EIU

ELECTRONICS INFORMATION UPDATE

A Mouser Magazine

EUROPE | MAY 2022

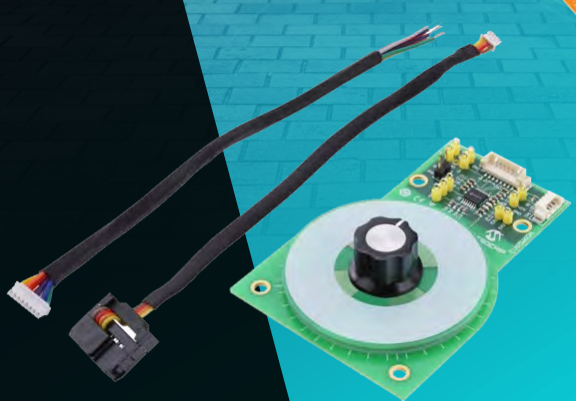
mouser.com

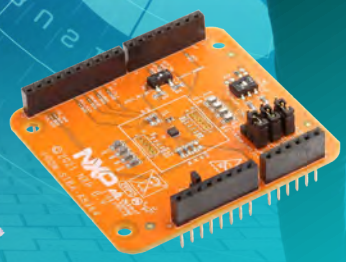
SENSE-ATIONAL!!

FEATURES

PLUS

REGULARS





Cover image credit: metamorworks/Shutterstock.com

EIU
ELECTRONICS INFORMATION UPDATE

mouser.com

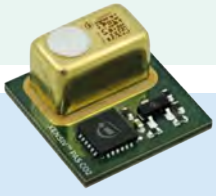
In this issue...

It all begins with a sensor, so our May issue presents articles on: Improving Indoor Air Quality; ToF System Design: Technology for Healthy Living; and 3D Hall sensors for precise, RT positioning.

We start a NEW six part series showcasing University Projects and continue our series on MCUs and on Motors. David Pike proves again he is the Connector Geek and Martin Hill spotlights sensors in T&M. Tech Tips considers the IoT Machine Authentication Dilemma. Plus a news round-up, Dev Kit Pick and, of course, a review of the most innovative products now in stock at Mouser. Now read on...

Published by Mouser Electronics.
For Editorial contact Nick Foot at *nick.foot@bwwcomms.com*.

For Advertising, contact Claudia Bertaccini at *claudia.bertaccini@mouser.com.*



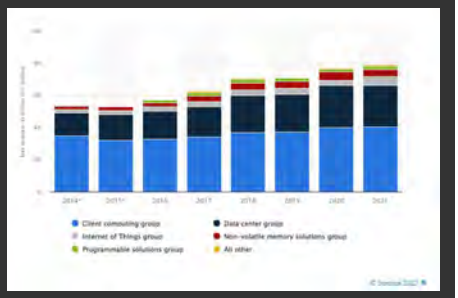
Intel's €80B EU Plan

Intel will invest as much as 80 billion euros in the European Union (EU) over the next decade in semiconductor-related technologies ranging from R&D to state-of-the art packaging solutions. Included are an initial 17 billion euros for a leading-edge semiconductor fab mega-site in Germany, a new R&D and design hub in France, and R&D, plus manufacturing and foundry services in Ireland, Italy, Poland and Spain. With the intent to create a next-generation European chip ecosystem and a more balanced and resilient supply chain, the planned investments along with the EU Chips Act will empower private companies and governments to advance Europe's position in the semiconductor sector.

The investment program is centered around balancing the global semiconductor supply chain with a major expansion of Intel's production capacities in Europe. In the initial phase, Intel plans to develop two first-of-their-kind semiconductor fabs in Magdeburg, Germany, the capital of Saxony-Anhalt. Construction is expected to begin in the first half of 2023 with production planned to come online in 2027. The new fabs are expected to deliver chips using Intel's most advanced, Angstrom-era transistor technologies as part of the company's IDM (integrated device manufacturer) 2.0 strategy.

