Security in the New Era of IoT Innovations
Horticulture LED Lighting

New horticultural products from the high power ceramic series. Specially chosen wavelengths (450 nm, 660 nm and 730 nm) increase photosynthesis, optimizing plant development and growth. With outstanding PPF-value, small size and low power consumption, the WL-SMDC is the future choice for horticultural lighting. Available ex stock. Samples free of charge.

For further information please visit:
www.we-online.com/leditgrow

For a short introduction of Horticulture LEDs read our Application Note:
www.we-online.com/AN-Horti
The Internet of Things (IoT) is one of the fastest growing technological revolutions the world has ever seen, with billions of devices connected in homes, smart factories, offices and even in remote locations. Yet, as the IoT proliferates, so do the potential access points for the security risks posed by malicious attackers. In the article on page 10, Infineon Technologies and EBV explore some of the implications of security breaches and consider how designers should approach the task of planning and implementing a secured IoT infrastructure.

For more information contact EBV Electrolink, +27 21 402 1940, capetown@ebv.com.

Analog, digital & mixed-signal ICs.......................... 20
Some of the newest and most advanced integrated circuits available to electronics designers.

Enclosures, racks, cabinets & panel products.......................................................... 23
Wall mounting, DIN-rail and general-purpose housings for electronic devices.

Circuit & system protection, EMI/EMC.................... 26
A detailed analysis of electromagnetic interference and compatibility, and a selection of board-level circuit protection components.
The ethics of AI

This year, employees at Google have very publicly protested against the company’s involvement in projects they are concerned about. The first protest was over Project Maven, a programme developed for the US military to speed up analysis of drone footage by automatically classifying images of objects and people. The fallout saw thousands of employees signing a petition and about a dozen resigning, citing ethical concerns over the use of AI (artificial intelligence) technology in drone warfare as well as worries about the company’s political decisions. The outcry ultimately led to Google announcing that it will not seek another contract in that arena.

The latest controversy revolves around Dragonfly, a project to provide China with search and personalised mobile news services that comply with the government’s censorship and surveillance requirements. In a letter to Google management, employees lamented that ‘currently we do not have the information required to make ethically-informed decisions about our work, our projects, and our employment. That the decision to build Dragonfly was made in secret, and progressed even with the AI Principles in place, makes it clear that the Principles alone are not enough. We urgently need more transparency, a seat at the table, and a commitment to clear and open processes: Google employees need to know what we’re building.’

The AI Principles referred to basically comprise a high-level construct equivalent to Isaac Asimov’s famed ‘Three Laws of Robotics’. In a nutshell, the principles Google engineers seek to uphold are that AI should: 1) Be socially beneficial; 2) Avoid creating or reinforcing unfair bias; 3) Be built and tested for safety; 4) Be accountable to people; 5) Incorporate privacy design principles; 6) Uphold high standards of scientific excellence; 7) Be made available for uses that accord with these principles. The Principles also explicitly exclude AI development for technologies that cause or are likely to cause overall harm or personal injury, and technologies that are unfairly used for surveillance.

On the one hand it’s encouraging to see engineers take an ethical stand like this. Far too often I think there is a tendency to just do the engineering and leave the ethics to somebody else. It also says a lot about Google’s company culture that employees feel empowered to take a stand like this, and about the power of social media and the Internet as a medium for them to bring their concerns into the public awareness.

On the other hand maybe ethics shouldn’t be the domain of engineers, or at least their problem. Maybe Google will just go out and find engineers who don’t have the same moral qualms, or are willing to sign away their rights to object when they sign their employment contract. If they were clever about it, they could probably compartmentalise a project’s development in such a way that the components all seem innocent but they are able to be integrated into a nefarious whole. But as we’ve seen time and time again, nowadays it just takes one leak about subterfuge of that kind and the scandal can bring even the biggest company to its knees (or at least give it a solid kick to the shins).

On an emotional level, it gives me a warm fuzzy feeling to see these guys taking a stand. To encourage or accept a culture in which people disengage their work from their ethical concerns is not the kind of world I want to live in. It also bodes well for the future of AI and for oversight of its application, seeing as it has the potential for so much harm.

AI might one day reach the point where the ‘intelligence’ part is indistinguishable from a human’s, but we must make sure the ‘artificial’ part never gets overlooked. We are not artificial, we are the real thing and it is important that we care about ethics and take a stand to protect them.
South Africa

- South Africa has launched a multimillion Rand global project in radio astronomy that will conduct groundbreaking science in astrophysics. To be located at the Square Kilometre Array (SKA) South Africa site in the Karoo, the Hydrogen Intensity and Real-Time Analysis eXperiment (HIRAX) telescope will have important synergies with the 64-dish MeerKAT, the country’s predecessor to the SKA. Jointly funded by the University of KwaZulu-Natal (UKZN) and the Department of Science and Technology (DST) through the National Research Foundation (NRF), HIRAX will be a compact radio telescope array of 1024 six-metre dishes that will map about a third of the sky during its four years of observation.

- Dr Rob Davies, the minister of trade and industry, has dissolved the board of the South African Bureau of Standards (SABS) and placed the entity under the control of three co-administrators. The co-administrators will remain in their position until 30 January 2019 and have been tasked with producing a diagnostic report and a turnaround plan for the entity. The SABS issued a statement assuring that there have been no interruptions to its operations, and that it has an approved business plan in place for 2018/19, has received its first transfer payment from the DTI and is expected to report on organisational performance for each quarter of the year.

Overseas

Business

- Keysight Technologies reported financial results for the third fiscal quarter of 2018 ended 31 July. Revenue grew 2% to reach $1,004 billion, when compared with $832 million last year. Net income was $121 million, or $0.63 per share, compared with a net loss of $18 million, or a loss of $0.10 per share, in the third quarter of 2017.

- Net sales for the first quarter of Microchip Technology’s fiscal 2019 were a record $1,213 billion, up 24.7% from the prior year’s first fiscal quarter. Net income for the first quarter of fiscal 2019 was $35.7 million, or $0.14 per diluted share, down from net income of $170.6 million, or $0.70 per diluted share, in the prior year’s first fiscal quarter. The current year’s net income results were significantly adversely impacted by purchase accounting adjustments associated with the company’s acquisition of Microsemi.

- Analog Devices announced revenue totalling $1,57 billion for its third fiscal quarter of 2018, which is up 4% sequentially and up 10% year-over-year, and earnings per share of $1.10. For the next quarter, the company expects to achieve roughly the same figure in revenue, with earnings per share in the region of $1.07.

Companies

- STMicroelectronics announced its acquisition of software specialist Draupner Graphics. Draupner is the developer and supplier of TouchGFX, a software framework offering outstanding graphics and smooth animations for embedded graphical user interfaces (GUI) with minimal resource requirements and power consumption. Hosted on 32-bit microcontrollers, TouchGFX enables high-end graphics across all devices and systems, including smart home and building automation systems, appliances, wearables, and audio and video systems.

- Digi-Key has expanded its agreement to distribute products from Würth Elektronik eSiSos to include wireless modules. The product range encompasses highly efficient wireless transmission solutions in the Bluetooth or Wireless M-Bus standard as well as proprietary wireless modules in the frequency ranges 169, 433, 868, 915 MHz and 2.4 GHz. Thanks to their low power consumption, these high-quality, compact components are ideal solutions for decentralised IoT and smart metering applications.

- Analog chip vendor Skyworks Solutions has acquired Avnera, a developer of analog systems-on-chip, for $405 million. By adding ultra-low power analog circuits to enable smart interfaces via acoustic signal processing, sensors and integrated software, Skyworks expects to expand its addressable market by over $5 billion. Target applications include AI speakers/microphones, virtual assistants, intelligent gaming controllers and vehicle in-dash systems as well as wired/wireless headsets.

Industry

- Samsung has extended its lead over Intel to 22% according to the latest global semiconductor sales ranking from IC Insights, achieving 36% year-on-year growth in the first half of 2018 with $39.8 billion in sales. For the first half of 2018, all but four of the top 15 companies had double-digit year-over-year growth. Moreover, seven companies had more than 20% growth, including the five big memory suppliers (Samsung, SK Hynix, Micron, Toshiba/Toshiba Memory and Western Digital/SanDisk) as well as Nvidia and STMicroelectronics.
Electronic component shortages – a South African perspective

By Brett van den Bosch.

It goes without saying that our insatiable demand for ever more advanced and ubiquitous electronic technologies is a good thing for the electronic engineering industry. The thriving market supports countless jobs throughout the supply chain and has made lots of companies very rich – just ask Apple.

The electronics supply chain is so sprawling and of such a global nature that when demand begins to outstrip supply, many interlocking cogs have to match up to keep the wheels turning. This has all led to a situation where there is currently an acute shortage of electronic components, and the industry is taking severe strain globally.

What’s the problem?
The shortage is resulting in long lead times for manufacturers of electronic products. Radio Data Communications (RDC), a company specialising in communication for the security sector, is one of the South African companies dealing with the consequences, according to chief technical officer Terry van Zyl.

“It’s been affecting our production planning for a few months already,” he says. “Some components are difficult to find and some are now on 40 to 70 weeks delay. This means we have to order almost a year ahead of production, which means our stock values increase, which is affecting operational and production costs.”

