: Industrial automation often needs to connect an electrical potential to process signals. And the SP99 is offering two potential connections per pole with a maximum diameter of 2 x 2.5mm. Downtime in a manufacturing system is expensive, therefore a quick fix should be provided when a malfunction occurs. For a general prevention of shortfalls, a systematic check of the different sectors of the system is necessary. Ideally, each wire can be released separately at the rail-mounted device. The SP99 allows for separate release of each wire with a pushbutton actuator for each cable entry and the 90° wire entry angle guarantee a user friendly experience. SP99 is a pluggable solution and therefore ideally suited for multiple quick connect and disconnect cycles.

To avoid misaligned connections and ultimately device or system damage, METZ CONNECT offers additional mechanical coding options for SP99: coding pins are inserted into the respective notches of the terminal block and the respective pin header to guarantee correct connections are made every time.

Product range

U|Contact: Connection systems for Printed Circuit Boards. Spring, screw and IDC type terminal blocks, board-to-board connectors, pin headers, USB, RJ12, RJ45 jacks and M12 Ethernet connectors.
P|Cabling: Copper and fibre optic structured cabling network solutions.

Standards and certifications

METZ CONNECT products are certified by: UL, SEV, CSA, CCA, DIN EN ISO 9001:2008, RoHS

Industries served

Industrial automation and electronics, building automation controls, data and communication systems.

Contact

METZ CONNECT GmbH
Im Tal 2
78176 Blumberg
Germany
Email (sales): rmacdougall@metz-connect.com
The digital age allows us to communicate in ways we have not previously been able to. This has been very empowering; the internet, for example, would not exist; but the digital age also poses new threats which electronic based system designers have to respond to.

How is security being addressed and what’s its positioning within electronic product design specification?

An understanding of locks and keys and the need to protect what is important or valuable to us is gained at an early age; it is part of our general education. Securing property is a familiar concept. It seems all the more surprising therefore, when reviewing requirements for electronic products, that security is often not featured within specifications.

One possible explanation is the need for security is taken for granted. A housebuilder, for example, would expect to fit a front door lock and the house-buyer would not necessarily check it is in the house specification. In that sense it is a ‘given’ but one that needs a very high level of attention.

Questions such as who should fit the locks and who should have the keys emerge; and, one fundamental question when considering each
instance, ‘What needs protecting and why?’

Before answering that question there are three very basic definitions when it comes to security:

**Security:** A thing that guards or guarantees a particular state. It provides a secure condition.

**Secure:** The description of something that is guarded and protected against attack; reliable and trustworthy. Measures taken to prevent escape.

**Privacy:** Freedom from intrusion or disturbance. The capacity to control how and what information is communicated.

From these definitions, it can be concluded that whilst a product is connected, security and privacy are two different things. Privacy is about the right to desist from or partake in activity including the dissemination of information. Security is required to protect privacy where appropriate, but not solely. Security also covers measures to ensure reliability and safety. One common error is to consider security and privacy as one element and in so doing omit to specify or wrongly specify the security requirements.

This is a key takeaway. When specifying an electronic product design, consider all aspects of the design that need to be held secure, including the requirements for privacy.

Where to begin? Possibly the place to start is to identify ‘the bad guys’. Who are they and what will they want? Will they want to access data? Will they want to cheat a system or will they want to embarrass or damage me? It can be hard to consider these scenarios but in so doing it will simply come down to deciding who is allowed access to what, where to put locks, under what circumstance to raise an alarm and who is allowed to have a key. Complacency and fear both need to be avoided when considering requirements. Too many locks and keys can stop a system being user-friendly and lead inadvertently to complacency. The art is to get the balance right and that will come back to considering the questions posed above.

Developing a security topology can be useful in getting the balance right. In a local network which is closed and locked, for example, security is provided to make it secure and privacy is controlled. Information is, however, transmitted to the internet, and at this point, the network becomes open. The security functions are handed over to the internet protocol handling and this will be okay so long as the privacy of the closed system is operating effectively. In this topology there will be other places where locks may be applied and the possibility of imposing a red-line security wall, through which nothing that has not been vetted can pass and from which nothing can escape.