In the expansion project at Leixlip in Ireland, Intel plans to spend an additional 12 billion euros doubling the manufacturing space and foundry services. This expansion will eventually bring Intel's total investment in Ireland to more than 30 billion euros. In Italy, Intel may develop a back-end manufacturing facility with an investment of up to 4.5 billion euros, creating approximately 1,500 Intel jobs plus an additional 3,500 jobs across suppliers and partners. This would be in addition to its planned acquisition of Tower Semiconductor, which has a partnership with STMicroelectronics, which has a fab in Agrate Brianza, Italy.

In total, Intel plans to spend more than 33 billion euros on these manufacturing investments.



Around Plateau de Saclay, France, Intel plans to build its new European R&D hub, creating 1,000 new high-tech jobs at Intel, with 450 jobs available by the end of 2024. In addition, Intel plans to establish its main European foundry design center in France. In Gdansk, Poland, Intel is increasing its lab space by 50%, and is expected to be completed in 2023. Intel is also developing partnerships in Italy with Leonardo, INFN and CINECA. In Spain, the Barcelona Supercomputing Center and Intel have been collaborating on exascale architecture, and are now developing zettascale architecture for the next decade. The supercomputing center and Intel plan to establish joint labs in Barcelona.

EU President Ursula von der Leyen commented: "With the EU Chips Act, we want to make Europe is a leader in global semiconductor production. And we also want to strengthen our resilience, with home-grown, secure technologies, which are invaluable assets in the turbulent world we live in. Our goal is to have 20% of the world's microchips produced in Europe, by 2030. That's twice as much as today, in a market that is set to double in the next decade."

"More than 43 billion euros of public investment, both EU and national investments, will support the EU Chips Act until 2030. It will make Europe a more attractive place for tech companies to invest in cutting-edge chips development and production. This is why I see today's announcement by Intel as a first major achievement under the EU Chips Act. It is a considerable contribution to the European Chips ecosystem that we are building right now. It will create new, well-paid jobs throughout Europe. And I'm sure that it will pave the way for more companies to follow suit."

Wireless BMS gets Top Auto Cybersecurity Pass

Analog Devices has announced that its Wireless Battery Management System (wBMS) is certified to ISO/SAE 21434, the new standard for cybersecurity risk management. TÜV NORD Mobilität, the assessor for this qualification, affirmed that ADI's wBMS is the first automotive system that it has certified for ISO/SAE 21434. The assessment confirmed that ADI performed appropriate assurance measures within the product development to fulfill the CAL 4 requirements.

"We conducted an intensive assessment to verify that ADI's wBMS conforms to ISO/SAE 21434 requirements. With ADI considering the CAL 4 classification conditions throughout product development, the cybersecurity assurance measures complied with the highest requirements," said Leif-Erik Schulte, Senior Vice President at TÜV NORD Mobilität. "This system certification is a key element to build trust across the full electrification ecosystem – from energy storage to OEMs to consumers – to support EV adoption and help reduce emissions."

"Personal vehicles are a major contributor to global warming, so accelerated EV adoption plays a critical role in achieving a sustainable future," said Roger Keen, General Manager of Battery Management Systems at Analog Devices. "Improving the security and accuracy of EV batteries removes roadblocks in end-users' buying considerations and advances OEMs' decisions to expand their EV offerings. With this certification, ADI can provide ongoing transparency and seamless deployment within the EV battery supply chain to progress our vision of a greener world. It further accelerates the speed to market for our customers by saving their cybersecurity development time and associated infrastructure investment."

www.analog.com

The Future of Improving Indoor Air Quality

By Philipp Seidel, Project Leader Marketing & Communications, Sensirion AG

When we think of "air quality", we tend to think of air pollution in the regions surrounding our homes. We rely on measures such as the Air Quality Index to let us know when airborne pollutants in our towns or cities reach levels that may cause or exacerbate health issues. When summer humidity brings an increased risk for asthma sufferers or when dangerous smog accumulates in cities, the message is simple: to protect your health, stay indoors.