There are knock-on effects too, such as the introduction of relabelled, out-of-date parts entering the supply chain in an effort to meet demand, as well as sub-standard and counterfeit components entering the market at a more attractive price.

When scarce components are available with shorter delivery times, they are 50-100% more expensive and only available in small numbers, says van Zyl: “Some components are more popular in certain sizes, usually the latest and smallest sizes used in cellular phones, tablets and other handheld devices. Because these popular components are also normally cheaper due to high production volumes, they are sometimes used in local designs to lower the overall cost and size.

“Now that these devices are increasingly taken up in huge numbers due to forward-buying by large companies to protect their new product stock for many months, smaller manufacturers are feeling the pinch. To satisfy this huge demand more component production lines are geared for these components and less capacity is available for the slightly larger but now lower-volume components. This is another reason why the most popular components locally used are more difficult to source.”

For manufacturers, the result is not only frustration but also a financial penalty. “We already had to do some small design changes to be able to use alternatives – mostly the package size that differs slightly. When such a design change is done, new printed circuit boards must be made and existing stock becomes unusable. This obviously affects the cost of a device and can only be absorbed up to a certain point before increasing the selling price,” van Zyl explains.

Who’s to blame?
In a sense, we’re all to blame for this problem since it’s our relentless demand for electronics that’s behind it. The major culprits, though, are the automotive and smartphone sectors, as the number of components that goes into them has risen dramatically, with no signs of slowing down. “The major cellular manufacturers like Samsung, Apple, LG and recently Huawei are buying up huge amounts of stock, leaving very small numbers for the rest of the manufacturers,” van Zyl laments. “They’ve got the buying power to do so, including signing contracts with manufacturers with penalty clauses included to guarantee continuous supply.

He says another problem that SA manufacturers face is the volatile exchange rate, recently hit by others developments in the world markets and affecting raw product cost. This applies largely to imports but also locally manufactured costs as most local products still have some imported cost components.

Saro Murabito, Johannesburg regional sales manager at broadline component distributor EBV Electrolink, believes that objectively speaking the problems are not necessarily worse in South Africa. “This is a global problem,” he says. “For sure, the larger companies, with larger forecasts and abilities to place longer-term orders longer in advance, would have been able to manage the shortages a bit better, but no one is immune to this.”

He goes on to point out that the current situation is nothing new: “The industry has generally run cycles of shortages and long lead times, followed by waves of ‘stock in abundance.’ The industry has been predicting this for some time now, and unfortunately the impacts are extreme on companies that were not in a position to plan long-term orders when the warning signs started appearing more than 18 months ago.”

What components are affected?
According to figures released recently by the Electronic Components Industry Association (ECIA) all component categories are being affected to a greater or lesser degree. Those figures indicate average lead times for interconnect and electromechanical components of roughly 67 days, and around 85 days for passives and semiconductors. Digging into these categories, the worst offenders were resistors (more than 125 days), capacitors (almost 110 days) and discrete semiconductors (roughly 130 days).

Van Zyl singles out high-volume components like small multi-layer ceramic capacitors and resistor packs as being the most problematic, due to the fact that all electronic devices use them for various reasons. “There is no substitute as other component variations can either not perform the same function, or when they can they normally cost many times more than the original component.

“Certain components are also made of scarce or rare-earth materials which are only mined in limited areas around the world, often in countries with unstable politics. Tantalum capacitors are part of this group. When a large manufacturer secures new product stock for many months, importers and distributors are finding it very difficult to supply local manufacturers with stock at short notice and often with many months’ lead time,” says van Zyl.

What’s to be done?
It’s only a matter of time before the market corrects itself, but the light at the end of the tunnel is still far in the distance, with even the most optimistic analysts predicting that a significant improvement won’t come until 2020.

Continued on page 6
The 4th edition of the IEEE Global Electromagnetic Compatibility Conference (GEMCCON), is coming to Stellenbosch in the Cape Winelands of South Africa.

The conference will cover many topics in EMC, including special sessions on
- Radio frequency interference.
- Time domain metrology.
- EMC in large installations.

Invited speakers

Keith Armstrong, Cherry Clough Consultants, United Kingdom - Techniques and Measures to Manage Functional Safety and Other Risks with Regard to Electromagnetic Disturbances.

Sarel van der Merwe, ITC Services, SA - A Brief History of EMC in South Africa.

Frank Leferink, University of Twente, Netherlands - Risk Based vs Rule Based EMC in Large Installations.

Ferran Silva, Universitat Politècnica de Catalunya, Spain - Time Domain Measurement Methods in EMC.

Paul van der Merwe, MESA Solutions, SA - EMI Measurements on Renewable Energy Plants.

7 to 9 November 2018  www.gemccon2018.emcss.org
Arrow Altech Distribution rebrands to Altron Arrow

JSE-listed Allied Electronics (Altron) recently unveiled its new brand which unites all its businesses under one brand identity.

The brand ushers in a significant shift, ensuring that the company goes to market under a single identity, making it easy for customers to streamline their business with the company.

“Our new brand brings with it a new culture of how we do business,” said Mteto Nyati, Altron Group chief executive. “Part of this is our renewed commitment to being a partner to our customers throughout their digital transformation journeys, and we want our customers to experience us as trusted advisors.”

Through its single brand identity, Altron aims to remove the complexity experienced when engaging with the various businesses within the group. “The joint venture between Altron and Arrow is a perfect partnership which allows us to deliver innovation that matters,” says Peter Griffiths, managing director of Altron Arrow.

Altron provides local corporate governance, value-based leadership, legal and financial capability; while Arrow is the leading distributor of electronic components in sub-Saharan Africa and has recently expanded its wide component range to include two new business divisions that deal with IoT solutions and sustainable technology.

Speaking at a launch event, Griffiths explained that the digital capability of world 4.0 will make good companies great, relevant and sustainable while the essence of the Alton brand is to make progress effortless for its customers. “Altron Arrow is a leading technology solutions provider in components, IoT solutions and sustainable technology in the ICT sector,” says Griffiths. “We are always eager to draw on the experience of our brand and are a proud business unit of Altron.”

For more information contact Altron Arrow, +27 11 923 9600, info@arrow.altech.co.za.

Forbatt brings Peak Power quality to SA

Forbatt SA recently introduced the Peak Power range of power solutions into the South African market. Peak Power is one of the few power supply manufacturers in China having a nationally recognised CNAS (China National Accreditation Service) Laboratory, assisting testing and calibration standards equivalent to ISO/IEC 17025:2005, which can perform product safety and energy efficiency testing according to the scope of review.

Peak Power’s dedication to quality extends beyond an emphasis on OQC (output quality control) and embraces QA (quality assurance) and QC (quality control) best practices to streamline production and ensure that the final products meet the company’s quality criteria. To this end, its factory has implemented such strict quality control systems whereby it has obtained ISO14001 and ISO 9001 certifications for environmental and quality management systems, in addition to its CNAS certification. The factory focuses on quality in the entire manufacturing process and carries out detailed quality management which entails a rigorous review of product design, raw material procurement, production process, ex-factory inspection and after-sales service.

The test report issued by the CNAS laboratory is approved in over 70 countries including China, the USA and most European countries, as well as over 80 certificate authorities. According to Forbatt SA’s Dr Russell Ruiters, “Peak Power can react quickly to its customers providing product testing, safety certification, reliability and other services according to international standards. This can ensure their power supply product is safe, reliable and shortens the product development cycle, providing market opportunities and improving product advantages and market competition.”

All Peak Power products meet or exceed IEC60950-1 standards (Safety of Information Technology Products) and have been issued Letters of Authority by the NRCS (National Regulator for Compulsory Specifications) in South Africa. “Ultimately, Peak Power is a quality partner you can trust where these same standards are built into every one of its CCTV power supplies, AC power supplies/adaptors and DC backup power packs,” says Ruiters.

For more information contact Forbatt SA, +27 11 469 3598, sales@forbatt.co.
RAPDASA (Rapid Product Development Association of South Africa) is a non-profit organisation that strives to be the official platform for rapid product development in South Africa. We connect leading innovators, entrepreneurs, industry partners and academics through various community engaging events.

Since its first conference in 2000, RAPDASA’s annual conferences have grown in both size and importance. They are now recognized as a showcase for the AM sector in South Africa, where international keynote speakers are regularly invited to introduce the latest developments on the global front.

With Johannesburg being one of South Africa’s major manufacturing hubs, RAPDASA 2018 provides an excellent opportunity for local industry to participate in the event and introduce the South African manufacturing sector to the latest developments in 3D printing.

RAPDASA 2018 will encompass a number of happenings, namely:

- A pre-conference workshop
- Conference
- An exhibition which will be open to industry representatives and members of the public who are not conference delegates

We would like to invite you to be a part of this exciting event. We have structured our exhibitor and sponsorship packages, with certain privileges for sponsorships on a specific level.

Please contact Tebogo Ranoto (tebogor@resolutioncircle.co.za) for more info.

Be part of 4.0. For more info visit www.rapdasa.org
MQTT protocol is giving hackers a backdoor into smart homes

Another warning has been issued to designers of Internet of Things (IoT)-connected products, with the cybersecurity firm Avast announcing recently that it discovered a severe flaw related to the MQTT (Message Queuing Telemetry Transport) protocol widely used by smart home devices.