Designing in security

Selecting the most appropriate topology is no simple task, but is the starting point for designing in security. The aim is to cover four key aspects: confidentiality, integrity, availability and attack response. The topology should highlight points at which security needs to be added in order to assure the four key aspects are covered. The choice of an appropriate gateway, for example, will be required to assure confidentiality. What access will be required, which elements are to be open and which closed and what security checks should be put into place.

Further detailing of the design is necessary to cover the remaining three aspects and decisions as to whether or not to provide security through software or hardware also have to be made. To support integrity, custom designed security chips can be incorporated in the design. These
Selecting the most appropriate topology is no simple task, but is the starting point for designing in security.”

Steve Norman

chips cannot be re-programmed and can be used to implement red-line security. Software algorithms can also be effective but care has to be taken that they cannot be tampered with. Other software techniques such as cross-checking the actions of independent functions and applying check-sums to data blocks and back-ups adds to integrity. Ensuring that a system’s function remains available requires monitoring. Many wireless systems have been subject to ‘Denial of Service’ (DoS) attacks, and techniques such as checking the signal-to-noise ratios, limiting numbers of requests and checking for bad data have been developed to deal with such attacks. Furthermore, if the system is to monitor for attacks, decisions will need to be made about how to deal with them. Wiping memory or locking down functions may seem like overkill, but may be necessary. As in real-life, sometimes having locks and keys is just not enough and the overall system requirement and design has to be robust enough to cater for this.

The Renesas Synergy Platform has been designed with security in mind. Built on highly scalable ARM Cortex-M microcontrollers, Synergy provides a complete embedded hardware and software platform, including the qualified, production-grade Synergy Software Package (SSP) for guaranteed operation, which is fully integrated and maintained. Additionally, designers can write their applications at the package API level, meaning time traditionally spent on repetitive, non-differentiated low-level coding can be spent on adding differentiated features.

Synergy microcontroller devices (referred to by their family names S1 (low power), S3 (high efficiency), S5 (high integration) and S7 (high performance), see the figure above) with in-built hardware encryption algorithms required for generating locks and keys, are available as are functions to ensure the integrity of data within the supplied system. The availability of these facilities means that the embedded system designer can more easily incorporate the necessary security features from the beginning, and is not left with the difficult task of trying to ‘add-in’ security to a fundamentally un-secure architecture.

The most important point for an embedded engineer is to design-in security from the start. Retrofitting security is unlikely to be as effective. The end goal can only be reached once a system is proven as ‘Launch Ready’. Evaluating the security of the system is a part of this process but more generally the designer must consider the overall confidence level and the evidence that backs this up. Using a platform such as Synergy, from Renesas, means that designers can gain momentum through ‘buying in’ functionality rather than looking to develop it all themselves.

Author details: Dr Valerie Lynch is CEO of AND Technology Research & Steve Norman Manager, Global Ecosystems at Renesas Electronics

You can learn more about Renesas Synergy strategies and tools for addressing security in your design by visiting https://www.renesas.com/en-us/products/synergy/security.html.
Thermal Management

Protection against thermal runaway

Thermal runaway is a growing threat that's poorly managed, but Schurter has a solution to hand.

A thermal runaway is an increasing threat to electronic devices where more and more power is packed in ever smaller spaces; it is a threat that is poorly dealt with using traditional means. SMD thermal fuses offer a solution that can be reflow-soldered at 260°C and still open at 210°C.

What is meant by a thermal runaway or the thermal damage of power semiconductors: A thermal runaway refers to the overheating of a technical apparatus due to a self-reinforcing process that generates heat. This damage usually causes the destruction of the apparatus and often leads to a fire or explosion.

The causes of a thermal runaway are varied and often random in nature. However, the ever-higher power density in electronic wiring and the trend towards miniaturisation are of particular importance. As more functions are packed in compact modules, which then also have a correspondingly high-power consumption, even slightly excessive currents in power electronics with only a little power loss lead to elevated temperatures of approximately 200°C. Possible consequences: damage or disconnection of surrounding components, damage to the printed circuit board structure or a fire.