However, some of the most polluted air we breathe is found indoors. From dust to formaldehyde to volatile organic compounds (VOCs), unseen elements and particulate matter inside our homes and offices can cause both short- and long-term health issues.Given that Americans spend about 90% of their time indoors, measuring and controlling indoor air quality should be a top priority.

With a growing body of research pointing to a link between virus infection risks and CO_2 concentrations as well as low humidity and/or high levels of pollution, being able to control and monitor these variables is more important than ever. In this article, we explore the causes of indoor air pollution, the steps we can take to improve indoor air quality, and, importantly, the future possibilities for improving indoor air quality in every home.

The causes and effects of indoor air pollution

Indoor air pollution can come from many sources. Some, such as fuel-burning appliances and indoor smoking, are relatively obvious. Others are not as readily apparent. Building materials including plywood, adhesives, and insulation – all found throughout the home – can also be sources of formaldehyde, benzene, and a host of other VOCs. Even some cleaning products, such as detergents and shampoos, can contain formaldehyde.

When it comes to pollution, enclosed spaces can be dangerous. Poor ventilation inside homes means that hazardous gases and airborne pollutants of all kinds can accumulate easily and hang around for long periods.

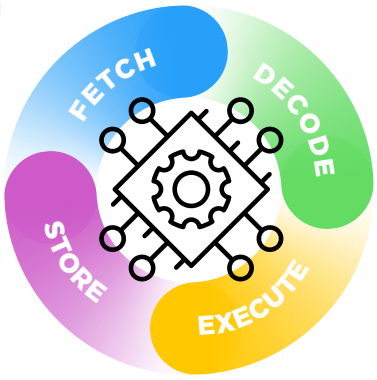
Low levels of ventilation combined with poorly sealed foundations, in particular, can also lead to the accumulation of radon, a hazardous radioactive gas, inside homes (the amount can vary drastically depending on where you live).

Micro matters

Microcontrollers - spanning a huge capability from 4-bit to 64-bit and beyond - are to be found everywhere. Therefore, we thought it was high time that Mouser's Electronics Information Update presented a series of articles looking at the MCU in detail, considering architectures, operation, selection, OS and tools. In the opening chapter, Adam Taylor, Founder and Principal Consultant at Adiuvo Engineering and visiting professor of embedded systems at the University of Lincoln, reminds us of MCU history.

Microcontroller Architecture

In our last article, we examined the development of microcontrollers and a small section of their history which led to the most popular architectures becoming dominant in the embedded world. In this article, we are going to take a deeper look at computer architecture and some of the possible architectural elements we need to understand.



At the core of all microcontroller architectures is the fetch, decode, execute and store cycle. In this cycle, the processor fetches an instruction from RAM and stores it in registers.

The control unit decodes the instruction, which is then executed by the Algorithmic Logic Unit (ALU).

Finally, the result of the ALU is written back into memory.

Over the years computer architects have improved upon this basic architecture to increase performance and throughput by introducing techniques such as the following:

Instruction Pipelining – The fetch, decode, execute, and store cycle is wasteful because only one element is being used at a particular time. Pipelining ensures each stage of the fetch, decode, execute, and store cycle is active therefore increasing the throughput because each stage is no longer idle for most of the cycle.

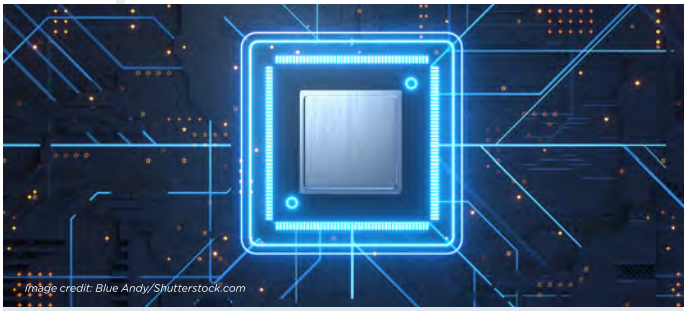


Image credit: Blue Andy/Shutterstock.com

Cache – A major contributor to the processing time is the time taken to access external memory. Cache is on-chip memory that enables very fast access. A cache controller is used to manage the contents of the cache. The cache contains frequently accessed instructions and data. Managing the cache and maintaining cache coherency across multiple cores is the subject of considerable research within computer engineering.