The company found more than 49,000 MQTT servers publicly visible on the Internet due to a misconfigured MQTT protocol. This includes more than 32,000 servers with no password protection, putting them at risk of leaking data. To be clear, this does not mean that the MQTT protocol itself is insecure, but rather that severe security issues can arise if it is incorrectly implemented and configured.

The MQTT protocol is used to interconnect and control smart home devices via home smart home hubs. When implementing the MQTT protocol, users set up a server. In the case of consumers, the server usually lives on a PC or some mini-computer such as Raspberry Pi, which devices can connect to and communicate with.

The implication of the flaw discovered by Avast is that cybercriminals could gain complete access to a home to learn when their owners are home, manipulate entertainment systems, voice assistants and household devices, and see if smart doors and windows are opened or closed. Under certain conditions, it says cybercriminals can even track a user’s whereabouts, which can be a serious privacy and security threat.

“It is frighteningly easy to gain access and control of a person’s smart home, because there are still many poorly secured protocols dating back to bygone technology eras when security was not a top concern,” said Martin Hron, security researcher at Avast. “Consumers need to be aware of the security concerns of connecting devices that control intimate parts of their home to services they don’t fully understand and the importance of properly configuring their devices.”

Hron describes five ways in which poorly configured MQTT servers can be abused by hackers:

1. Open and unprotected MQTT servers can be found using the Shodan IoT search engine, and once connected, hackers can read messages transmitted using the MQTT protocol. Avast research shows that hackers can read the status of smart window and door sensors, for example, and see when lights are switched on and off. In this particular case, Avast also found that outsiders could control connected devices or at least poison data using the MQTT protocol on behalf of devices. This way, for example, an attacker could send messages to the hub to open the garage door.
2. Even if an MQTT server is protected, Avast found that a smart home can be hacked as in some cases, the dashboard used to control a smart home’s control panel runs on the same IP address as the MQTT server. Many users use default configurations that come with their smart home hub software, and these are often not password protected, meaning a hacker can gain complete access to a smart home’s dashboard, allowing the hacker to control any device connected via the dashboard.
3. Even if both the MQTT server and dashboard are protected, Avast found that in the case of smart hub software, Home Assistant software, open and unsecure SMB shares are public and therefore accessible to hackers. SMB is a protocol used for sharing files on internal networks, mainly on the Windows platform. Avast found publicly shared directories with all the Home Assistant files including configuration files. In the exposed files, it found a file storing passwords and keys stored in plain text. The passwords stored in the configuration file can allow a hacker to gain complete control of a person’s home.
4. Smart homeowners can use tools and apps to create a dashboard for an MQTT-based smart home, to control their connected devices. A particular application, MQTT Dash, allows users to create their own dashboard and control panel to control smart devices using MQTT. Users have the option to publish the settings they set up using the dashboard to the MQTT server, so they can easily replicate the settings on as many devices as they would like. If the MQTT server used is unsecure, a hacker can easily access the user’s dashboard, which allows them to easily hack the smart home.
5. Avast found that MQTT can, in certain instances, allow hackers to track users’ location, as MQTT servers typically concentrate on real-time data. Many MQTT servers are connected to a mobile application called OwnTracks. OwnTracks gives users the possibility to share their location with others, but can also be used by smart homeowners to let the smart home devices know when the user is approaching the home, to activate smart devices, like smart light lamps. In order to configure the tracking feature, users have to configure the application by connecting to an MQTT server and expose the MQTT server to the Internet. During this process, users are not required to setup login credentials, meaning anyone can connect to the MQTT server. Hackers can read messages that include a device’s battery level, location using latitude, longitude and altitude points, and the timestamp for the position.

For more information visit www.avast.com

MPU prototyping board up for grabs

Microchip Technology and Dataweek are offering readers a chance to win a Microchip SAMASD2 Xplained Ultra board – a fast prototyping and evaluation platform for the SAMASD2 series of MPUs (microprocessor units).

The SAMASD2 series is a high-performance, ultra-low-power ARM Cortex-A5 processor based MPU. The Cortex A5 processor runs up to 500 MHz and features the ARM NEON SIMD engine, a 128 KB L2 cache and a floating point unit. It supports multiple memories, including latest-generation technologies such as DDR3, LPDDR3 and QSPI Flash.

SAMASD2 devices integrate powerful peripherals for connectivity (EMAC, USB, dual CAN, up to 10 UARTS, and more) and user interface applications (TFT LCD controller, PCAP and resistive touch controllers, touch controller, class D amplifier, audio PLL, CMOS sensor interface, etc.). The devices offer advanced security functions to protect customer code and secure external data transfers. These include ARM TrustZone, tamper detection, secure data storage, hardware encryption engine, on-the-fly decryption of code stored in external DDR or QSPI memory, and a secure boot loader.

The SAMASD2 Xplained Ultra board (ATSAMASD2-XULT) allows users to extensively evaluate, prototype and create application-specific designs. The board includes eMMC and DDR3 memories as well as a rich set of connectivity options.

A Linux distribution and software package allows users to easily get started with their development, and connectors and expansion headers allows for easy customisation and quick access to leading-edge embedded features such as the Class D amplifier or the capacitive touch controller (PTC).

For your chance to win a Microchip SAMASD2 Xplained Ultra board, visit http://page.microchip.com/datweek-samasd2.html and enter your details in the online entry form.
Arrow Altech Distribution (Pty) Ltd - South Africa’s leading electronic components distributor, takes pleasure in announcing the launch of its new brand - Altron Arrow. By bringing together Altron Limited and Arrow Electronics Inc, the company intends to deliver innovative, high value electronic components and IoT distribution solutions that matter to the South African market. By providing leading technologies to its customers; vision becomes reality. From concept to finished product, Altron Arrow strives to be the strategic electronic component and IoT supply chain partner of choice.
The role of security in the new era of IoT

By Esther Cairos of Infineon Technologies and Christian Krieber of EBV.

The Internet of Things (IoT) is one of the fastest growing technological revolutions the world has ever seen, with billions of devices connected in homes, smart factories, offices and even in remote locations.

Yet, as the IoT proliferates, so do the potential access points for the security risks posed by malicious attackers. In many ways, as machine-to-machine (M2M) communication is central to the IoT, these attacks are far more significant than ‘normal’ computer attacks as actual physical machines can be taken over.

In this article, Infineon Technologies and EBV will look at some of the implications of security breaches and consider how designers should approach the task of planning and implementing a secured IoT infrastructure. The article will look at how hardware-based security has a pivotal role to play as well as some services – particularly the device personalisation service by EBV – that significantly ease the deployment of hardware-based security solutions.

The need for IoT security

There are a huge number of businesses basing part or all of their future prosperity on the myriad of applications that use cloud services and artificial intelligence to deliver revenue streams. In fact, Cisco recently estimated that in the next five years this business sector will add some $19 trillion to global GDP.

The billions of connected devices that are already deployed are key enablers of this significant new sector of the economy. And, while their connected nature allows them to deliver value, it also exposes them to the possibility of malicious attacks that could result in intellectual property theft, stolen personal information, interruption of business operations and even endangering a company’s brand image and, ultimately, its existence.

The threat is very real and global, affecting many large organisations, both commercial and government. More damaging than simple computer viruses, as many IoT devices are directly connected to machinery and infrastructure, attacks on IoT infrastructure have reportedly led to the shutting down of steel plants, power stations, major businesses and even a nuclear facility. At the consumer level, Incontrol reported that 71% of consumers fear that their personal information may be stolen, which is clearly slowing the adoption rate of this new technology.

As fast as new IoT technology is being developed, the ‘bad guys’ are developing ever more sophisticated ways of compromising the security measures. Popular methods include physically microprobing the ICs, analysing electromagnetic emission, inducing faults in operation by power supply manipulation or through adding clock glitches.

IoT security for designers

In order to be properly protected, security is needed in all aspects of the system, covering the application, communications to/from the device and also within the physical device itself. Properly executed (Figure 1), this approach will protect confidentiality, integrity and availability.

The first step for any designer is to consider what levels and types of security are appropriate for the task at hand. The nature of the target and its value are important considerations, as is brainstorming possible attack methods, the likelihood of such attacks and the impact of any successful attack.

Having weighed up these factors the designer will then go on to consider how attacks can be avoided and the costs of doing so, as well as any impact the measures will have on overall system performance and maintenance.

Given their nature, IoT devices have some specific needs and challenges where security is concerned (Figure 2). Generally speaking, IoT devices have limited MCU and memory resources and utilise non-rich operating systems, so security devices must support these embedded OS and work within the small host memory footprint. Physically, IoT devices are small and this must be mirrored in the chosen security solution.

Continued on page 12
Widest selection of electronic components

In Stock

TRX Electronics
Authorised Mouser Partner in South Africa
Tel: 086 111 2844 | trx-e.com

MOUSER ELECTRONICS
mouser.co.za

ORDER WITH CONFIDENCE
Authorised Distributor of semiconductors and electronic components
Many IoT devices are powered by coin cells or energy harvesting techniques, so the security devices must be extremely frugal with their energy usage, as well as offering a low cost to align with the cost sensitivity of most IoT devices.