With a power semiconductor (e.g. MOSFET) the drain-source transmission resistance increases with rising temperatures, when connected, which results in increasing loss of power in the barrier layer. If the elements are not sufficiently cooled, the power loss output in the form of heat cannot be sufficiently dissipated, which also increases the transmission resistance. This process escalates and ultimately leads to destruction of the component.

How to protect against a short circuit?
The cooling of a system must dissipate at least as much energy as it is supplied with. The overcurrent during a thermal runaway is too low to cause a conventional fuse to trip. Thermal circuit breakers or PTCs would, in principle, be used, but the products available for the assembly of an SMD printed circuit board are too complicated or completely unsuitable.

Solution
SCHURTER have developed and manufactured the RTS Reflow Thermal Switch. The RTS can be reflow soldered @ 260°C after which it is mechanically activated and can still effectively trip at 210°C. The RTS is optimised for standard SMD processes like pick and place other features include:

- High operating current up to 100 A
- High rated voltage 60 VDC (arrow competition is limited to 16 VDC
- Low resistance: 120µOhm
- Very high Breaking Capacity

For further information:
https://uk.schurter.com/content/download/2357131/40537784/file/ApplicationNote_ThermalRunaway_EN.pdf
Machine vision has long been used in industrial automation systems to improve production quality and throughput, but the biggest advancement in machine vision has been processing power. With processor performance doubling every two years and a continued focus on parallel processing technologies like multicore CPUs and FPGAs, vision system designers can now apply highly sophisticated algorithms to create more intelligent systems.

This increase in performance helps designers to acquire images faster but also process them faster. Pre-processing algorithms such as thresholding and filtering or processing algorithms such as pattern matching can execute much more quickly meaning designers are able to make decisions based on visual data faster than ever.

As more vision systems that include the latest generations of multicore CPUs and powerful FPGAs reach the market, vision system designers need to understand the benefits and trade-offs of using these processing elements.

**Inline vs co-processing**

When developing a vision system based on the heterogeneous architecture of a CPU and an FPGA, you need to consider two main use cases: inline and co-processing.

With FPGA co-processing, the FPGA and CPU work together to share the processing load. This architecture is most commonly used with GigE Vision and USB3 Vision cameras because their acquisition logic is best implemented using a CPU. You acquire the image using the CPU and then send it to the FPGA via direct memory access (DMA) so the FPGA can perform operations such as filtering or colour plane extraction. Then you can send the image back to the CPU for more advanced operations such as optical character recognition (OCR) or pattern matching. In some cases, you can implement all of the processing steps on the FPGA and send only the processing results back to the CPU.

In an inline FPGA processing architecture, you connect the camera interface directly to the pins of the FPGA so the pixels are passed directly to the FPGA as you send them from the camera. This architecture is commonly used with Camera Link cameras because their acquisition logic is easily implemented using the digital circuitry on the FPGA. This architecture has two main benefits. First, you can use inline processing to move some of the work from the CPU to the FPGA by performing pre-processing functions on the FPGA. This reduces the amount of data that the CPU must process because it implements logic to only capture the pixels from regions of interest, which increases overall system throughput. The second benefit of this architecture is that it allows for high-speed control operations to occur directly within the FPGA without using the CPU.

**Vision algorithms**

With a basic understanding of the different ways to architect heterogeneous vision systems, you can look at the best algorithms to run on the FPGA. First, you should understand how CPUs and FPGAs operate. Consider a theoretical algorithm that performs four different operations on an image and examine how each of these operations runs when implemented on a CPU and an FPGA.

CPUs perform operations in sequence, so the first operation must run on the entire image before the
second one can start. In this example, assume that each step in the algorithm takes 6ms to run on the CPU; the total processing time is 24ms.

Because FPGAs are massively parallel in nature, each of the four operations, when running the same algorithm can operate on different pixels in the image at the same time. This means the amount of time to process the entire image is 4ms, so total processing time is 6ms.