Branch Prediction – Programs executing on the microcontroller either operate sequentially (meaning they execute instructions in order), loop execute instructions in a loop, or branch to execute different instructions depending upon the previous operations or readings from external sensors. Branching is expensive when a branch instruction is detected. The instruction pipeline must be stalled until the branch decision is known. Stalling the pipeline reduces performance so branch prediction makes a predication as to which path of the branch will be taken thereby setting up the pipeline to process the predicted branch.

The pipeline then only must be stalled and flushed if the branch prediction is wrong.

University TECHNOLOGY EXPOSURE

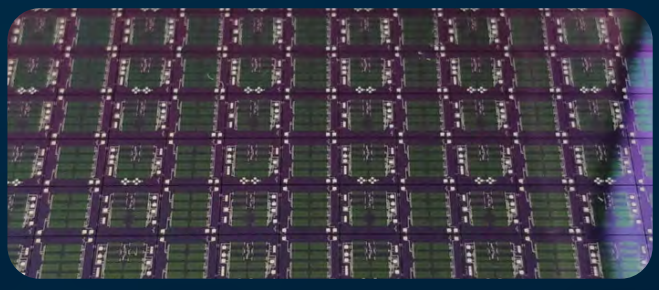
This year, Mouser began a sponsorship of a University Technology Exposure Program with the Wevolver Community. Wevolver aims to empower people to create and innovate by providing access to engineering knowledge. The community provides inspiring, informative content to millions of engineers every month through a number of web and social channels. The University Technology Exposure Program enables students to share their work with the global engineering community and industry.

Mouser has a long history of supporting the University sector (which is detailed here). The Wevolver program will last six months and we will detail submissions in a regular blog in EIU. Readers can vote for their favourite project.

Smart fabrics, turbines, woodpeckers...and much more

#1. Novel circuit design approach makes pressure sensors smaller and more sensitive by Mikhail Basov

Micro-electromechanical systems (MEMS) sensors are miniature devices built by fabricating mechanical and electronic components responsible for carrying out the sensing process on a silicon chip. These devices have the advantage of small size and are widely used in various sectors, including manufacturing industries, biomedical applications, consumer products, and more. Balancing the performance and size of components is one of the main challenges faced by an R&D engineer working in the field of MEMS.



New sensor design and fabrication processes add incremental improvements to the technology, but most sensors have used the classic Wheatstone bridge circuit for more than 50 years. Mikhail proposes a novel circuit design, 'piezo sensitive differential amplifier with negative feedback loop (PDA-NFL)', that aims to significantly improve the sensitivity and reduce the size of the sensor.

Read the full article here.

#2. Small Wind Turbines for sustainable livelihoods by Paul Chris Mwale

The next article relates to a small wind turbine built with locally available resources like timber, scrap metal, junk electronics, and some salvaged parts from automobiles and household items. Paul, the author of the article, explains how he built the blades, generator, and control circuits for a fully functional wind turbine. Details about the blade design, electronic circuits, control algorithm, and the specifications of the developed windmill are explained briefly.

Access the full article from this link.

Tech Tips

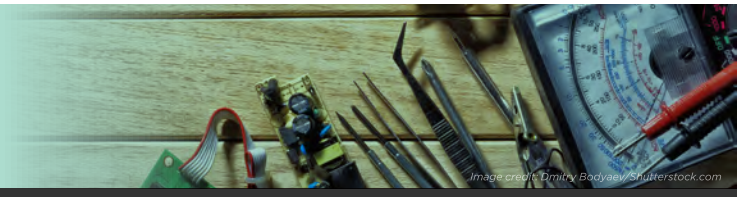


Image credit: Dmitry Bodyaev/Shutterstock.com

The IoT Machine Authentication Dilemma

Image credit: your/Shutterstock.com

By Jon Gabay for Mouser

Most of the time, we're surrounded by dozens of devices that contain connectivity to the world wide web. Whether they are directly part of our inventory or buried in our environment, these devices are in constant contact with anyone savvy enough to detect and connect to them.