Finally, many IoT designers are not experts (or even experienced) in security, so the chosen solution must be easy to implement. More often than not this means selecting a supplier with an extensive support infrastructure available, both directly and through technically competent channels of distribution.

**Hardware is an essential ingredient**

While software and encryption can provide a level of security, there are some notable weaknesses to a software-only approach. For example, during the process of authenticating an IoT node (Figure 3), certificates and public / private keys are exchanged and processed to ensure the recipient device is properly identified and authorised. However, in a software-only system this can mean moving the private key into non-secure memory to allow processing to be performed. This exposes the private key to malicious attackers, thereby compromising the overall security of the system.

Hardware-based security solutions, such as the OPTIGA Trust X from Infineon Technologies, operate as a secure element. This means that the private key is processed only inside the secure element, thereby protecting the private key from being discovered and guarding system security from being compromised.

OPTIGA Trust X is a fully featured device security solution that offers premium-grade security based on a CC EAL 6+ (high) certified security controller that supports TLS/DTLS and X.509 certificates. It is TRNG AIS-31 certified and supports USB Type-C authentication as well as providing a cryptographic toolbox that allows flexible customisation.

The ability to customise and tailor OPTIGA Trust X allows it to be used in an extensive set of use cases including mutual authentication, secured communication, data store protection, lifecycle management, power management and the all-important secured updates that keep IoT devices bug-free and up-to-date.

Despite the power of OPTIGA Trust X, the turnkey solution is easy to integrate into IoT applications. Infineon provides all necessary host code, a customer specific public key system, an evaluation kit and a wealth of knowledge and expertise that is made available to designers.

**Device personalisation**

Adding a secure element to a design and making use of its authentication or encryption features is only one aspect. Since crypto keys are the heart of any security measures they have to be generated in a secure way and in an area where only authorised people have access. Furthermore, certificates have to be generated and signed with a private key which must never leave the HSM (hardware security module). All these requirements demand a significant investment in terms of time, knowledge and equipment.

This is where EBV can help customers with their personalisation service under its ‘Secure-it’ brand. Along with a highly trained and experienced technical support team, EBV is able to offload the customer from the programming effort. Through the service, the company can offer the generation of certificates as well as the creation and programming of security keys, delivering customer specific devices for IoT applications in an easy way (Figure 4).

The programming is carried out using Data I/O hardware that is held in a physically secured environment and housed in a fenced area at EBV’s facilities in Germany. None of the equipment is connected to the Internet and, therefore, is not susceptible to any form of attack or malicious tampering – protecting all aspects of an IoT system from being compromised.

Protecting all aspects of an IoT system is essential, as is tailoring the security approach and levels to the value of the application and the probability of an attack happening. While software and encryption go some way towards offering security, a hardware-based security approach is a far stronger solution.

Infineon’s OPTIGA Trust X is a fully featured turnkey security solution for IoT devices that meets the many and somewhat challenging needs for deploying security in an IoT environment. Included in the support ecosystem is a high level of support as well as the device personalisation service from Infineon’s trusted partner, EBV.

For more information contact EBV Electrolink, +27 21 402 1940, capetown@ebv.com.

**Summary**

Continued from page 10
LPWA technologies in South Africa – which is best?

The end of 2G is inevitable – internationally, we have already seen its discontinuation in the likes of the US and Australia. Even 3G may not be available for long in some countries. In South Africa, we probably have a good few more years but ultimately a replacement technology is needed.

Companies offering services like vehicle tracking and alarm systems, for example, that have built their systems on the 2G network will need to have an alternative. Low power wide area (LPWA) technologies fill the gap between mobile (3G, LTE) and short-range wireless (e.g. Bluetooth and Wi-Fi) networks.

**What will LPWA do?**

LPWA technologies will enable the connection of billions of IoT devices onto the Internet. They are designed to provide connectivity to devices and applications that require low speed and low data bandwidth. This will be critical in the development of the IoT applications. The LPWA devices are ideal for applications that have low data transfer rates and don’t need data very often, so will handle small amounts of fairly infrequent data.

IoT devices and sensors will be used in a wide range of industries and applications which will require a large number of low-throughput devices and where a delay in communications will not result in a material loss of service. One of the early use cases is in energy and water meters, where meters do not need to transmit data frequently or in real-time, and can be sited in difficult-to-reach locations.

**How will it do it?**

The main drivers behind the development of LPWA technologies were to reduce cost (in terms of device as well as deployment) and power consumption, at the same time as increasing coverage and the number of devices that can be connected, compared with cellular and other wireless networks.

These devices will typically be battery powered and not connected to mains power, so most of these technologies promise to achieve up to 10 years’ battery life on a single charge. They incorporate technologies that enable devices to power down when data is not being transmitted to conserve battery life.

There are many competing LPWA technologies in this space but in South Africa they are mainly LoRa, Sigfox and now Narrowband IoT (NB-IoT).

**Sigfox**

French based Sigfox is one of the early starters in this space. Globally they partner with companies in various countries to roll out their IoT ecosystem, including platform providers, device and other manufacturers and tech hubs. Their technology uses ultranarrowband (UNB) modulation in unlicensed frequency bands.

One advantage of Sigfox is that it is one global IoT network and can listen to billions of objects broadcasting data, without the need to establish and maintain network connections. Another advantage is that it uses very low power as there is no signalling overhead and the objects are not constantly attached to the network. Sigfox offers a software-based communications solution, where all the network and computing complexity is managed in the cloud, rather than on the devices.

<table>
<thead>
<tr>
<th></th>
<th>GSM</th>
<th>Sigfox</th>
<th>Lora</th>
<th>LTE-M</th>
<th>NBIOT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Frequency</strong></td>
<td>900/1800 Mhz</td>
<td>868 Mhz</td>
<td>868 Mhz</td>
<td>NA</td>
<td>900 Mhz</td>
</tr>
<tr>
<td><strong>Potential Coverage</strong></td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td><strong>Deployment</strong></td>
<td>Good</td>
<td>Good</td>
<td>Medium</td>
<td>Poor</td>
<td>Medium</td>
</tr>
<tr>
<td><strong>Data Rate</strong></td>
<td>Good</td>
<td>Low</td>
<td>Medium</td>
<td>Good</td>
<td>Medium</td>
</tr>
<tr>
<td><strong>Module Cost</strong></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Power Requirements</strong></td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Limited</td>
</tr>
<tr>
<td><strong>Mobility</strong></td>
<td>Good</td>
<td>Low</td>
<td>Good</td>
<td>Good</td>
<td>Limited</td>
</tr>
</tbody>
</table>

Comparison of LPWA technologies in South Africa.

Continued on page 14
Continued from page 13

**LoRa**

Based out of California, the LoRa Alliance is an open, non-profit association with 330 members globally among telcos, system integrators, startups and manufacturers. The alliance claims there are live LoRaWAN networks in more than 120 cities.

LoRa technology offers a very compelling mix of long range, low power consumption and secure data transmission. One of the main benefits of this technology is that it allows the creation of both public and private networks and can provide coverage that is greater in range compared to that of existing cellular networks. If there is a coverage issue, it is relatively inexpensive to add coverage privately. It is also easy to plug into the existing infrastructure and offers a solution to serve battery-operated IoT applications.

**Narrowband IoT**

NB-IoT is a low power wide area network (LPWAN) radio technology standard developed by 3GPP specifically for the IoT, for devices that require small amounts of data and ultra-low power requirements. The cellular networks are embracing this technology and see it as an enabler for mass IoT deployment due to its low power requirements and wide area coverage.

Ultimately, the end devices will have to be as low cost as possible to enable the huge number of IoT devices that are predicted to be connected. Because it uses a network with licensed spectrum, NB-IoT is more secure and less susceptible to interference than unlicensed spectrum LPWA solutions, and it also enables global roaming.

NB-IoT specifically suits battery powered IoT applications that do not move (static installations). It is perceived to have cost and coverage advantages over another evolving technology called LTE-M (also known as LTE-MTC). LTE-M is more suited to applications that require slightly higher throughput and mobility, such as tracking. This is perhaps a better 2G alternative but right now the local cellular networks are focusing on NB-IoT and it will most likely be a while before they will invest in rolling out LTE-M.

There must be uninterrupted coverage in order for IoT applications to work, with coverage over long distances and deep penetration. NB-IoT must therefore provide coverage of remote and rural areas, hard to reach places such as underground locations, and deep inside buildings.

Power spectrum density (PSD) boosting and repetition in NB-IoT can deliver coverage gains of 20 dB when compared with GSM networks, enabling about ten times better area coverage. NB-IoT needs just 200 kHz of bandwidth (hence the name ‘narrowband’) which means it can run adjacent to existing cellular networks. The unit cost of NB-IoT devices is expected to be low and to fall as demand picks up.

**Conclusion**

While the number of connected devices continues to rise (and is expected to reach 125 billion by 2030), the maturing wireless technologies that support them are also continuing to get a good deal of attention. NB-IoT, LoRa and Sigfox, all low-power, wide-area network (LPWAN) technologies, are often pitted against one another with an expectation for one to be the clear winner. However, if you understand each of the technologies and their features, you will see that there is probably a place for all of them and each can play a role in IoT.