Even if you use an FPGA co-processing architecture and transfer the image to and from the CPU, the overall processing time is much shorter than using the CPU alone.

In a real-world example you will apply a convolution filter to sharpen the image. You then run the image through a threshold to produce a binary image – this reduces the amount of data in the image by converting it from 8-bit monochrome to binary but also prepares the image for binary morphology. The last step is to use morphology to apply the close function. This removes any holes in the binary particles.

If you execute this algorithm only on the CPU, it has to complete the convolution step on the entire image before the threshold step can begin and so on. This takes 166.7ms when using the NI Vision Development Module for LabVIEW and the cRIO-9068 CompactRIO Controller based on a Xilinx Zynq-7020 All Programmable SoC, but if you run this same algorithm on the FPGA, you can execute every step in parallel as each pixel completes the previous step reducing the time to complete to just 8ms. In some applications, you may need to send the processed image back to the CPU for use in other parts of the application.

Factoring in time for that, this entire process takes only 8.5ms.

Though the FPGA has benefits for vision processing over CPUs, those benefits come with trade-offs. For example, FPGA clock rates are on the order of 100MHz to 200MHz, significantly lower than those of a CPU. Therefore, if an application requires an image processing algorithm that must run iteratively and cannot take advantage of the parallelism of an FPGA, a CPU can process it faster. In the previous example each of the processing steps operates on individual pixels, so the algorithm...
can take advantage of the massive parallelism of the FPGA to process the images. However, if the algorithm uses processing steps such as pattern matching and OCR, which require the entire image to be analysed at once, the FPGA struggles to outperform.

Overcoming complexity

The advantages of an FPGA for image processing depend on each use case, including the specific algorithms applied, latency or jitter requirements, I/O synchronization, and power utilization. Often using an architecture featuring both an FPGA and a CPU presents the best of both worlds.

The problem with an FPGA-based vision system is overcoming the programming complexity of FPGAs. Vision algorithm development is, by its very nature, an iterative process, you need to determine not which approach works but which approach works best, and “best” is different from application to application. For some applications, speed is paramount. In others, it’s accuracy so you need to try a few different approaches to find the best one for any specific application.

To maximise productivity, you need to get immediate feedback and benchmarking information on your algorithms regardless of the processing platform you are using. Seeing algorithm results in real time is a huge time-saver when you are using an iterative exploratory approach and having the ability to make changes and see the results quickly is key. However, the traditional approach to FPGA development can slow down innovation due to the compilation times required between each design change of the algorithm. One way to overcome this is to use an algorithm development tool that helps you develop for both CPUs and FPGAs from the same environment while not getting bogged down in FPGA compilation times.

The Vision Assistant from NI is an algorithm engineering tool that simplifies vision system design by helping you develop algorithms for deployment on either the CPU or FPGA. You also can use it to test the algorithm before compiling and running it on the target hardware while easily accessing throughput and resource utilisation information.

When considering whether a CPU or an FPGA is best for image processing, the answer is, “It depends.” You need to understand the goals of your application and use the processing element that is best suited to that design.

However, regardless of your application, CPU- and FPGA-based architectures and their many inherent benefits are poised to take machine vision applications to the next level.
10 MAY 2018
NATIONAL MOTORCYCLE MUSEUM, BIRMINGHAM

PCB DESIGN & MANUFACTURING LIVE

UK’s dedicated exhibition for sourcing the electronic components & services needed to develop your PCB design

WHY VISIT?

INNOVATIVE NEW SOLUTIONS
Solve your PCB design problems by connecting with market leading UK suppliers

NETWORK WITH PCB EXPERTS
Speak to PCB Design Consultancies & Electronic Manufacturers and save time and money on your designs

ATTEND TECHNICAL SEMINARS
Learn new techniques and discover technologies to improve your PCB design skills

Take a tour of the world’s largest collection of British motorcycles

Register for FREE to attend at www.pcbdmlive.co.uk
In Stock.
On Your Doorstep.
48 Hours.*

Free Shipping on Orders Over £33 or $50 USD*