In some cases there's less concern, because the information being accessed is less sensitive. If someone hacks into our Fitbit or smartwatch, they get a kick out of knowing our real-time blood pressure and heart rate. In many cases, though, the concern is greater, due to the sensitive nature of the information.

This is because more of our lives depend on devices like phones that hold our contacts and all their sensitive information such as email addresses, locations, passwords, banking, and credit card information. In addition, they can double as remote surveillance with cameras, microphones, and location data.

Identity management is perhaps one of the most critical concerns as our information infrastructure moves forward and evolves.

These concerns include locally and globally accessing devices and governmental, capitalistic, and society-dependent energy, transportation, distribution, and management. If machines can't reliably identify and authenticate themselves, the situation begins to devolve quickly.

Therein lies the problem. The internet was an outgrowth of a data-sharing topology used by Defense Advanced Research Projects Agency (DARPA) and universities to help researchers collaborate. Its protocols were not designed to be secure. As it became a public information exchange network, attempts have been made to encrypt the data payloads. While this can help, the structure of data centers, routers, and switches makes several types of attacks possible. We will look at some of these attacks—and solutions the industry uses to fight back.

Basic Security Concerns

The most basic level of security for the average internet user and device is identity verification and protection. We all use passwords as authentication mechanisms for our emails, apps, and service subscriptions.

These are examples of one-way authentication. The service we are trying to access requests the password. Anyone who knows the password can gain access. Two-way authentication requires users to provide more information. And so on.

Typically, passwords and login information are not encrypted, but this is changing. Several communications apps and messengers advertise end-to-end encryption, which is a good start. This can be applied to handheld mobile devices or embedded and buried IoT devices.

Another level is independent verification. Here, an email program, for example, will contact a cell phone and ask if it is a valid login attempt. It will also notify the account holder to let them know if a login attempt is made on another device. This approach works well if a would-be hacker doesn't have access to all the back channels, but this may not be as feasible for buried IoT devices that typically have just one way of communicating. Even if it has Bluetooth® and Wi-Fi, both will normally use the same access point.

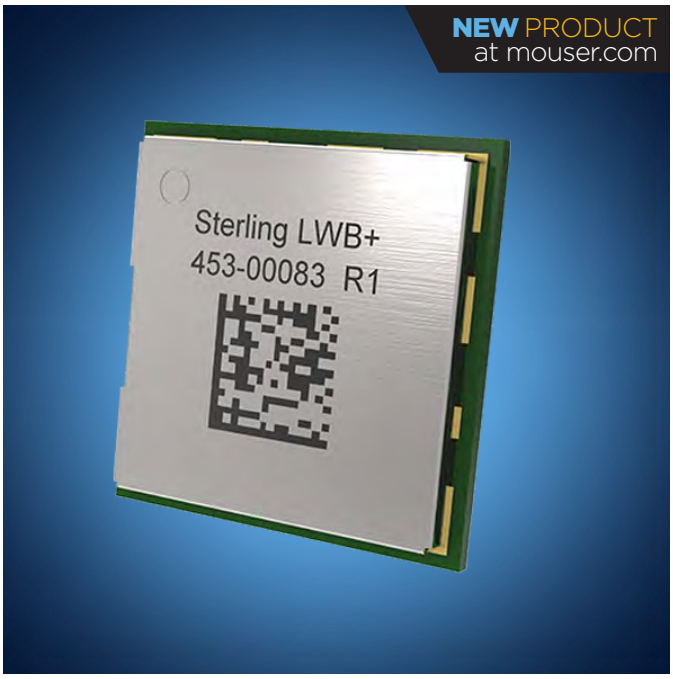
Wi-Fi and BLE connectivity for IoT

Mouser is now stocking the new Sterling-LWB+ modules from Laird Connectivity.