For more information contact Gyula Wendler, Altron Arrow, +27 11 923 9709, gwendler@arrow.altech.co.za.
Design choices for Bluetooth Low Energy

Now in its fifth major release, Bluetooth has many features and options that make it possible to tune wireless communication to the precise needs of the application.

One of the most important factors for IoT applications is the availability of Bluetooth’s low-energy profile, BLE. But there are a number of factors to consider when it comes to designing BLE into the end equipment.

Implementing Bluetooth from scratch is a complex undertaking but, for most IoT applications, it is not a necessary step. There are numerous solutions available that provide Bluetooth and BLE integration. The key is to select the solution that has the best fit for the application’s requirements.

One of the key reasons for choosing BLE in IoT designs over traditional Bluetooth is its lower power consumption. The designers of BLE recognised that typical implementations would only need to send short packets at widely spaced intervals. A connection might last only for a few milliseconds with readings being taken a second or more apart.

BLE saves energy by allowing the interface and its control electronics to move into a low-energy sleep mode between transitions if it does not need to listen for incoming packets. Conventional Bluetooth transceivers will often remain awake during those quiet periods to listen for keep-alive messages. The sleep period is dynamic. If an active phase does not result in the transfer of application data, the protocol can extend the sleep period.

As receive and transmit power is typically on the order of 10 mA to 30 mA, the ability to sleep for long periods means BLE transceivers and their host MCUs can work on devices that are powered by sources such as lithium coin cells. BLE further reduces the energy burden by restricting the number of channels on which a transceiver needs to perform discovery – 3 versus the 32 of traditional Bluetooth. This makes discovery faster with far fewer searches.

Designers working on an IoT application can choose a dedicated BLE interface IC, a module-level solution or opt to use an integrated MCU with BLE support built in. Each of these options has implications for the project, such as time to market and form factor.

RF antenna options

The antenna is a key consideration. An effective antenna design is required to ensure that the end product meets user requirements for range and power efficiency as well as compliance with regional standards intended to prevent spurious RF emissions.

The time-to-market advantage of a module-based Bluetooth implementation, such as the Microchip Technology RN4020 or Panasonic PAN1760A, is that the antenna can be integrated into the module itself. This greatly reduces design and test time. Module implementers take great care in optimising the antenna design to ensure it operates at high efficiency over a wide operating range.

However, the use of a module may place constraints on the design of the baseboard and enclosure that do not suit the end application, particularly if there are specialised requirements for the device. For example, a wearable will often need to use an enclosure that is comfortable for the user. Often, these devices will form the antenna into the enclosure design itself, which demands a customised solution. In this case, a dedicated Bluetooth transceiver IC designed to work with a custom antenna is required.

Space constraints will tend to favour the use of a single Bluetooth-enabled SoC that performs application and communications functions. If the aim is to add Bluetooth to an existing product line that already has an extensive base of firmware developed specifically for it, the integrated SoC solution may not be a viable option.

Protocol support

One key advantage of a Bluetooth module or dedicated transceiver is that it makes it possible to offload most communications functions from the host CPU. The Kinetis KW35/36 series of BLE ICs from NXP include an ARM Cortex-M0+ processor core running at 48 MHz to handle the Bluetooth protocol stack in addition to the CAN-FD and LIN standards used in automotive body electronics.

This processor core is powerful enough to run, in addition to the BLE protocol, other applications, allowing it to function as a complete SoC as well as a smart transceiver. Typical use-cases for the KW35/36 are for remote keyless entry and tyre condition monitoring. The device supports up to eight concurrent, secure connections.

The Panasonic PAN1760A module, which integrates filter electronics and antenna for ease of integration, is based around the CC2540 transceiver made by Texas Instruments. Protocol-stack handling is performed by an integrated 8051 processor core.

The RN4020 developed by Microchip Technology can act as a BLE module for a larger

Continued on page 16
Continued from page 15

Higher performance to support higher-performance applications that require BLE connectivity is available from devices such as the Nordic Semiconductor nRF52832, which integrates an ARM Cortex-M4F core, 512 KB of flash memory and 64 KB of RAM. BLE SoCs and modules can provide a number of ways in which the wireless protocol can be integrated into an application. The Microchip RN4020 offers a scriptable mode to support rapid prototyping and implementation of BLE-enabled applications. The scripting language can be used to build applications that read sensor data and relay the information over a Bluetooth connection to a paired device.

Inside the BLE stack

In most cases, an integrated SoC with BLE support will provide firmware libraries that provide access to the functions of the protocol stack. The BLE stack itself is divided into a number of layers and component parts that can be implemented on top of a real-time operating system (RTOS) that may be supplied by the vendor, a custom solution or a third-party offering.

The stack will often communicate with the RTOS through semaphores, flags and callback functions. Some porting effort will be required to map the function calls from a vendor’s BLE stack to the underlying kernel if a custom or third-party RTOS is employed. Key elements of the BLE stack are the Generic Access Profile (GAP), the Generic Attribute Profile (GATT) and the Security Manager (SMP).

The GAP performs a number of tasks including the sending of data broadcasts without first establishing point-to-point connections, the discovery of nearby devices and the setup and teardown of connections between peers that have been paired. The GATT takes on the tasks of sending data to and receiving data from peers that have been paired. Packets sent by the GATT can be set to demand a response to ensure correct delivery or they can be set to expect no confirmation.

The data sent using the GATT layer will often fit into one of the Bluetooth standard’s many application-specific profiles. By making use of these profiles rather than using custom packet formats, IoT node vendors can help ensure interoperability with a wide range of peer devices, such as medical sensor nodes that report blood pressure and heart rate or building automation systems that relay environmental data.

The SM implements the functions needed to pair devices securely and send protected messages after pairing. The SM includes functions for exchanging encryption keys and – an increasingly important factor in IoT designs – for encrypting data before transmission.

Security is becoming a key focus for many IoT developers. As well as encryption of inflight data, it is important that systems are made resistant to attacks vectors such as BlueBorne. This may make it important to put a simple user interface onto the device so that an installer can enter a secure code during commissioning. Alternatively, an additional RF channel such as NFC can provide the necessary authentication from a mobile phone running an appropriate app or a custom hardware tool used for installation and commissioning.

API considerations

The decision on whether the Bluetooth interface runs within the host MCU or separately will affect the structure of the software. But vendors often provide tools to aid with moving from one to another where changes in applications demand it. When the application is based on standalone Bluetooth-enabled MCU, the stack is typically accessed through C function calls. As an external smart transceiver IC, the same API functions may be accessed in a coprocessor mode through a serial interface such as a UART. The serial protocol may be based on AT commands similar to those originally employed for simple modems, or on a custom protocol. The serial protocol will carry commands from the host to the Bluetooth stack and responses and events from the Bluetooth stack back to the host.

Other tools that aid the construction of profiles can include compilers that take as input XML files that define the messaging requirements of the application and convert them into C code and header files. This makes it easier to send data such as blood pressure readings that fit into standard Bluetooth profiles. Multicore IoT-node implementations, such as those that employ a separate Bluetooth transceiver IC or module, have the opportunity to optimise energy consumption by coordinating sleep cycles. With an intelligent transceiver, there is no need for the host CPU to remain awake while RF communication is taking place. Once a command has been issued to send data and the packet is placed in a suitable buffer, the host CPU can move into a low-energy sleep mode while the transmission or reception occurs.

An intelligent transceiver can monitor incoming packets for content and ensure only those with important data for the host CPU will cause it to wake up for processing. Broadcast messages that only concern network management can be dealt with by the Bluetooth transceiver’s own processor. This allows features such as packet relaying in a Bluetooth 5.0 mesh network to be performed without disturbing the host CPU.

Messages that affect the IoT node but have a low priority, such as server status updates, can be buffered locally. The host CPU need only be woken to empty the buffer or when a command from a server that needs immediate attention is received. To implement this functionality, a software state machine that interprets incoming data needs to be written on top of the core Bluetooth firmware supplied for the transceiver’s CPU.

As a BLE transceiver needs to stay awake to listen for incoming packets, this can lead to energy consumption that is greater than planned. A typical scenario is when the GATT layer sends a packet that requires a response from the receiver. As a result, the node will not be able to sleep until this confirmation is received or the transaction times out.

Some urgent packets that are mission critical will need to use such confirmations. However, many data items will be sent that do not need immediate confirmation. Instead, the guarantee of delivery can be performed by application-layer protocols. For example, a custom protocol may synchronise with the remote peer when it next wakes up using packet-sequence numbers or codes. This allows the node to sleep as soon as it has sent the last update packet within the current wake-sleep cycle. The sniff subrating mode employed by BLE synchronises the two endpoints so that a master will hold on to data until the next wakeup or sniff period.

Conclusion

By making smart modules and transceivers that are supported by extensive firmware libraries, manufacturers have achieved the goal of making BLE accessible to practically all IoT designs. The solution that is most suitable for a given design depends on its requirements and application goals, but the wide choice of options means there is one that provides a good fit.

For more information contact Farnell element14, 0800 111 057, info-za@farnell.com.

Image courtesy Microchip Technology.
Real-time EMF monitoring system

Microwave Vision Group (MVG) launched the new EME Spy Evolution, a state-of-the-art continuous EMF exposure monitoring system for monitoring personal exposure to electromagnetic fields and identification of the contributors. The instrument has the ability to monitor up to 20 frequency bands from 80 MHz to 6000 MHz.

The EME Spy Evolution is ideally suited for municipalities, governmental agencies, regulatory bodies, research laboratories, universities, broadcasters, PMR, site installers, maintenance crews and mobile phone operators. According to MVG, with today’s focus on occupational health and safety no manager should allow access to any communication site without an accurate way to monitor radiation. With the EME Spy Evolution’s real-time monitoring, this risk is mitigated and all personnel will have the opportunity to work in a safe environment.

For more information contact Conical Technologies, +27 66 231 1900, daniel.haywood@conical.co.za.

Wireless software merges Bluetooth and sub-Ghz

Silicon Labs has released new software options for its Wireless Gecko portfolio, enabling simultaneous sub-GHz and 2.4 GHz Bluetooth Low Energy (LE) connectivity on a single chip. This solution enables commercial and industrial IoT applications to combine long-range sub-GHz communications with Bluetooth connectivity, simplifying device setup, data gathering and maintenance.

The company's new Wireless Gecko hardware and software solution enables users to set up, control and monitor sub-GHz IoT devices directly over Bluetooth with mobile apps. By adding Bluetooth LE connectivity to wireless networks in the sub-GHz band, developers can deliver new capabilities such as faster over-the-air (OTA) updates and deploy scalable, location-based service infrastructure with Bluetooth beacons.

Proprietary sub-GHz protocols are commonly used in low-data-rate systems, from simple point-to-point connections to large mesh networks and low-power wide area networks (LPWAN), where extended range, robust radio links and energy efficiency are top priorities. Sub-GHz connectivity is a good fit for long-range wireless sensor networks, smart metering and building automation, and commercial lighting. This solution makes it easy to add Bluetooth LE connectivity to these sub-GHz applications.

For more information contact NuVision Electronics, +27 11 608 0144, gdeklker@nuvisionelec.co.za.

IoT middleware toolkit for DesignSpark

RS Components announced the signing of a partnership agreement with Zerynth, an innovative startup company that develops ‘middleware’ software for Internet of Things (IoT) projects and applications. The essence of the agreement is that the Zerynth IoT development environment will be available via a unique portal on the DesignSpark engineering community, enabling easy access for customers to download the tools.

Zerynth has developed a powerful suite of software tools that enables the programming of highly popular 32-bit microcontrollers and their connection to leading cloud infrastructures, enabling the fast deployment of IoT-enabled technology. The suite is a free and cross-platform integrated development environment that runs on Windows, Linux and Mac OS X based computers.

The toolkit includes a compiler, debugger and an advanced code editor, as well as providing tutorials and example projects, and allows engineers and developers to use either the Python programming language or a hybrid version of C/Python. Engineers can start to program after installing Zerynth VMs (virtual version of C/Python). Engineers can start to program after installing Zerynth VMs (virtual version of C/Python). Engineers can start to program after installing Zerynth VMs (virtual version of C/Python).

 strerrorVMs enable access to large cloud infrastructures, including many supported microcontrollers from leading manufacturers including Espressif, Nordic Semiconductor, NXP, Microchip/Atmel and STMicroelectronics, and connect them to leading cloud services from Amazon, Google, IBM or Microsoft.

The DesignSpark Zerynth Studio suite is available to download from the DesignSpark community website, which offers a suite of free software tools and a host of resources and information to help engineers develop their electronics projects and quickly take them from concept to the creation of prototype devices.

“This agreement represents a pivotal step in the evolution of our partnership model and the augmentation of RS’ strategy for the IoT,” said Richard Curtin, vice president of strategic alliances at RS. “It is the first global IoT-based SaaS (software as a service) commercial agreement for RS and Electrocomponents plc and is a supreme example of our commitment to innovation and to bringing world-class products, technologies and solutions to our customers. The Zerynth suite is fast becoming the ‘Android’ for embedded IoT applications and is a key addition to the DesignSpark suite of enabling design and development tools for engineers.”

For more information contact RS Components, +27 11 691 9300, sales.za@rs-components.com.
LoRa transceiver module

The S76S LoRa wireless communication module, designed and manufactured by AcSiP Technology, is a system-in-package (SiP) housed in a 13 x 11 x 1,1 mm LGA form factor.

Powered by an integrated Semtech SX1276 transceiver and STMicroelectronics STM32L073x microcontroller, it is capable of two-way communication over a distance of up to 16 km on the global 863 MHz and 928 MHz ISM bands.

The device’s ARM Cortex-M0+ 32-bit RISC core operates at 32 MHz and features 192 KB of embedded Flash memory and 20 KB of RAM. Supported modulation schemes are FSK, GFSK, MSK, GMSK, LoRa and OOK, and the packet engine handles up to 256 Bytes with cyclic redundancy checking (CRC). The bit rate is programmable up to 300 Kbps.

The S76S is offered with a complete SDK (software development kit) library and ready-to-go HDK (hardware development kit).

For more information contact Andrew Hutton, RF Design, +27 21 555 8400, andrew@rfdesign.co.za.

Industrial IoT development kit

RS Components has launched an Iot (Industrial Internet of Things) development kit for the Harting MICA (Modular Industry Computing Architecture) edge computer.

The Harting MICA CISS (Connected Industrial Sensor Solution) Iot kit (RS part no. 176-2224) is a simple plug-and-play system that enables fast digital condition monitoring of multiple sensor inputs from machinery. This is the first plug-and-play Iot development kit to offer IP54 protection, making it suitable for long-term use in factory automation environments as well as for prototyping and evaluation.

Condition monitoring using physical measurements such as temperature and vibration is an efficient way to constantly monitor and improve the operation of machinery and plants. Changes in machine behaviour can be identified quickly and appropriate action taken. However, it can be expensive to integrate suitable monitoring equipment into existing industrial systems.

The MICA CISS Iot kit – developed between the Harting Technology Group and Bosch Connected Devices and Solutions – integrates a Bosch CISS multiple-sensor unit with a MICA edge computer. Firing up the software requires only a few simple steps, so sensor data is acquired almost immediately.

The compact, IP54-rated CISS sensor unit can be attached to any surface and can measure up to eight physical parameters: temperature, humidity, vibration, change of position, pressure, light, magnetic field and acoustics. The robust, IP67-rated MICA computer can be installed right next to machinery, without the need for a control cabinet. MICA connects to the sensor unit and a local network via industry standard connectors.

Sensor data is displayed in MQTT (Message Queue Telemetry Transport) format via the integrated, browser-based Node-Red dashboard. Data can be analysed and stored in any IT system or Iot platform. A Microsoft Azure Cloud gateway is preinstalled and configured using Node-Red.

RS offers several ways to power the MICA CISS Iot kit, depending on the operating environment. Engineers with access to a benchtop power supply can purchase a simple M8 A-coded power lead (RS part no. 111-3557); wiring guidelines are included with the development kit. Engineers without benchtop power will need a power-over-Ethernet (PoE) plugtop power supply (RS part no. 765-3345, multiregion capable) and an RJ45 Ethernet cable (RS part no. 843-6511).

The Harting MICA CISS Iot kit is now available from RS.

For more information contact RS Components, +27 11 691 9300, sales.za@rs-components.com.

I/O and serial data via a wireless interface

The proprietary Radioline wireless system from Phoenix Contact is now able to transmit I/O signals and serial modbus/RTU data in parallel. Devices with firmware 1.80 or higher support dual mode PLC/modbus RTU, while any older devices can be updated via the PSI-CONF 2.50 software free of charge. I/O modules from the product range can then be added to a Radioline device and additional modbus/RTU slaves can be connected via the serial interface.

This dual mode now makes it possible to transfer information from a serial measuring station and additional I/O data simultaneously. This data can, for example, include door contacts or alarm signals from passive sensors. While in the past a parallel communication path or additional modbus/RTU station was required for this purpose, the I/O function of the Radioline system can now be accessed.

The proprietary Radioline wireless system from Phoenix Contact is now able to transmit I/O signals and serial modbus/RTU data in parallel. Devices with firmware 1.80 or higher support dual mode PLC/modbus RTU, while any older devices can be updated via the PSI-CONF 2.50 software free of charge. I/O modules from the product range can then be added to a Radioline device and additional modbus/RTU slaves can be connected via the serial interface.

This dual mode now makes it possible to transfer information from a serial measuring station and additional I/O data simultaneously. This data can, for example, include door contacts or alarm signals from passive sensors. While in the past a parallel communication path or additional modbus/RTU station was required for this purpose, the I/O function of the Radioline system can now be accessed.

For more information contact Kevin Preston, Phoenix Contact, +27 11 801 8200, kevinp@phoenixcontact.co.za.
The Electronics Buyers’ Guide

www.ebg.co.za

The only place to find the product or brand you are looking for . . .