The Wi-Fi 4 (802.11b/g/n) and Bluetooth® 5.2 Low Energy-enabled devices are designed specifically for next-generation IoT products, such as battery-powered medical devices, industrial IoT sensors and rugged handheld devices.

The Laird modules are powered by the Infineon AIROC™ CYW43439 chipset solution, supporting reliable and secure performance in industrial IoT settings, supporting a full industrial temperature range (-40°C to +85°C). Incorporating a fully featured Wi-Fi 4 radio enabled with software drivers and support, the secure, high-performance SDIO solution allows easy integration with any Linux- or Android-based system. The modules are mechanically and pin compatible with the Sterling-LWB module, offering a simplified upgrade path for existing designs.

The Sterling-LWB+ modules support the latest WPA3 security standards, and the devices' integrated power amplifier and low-noise amplifier (LNA) ensure reliable connectivity even in challenging RF environments. The Sterling-LWB+ devices are available with either an on-board chip antenna or a MHF connector for an external antenna, which can connect to range of Laird Connectivity-certified internal antennas.



For development and evaluation, Mouser also stocks the Sterling LWB+ development kit, available with either an on-board chip antenna or a MHF connector. The modules are certified to FCC, ISED, CE, UKCA, RCM, MIC, and Bluetooth SIG registration, further speeding time to market.

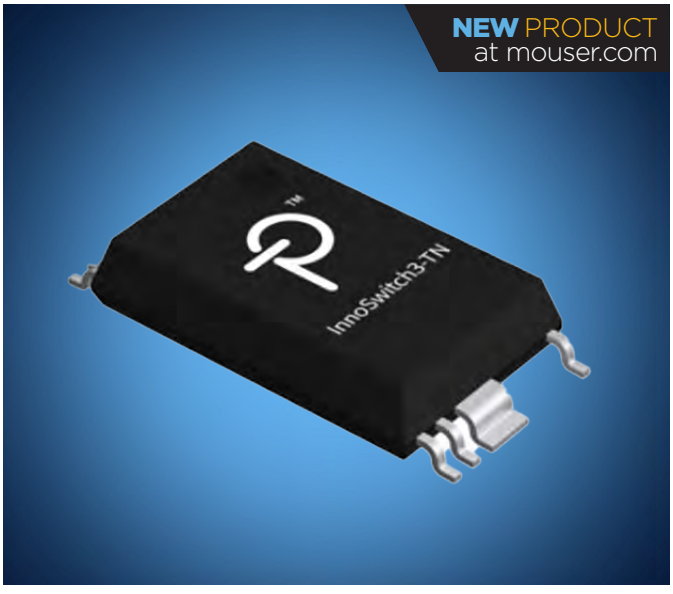
Click for More Information

High efficiency flyback switcher ICs

Now available through Mouser, Power Integrations' InnoSwitch3-TN CV/CC QR flyback switcher ICs are high-efficiency offline ICs with a 725V primary MOSFET, synchronous rectification, and integrated secondary side-control.

The InnoSwitch3-TN ICs dramatically increase the efficiency of auxiliary power supplies used in appliances, consumer products, and industrial applications. Ideal for isolated and non-isolated designs, these advanced flyback controllers can achieve up to 90% full load efficiency, flat efficiency across the load range, and very low no-load consumption. The InnoSwitch3-TN components may be used as an accurate 5V single-output power supply, with two positive rails or with both positive and negative rails.

In the InnoSwitch3-TN CV/CC QR flyback switcher ICs, 725V primary MOSFET and the primary/secondary flyback controllers are coupled using the proprietary FluxLink communications channel. Safety-rated FluxLink communication ensures reliable synchronous rectification and accurate output CV and CC.



Comprehensive safety features include output over-current protection and over-temperature protection. The small MinSOP package and a low number of external components make the InnoSwitch3-TN ICs ideal for compact designs.

Click for More Information