South Africa’s most comprehensive directory of who’s-who in the industry

- Comprehensive directory listing of manufacturers, suppliers and service providers
- Comprehensive listing of manufacturers and brand names, and the South African suppliers thereof
- Categorised and indexed for fast, easy reference

Request your own copy
if you aren’t already a subscriber to Dataweek
email: nicole@technews.co.za or Tel: +27 (0)11 543 5800
The ultra-low power, low-cost RX130 group adds higher responsiveness and functionality for touch-based home appliances, and building and industrial automation applications requiring 3 V or 5 V system control and low power consumption.

The devices combine enhanced sensitivity and noise tolerance, making it possible to develop touch keys employing a variety of cover materials for use in a broad array of applications. These include control panels for electric appliances used in locations where they are likely to get wet, home equipment employing recessed switches for a more attractive design, and industrial machinery that must be operated wearing gloves for safety reasons.

For more information contact Callie Lombard, Hi-Q Electronics, +27 11 894 8083, callie@hi-q.co.za.

Renesas Electronics has added 38 new microcontrollers (MCUs) in its RX130 group. The new MCUs extend Flash memory size to 256 KB, 384 KB and 512 KB, and increase package size up to 100 pins to provide higher performance and compatibility with the RX231/RX230 group of touch MCUs.

For more information contact Conrad Coetzee, Altron Arrow, +27 11 923 9600, ccoetzee@arrow.altech.co.za.

The expanded RX130 group of MCUs features a new capacitive touch IP that supports both self-capacity and mutual-capacity for improved robustness and sensitivity. The capacitive touch sensor also significantly improves noise immunity and sensitivity for operation in wet conditions or dirty conditions. This allows manufacturers to apply touch keys to a variety of challenging, non-traditional materials, such as wood, glass or thick acrylic, opening up capacitive touch to a wider range of use in wet materials, while reducing safety or malfunction risks.

For more information contact Supreme Electro Magnetics, +27 10 591 3500, info@semcc.co.za.
MPLAB® Mindi™ Analog Simulator

Microchip’s Free Software for Circuit Design

MPLAB® Mindi™ Analog Simulator reduces circuit design time and design risk by simulating analog circuits prior to hardware prototyping. The simulation tool uses a SIMetrix/SIMPLIS simulation environment, with options to use SPICE or piecewise linear modeling, that can cover a very wide set of possible simulation needs. This capable simulation interface is paired with proprietary model files from Microchip, to model specific Microchip analog components, in addition to generic circuit devices. Finally, this simulation tool installs and runs locally, on your own PC. Once downloaded, no internet connection is required, and the simulation run time is not dependent on a remotely located server. The result is fast, accurate analog circuit simulations.

**Key Benefits**

- Perform AC, DC and transient analysis
- Validate system response, control and stability
- Identify problems before building hardware

The Microchip name and logo, the Microchip logo and MPLAB are registered trademarks and Mindi is a trademark of Microchip Technology Incorporated in the U.S.A and other countries. All other trademarks are the property of their registered owners. © 2017 Microchip Technology Inc. All rights reserved. DS20005860A. MEC2196Eng12/17
Dual-mode power monitoring IC

Recently released by Microchip Technology is a flexible dual-mode power monitoring IC that measures both AC and DC modes with accuracy of 0,1% error across a wide 4000:1 range.

Power calculations and event monitoring are included, reducing bill of materials cost and firmware development time. The MCP39F511A is a highly integrated device that addresses the growing need for more accurate power measurements in high-performance designs. Power monitoring has become more prevalent in growing markets such as smart cities and smart homes as developers look to monitor product performance and improve energy usage.

To simplify calibration procedures and support most accuracy requirements, two 24-bit delta-sigma analog-to-digital converters (ADCs) with 94,5 dB of signal-to-noise ratio plus distortion (SINAD) performance and a 16-bit calculation engine are included.

Suitable for a range of consumer, Internet of Things (IoT) and industrial applications, the MCP39F511A automatically senses power supply types and switches between AC and DC modes, optimising measurement results. The device also helps developers troubleshoot events, as well as an integrated low-drift voltage reference and internal oscillator to reduce implementation costs.

Other benefits of using the MCP39F511A include its flexibility and ease of implementation. The device provides standard power calculations such as active, reactive and apparent power, active and reactive energy, root-mean-square (RMS) current and voltage, line frequency and power factor, which enable designers to easily add highly accurate power monitoring functions to end applications with minimal firmware development.

To further simplify development efforts, the chip includes advanced features, such as auto-save and auto-load of power quantities to and from the EEPROM at power loss or start, ensuring that measurement results are never lost if power is disrupted unexpectedly. Event monitoring of various power conditions also enhances preventative system maintenance and enables developers to better manage power consumption.

The device is supported by the MCP39F511A power monitor demonstration board (ADM00667), which is a fully functional single-phase power and energy monitoring system. The system calculates and displays active power, reactive power, RMS current, RMS voltage, active energy (both import and export) and four-quadrant reactive energy. It connects easily through USB to the Power Monitor Utility software that offers automated control to allow users to easily evaluate all system configuration settings.

For more information contact Dirk Venter, Altron Arrow, +27 11 923 9600, dventer@arrow.altech.co.za.

Magnetometer and eCompass

With industrial-grade longevity that assures availability for 10 years, the STMicroelectronics LIS2MDC magnetometer and ISM303DAC eCompass enable both reliable, low-power tamper detection for smart meters and precision motion and distance sensing in applications from industrial automation and robotics to smart buildings, smart security and medical devices.

Both sensors contain an AMR (anisotropic magneto-resistive) magnetometer with high dynamic range of ±50 Gauss, which meets best-in-class benchmarks for resolution and low power consumption. Each also features an integrated temperature sensor, and provides a 16-bit digital output via a built-in I²C/SPI serial interface.

The ISM303DAC’s additional integrated low-noise 3-axis accelerometer with user selectable full-scale range up to ±16 G enables dual-mode magnetic/physical tamper detection. It also serves applications such as antenna pointing, positioning and navigation, robot guidance, and general industrial motion tracking or distance sensing. The magnetic and accelerometer blocks can be powered down independently to maximise energy savings.

Both devices can be configured to generate an interrupt signal for magnetic-field detection and automatically compensate for hard-iron offsets provided from the higher application layer. Additionally, the ISM303DAC can also generate interrupts upon recognition of freefall events, tap and double-tap, activity or inactivity, 6D-orientation thresholds, and wakeup events. A built-in FIFO stores accelerometer data to minimise main processor intervention and, as a result, reduce system power consumption.

Development support includes drivers for both sensors, and software examples including tilt-compensated electronic compass, dynamic magnetometer calibration, and 6-axis or 9-axis sensor fusion. The STEVAL-MKI185V1 adapter board for the LIS2MDC and STEVAL-MKI184V1 for the ISM303DAC are also available, ready to plug into a standard DIL24 socket on a motherboard such as the STEVAL-MKI109V3 professional MEMS board to assist development using ST’s Unico GUI.

For more information contact EBV Electrolink, +27 21 402 1940, capetown@ebv.com.
Electronic housings with standardised interfaces

High-performing, easily adaptable and highly available – for quite some time now embedded systems have been more than just invisible mini-computers.

In decentralised automation structures, they fulfil an assortment of control, regulation and communication functions. Thanks to the rapid increase in the performance of integrated software and hardware, embedded systems play a key role in the efficient networking of autonomous functions to complex, complete systems.

**Complexity of requirements**

Current technological developments – Industry 4.0, Internet of Things, e-mobility, energy efficiency – call on developers of embedded systems to meet a variety of requirements. Extreme miniaturisation, continuously growing computing power and efficient communication between systems in a network have long become routine.

The major areas of focus for users of embedded systems are the reliability of the electronics as well as the suitability for trendsetting applications. And the desire for high flexibility and long-term availability consistently plays a key role in this context.

The development of electronic devices based on embedded systems boasts many advantages for device manufacturers, and they can respond swiftly to new market requirements. A comprehensive range of components on the market reduces development work, meaning the device manufacturer also benefits economically from the time saved. With the symbiosis of adaptive housing solutions and standardised interfaces, Phoenix Contact offers reliable solutions based on established standards and common norms for different market requirements.

The Universal Case System ‘UCS’

Device manufacturers use both standardised and in-house developed printed circuit boards, which require a housing that effectively protects against environmental impacts. The market offers an almost inconceivably large number of enclosure systems serving this purpose. The systems are manufactured either specifically for an application, or basic housings are modified for the respective application at great expense.

If the electronics are to be used both inside and outside the control cabinet, then different housing solutions are required, and oftentimes housings are purchased from different manufacturers. More and more device manufacturers also want to stand out from the competition through the sophisticated design of their devices, and they want to be able to respond quickly to customer-specific requirements. This is where the modular design of the Universal Case System (UCS) is particularly advantageous to the device manufacturer seeking the right solution for their electronics (Figure 1).

The UCS housing consists of two identical half-shells, removable side panels and colour-contrasting corner inserts. If more installation space is required for the same area, the system offers an interesting solution: side panels and screws are replaced by a 20 mm higher version and supplemented by a height adaptor. This makes it easy to generate a new housing size.

The design can also be easily modified using other colours or materials. Corner inserts and

Continued on page 24
half-shells can still be used. The UCS system was designed so that the longer side panel can also be used as the shorter side panel in the next larger housing variant. The advantage here is that the easy-to-machine side panel for integrating the corresponding interfaces is available for various applications.

Variable or fixed PCB mounting
The Universal Case System offers two ways of mounting PCBs. In order to make maximum use of the PCB surface, the PCBs are fixed directly to the corner insert with an integrated screw boss. If maximum flexibility is to be achieved in the positioning of the PCBs, the corner inserts are used without the integrated screw boss.

To fasten the PCB, specially designed screw bosses are used that are simply glued in place. This allows different PCBs to be accommodated in one housing. The modular UCS housing also offers the possibility of positioning several PCBs in each of the two half-shells.

Connections for efficient wiring
The housing itself is one strength of the UCS. The other strength is the universal and standardised interfaces – on the PCB and externally. With COMBICON, a product range that has been on the market for decades, Phoenix Contact has appropriate interfaces on offer here (Figure 2). The range includes screw or push-in spring connections, PCB terminal blocks and connectors. Common manufacturing processes such as soldering, press-fitting or direct plugging are also supported.

Connection technology requirements on the PCB have changed in recent years. Today the type of connection technology, the required installation space on the PCB and the soldering process itself play a major role. In the field of connection technology, the push-in spring connection is now largely established on the market and has excelled in particular. With the push-in connection, rigid and stranded conductors with ferrules can be connected simply by plugging them in, without having to open the terminal compartment.

Miniaturisation also does not stop at the components on the PCB. Here, too, a comprehensive product range of corresponding connectors is available. These connectors, which have been designed for high contact density, can also be easily handled in SMD (surface-mounted device) and THR (through hole reflow) soldering processes.

Signals, data and power
Intelligent devices based on embedded systems only achieve their high functionality with appropriate device interfaces and transmission solutions. Passive connection components such as device and field connectors determine how functional a device is and how flexibly it can be adapted to different areas of application.

For the transmission of signals, data and power, Phoenix Contact has its PLUSCON connector range, which has also been available on the market for decades (Figure 3). The M5 to M12 circular connectors can be used to implement universal cabling systems.

In order to integrate these optimally into the embedded systems, the circular connector solutions are available for all common soldering
The connectors from the PLUSCON data product range were designed for secure and reliable data transmission. With their industrial design and innovative connection technology, these connectors add important external functions to the UCS housing solution.

Summary
The market for embedded systems will continue to grow strongly, especially in view of the major transformations being brought about by Industry 4.0 and the Internet of Things. In this dynamic environment, manufacturers of electronic devices need universal and flexible housing solutions.

The Universal Case System and the numerous connection technologies offer manufacturers great potential for implementing creative product ideas. In particular, the modular design of the housing and standardised connection technologies reduce production costs and enable the device manufacturer to quickly and easily meet market requirements.

For more information contact Richard Schoonebeek, Phoenix Contact, +27 11 801 8200, rschoonebeek@phoenixcontact.co.za.

---

**Concealed wall mounting for Synergy enclosures**

OKW’s Synergy enclosures can now be wall mounted using a new concealed suspension element.

This new suspension element is compatible with the circular R120 (12 cm diameter) and R140 (14 cm diameter) variants, and its hidden fixings are even more discrete than Synergy’s existing wall suspension element (which can be installed with only one screw).

The new wall suspension element’s adapter is attached to the housing using customised double-sided foil on a foam rubber carrier. This adapter fits into a housing which is either screwed to the wall or attached using adhesive foils (available as an accessory). A clever locking pin system provides removal protection.

Each kit is supplied with an adapter, two adhesive foils, one holder and two locking pins. All the plastic components are moulded from ASA+PC-FR for added strength and UV stability. The standard colour is black (RAL 9005). These anodised aluminium enclosures are available in four shapes (square, rectangular, circular and oval). Enclosures can be specified with or without battery compartments for 1.5 V AA cells.

All the fixings are concealed thanks to Synergy’s smart fast-connect construction system. Four internal assembly pillars hold each enclosure together. They snap into the recessed top panel, locate the assembly extrusion and are fixed to the bottom part with four stainless steel Torx T10 anti-tamper screws.

OKW can supply the enclosures fully customised ready for the installation of PCBs. Services include CNC machining, lacquering, printing of legends and logos, RFI/EMI shielding, plastic and aluminium panels, membrane keypads, display windows and assembly.

For more information contact Pieter Engelbrecht, Avnet South Africa, +27 11 319 8600, pieter.engelbrecht@avnet.com.

---

**Plastic DIN rail mounting frames**

The new HC-CIF DIN rail mounting frames from Phoenix Contact can be used to install pre-assembled contact inserts quickly and easily directly on the DIN rail in a control cabinet. As a result, entire marshalling levels can be eliminated for the user.

The corresponding DIN rails are NS 35 and NS 7,5. Made from robust high-performance plastic, the frames are stable, very light, and also accommodate plastic sleeve housings from the Heavycon EVO B series of connectors. One base part for all sizes enables easy adjustment to the desired size. This reduces the number of variants.

Locking clips are used to interlock the base and carrier element. The open cable space on the base frame simplifies installation of inserts. The connecting cables can be secured and relieved of strain using cable binders on the angled cable entry of the carrier element.

For more information contact Richard Schoonebeek, Phoenix Contact, +27 11 801 8200, rschoonebeek@phoenixcontact.co.za.
Electromagnetic interference and compatibility

By definition, electromagnetic compatibility (EMC) describes the ability of a system, a piece of equipment, or some other electrical device that utilises electromagnetic energy, to operate in its intended environment without suffering an unacceptable degradation in its performance, or negatively impacting the ability of another device to perform its intended function.

This article provides a basic understanding of electromagnetic interference and compatibility, the various standards and specifications associated with being compliant, the types of testing available to help the engineer quantify the performance of the equipment, and some of the basic approaches utilised to help meet their requirements.

Electromagnetic interference

Electromagnetic interference (EMI) is either a continuous or intermittent electromagnetic disturbance or electrical signal that, if not properly addressed, can be transmitted into, or out of, electronic equipment and can disturb the normal and intended operation of electronic systems.

EMI is discernible across the entire electromagnetic spectrum and can be generated across either a narrow band or a broad spectrum of frequencies, with the more typical areas of interest extending from the low kHz range to the upper GHz range.

Continuous noise is generally characterised as being low-voltage in nature and common low-frequency sources would be switch mode power supplies (SMPS), electric brush motors, ignition systems and fluorescent lighting. Radio frequency interference is a common term that generally defines a wide range of continuous higher-frequency sources, ranging from high-power radio transmitters to computer clock oscillators.

Intermittent or transient noise is generally distinguished from continuous noise as having duration of less than 16,667 milliseconds, or 60 Hz. Intermittent signals are further classified as being either repeatable or random in nature.

Repeatable transients are internally generated within the circuit, are predictable and can be quantified in terms of amplitude, energy and duration, which typically allows the designer to safeguard the system through selection of a suitable transient protection device. Repeatable transients, for example, can be generated during the switching cycles of inductive loads utilised in welding equipment and motors.

Random noise, on the other hand, is not predictable and cannot be quantified. Examples of random noise would be an electromagnetic pulse in the form of lightning, solar flares, cosmic noise or a nuclear reaction, or an electrostatic discharge, and as such the selection of a suitable safeguard is generally tied to the use of statistical data and trend analysis.

Propagation of EMI

For EMI to occur, three essential components have to exist: the emission source, which was discussed above, the receptor and the coupling mechanism (see Figure 1). The receptor or victim source can be any apparatus, that when exposed to electromagnetic energy from an emission source, will exhibit degradation or malfunction in performance.

In fact, many devices can behave as both receptors and emitters of electromagnetic interference. Communication systems like cell phones, for example, utilise both transmitters and receivers, which can emit an EMI signal.
that has the potential to not only affect other systems, it can also couple back onto itself. The means by which EMI is coupled between pieces of equipment (Figure 2) are generalised as being either conducted or radiated in nature, or a combination of both. Conduction refers to a type of transmission whereby a signal is conveyed along a lead wire or cable that is leaving and entering a piece of equipment. EMI within this classification is usually considered to be low-frequency in nature, with 30 MHz generally acknowledged as the upper limit. Radiated emissions are higher-frequency signals coupled from one device to another without a direct electrical connection. The transmission mechanism is wireless and capable of travelling through non-conductive materials such as air, space, plastic and insulators.

In situations where a combination of both conducted and radiated emissions are at work, signal, power and ground cables can act like receiving or transmitting antennas, as illustrated in Figures 3 and 4.

**EMI suppression**

Depending on the means of propagation, unwanted electromagnetic signals can generally be suppressed through the use of proper shielding, filtering and grounding techniques, or a combination thereof (Figure 5).

Where the designer is dealing with radiated emissions, suitable shielding, through the use of tightly sealed metal or metalised housings, will help to mitigate transmission of unwanted EMI into and out of the enclosure. Unfortunately, this approach is not considered practical, as some openings are obviously needed to accommodate conductors that connect to external sources and loads.

In this case, the selection of a suitable electrical filter, placed in line with these conductors and properly grounded at the housing access or egress point, will not only provide for further shielding, but will also allow for elimination of conducted EMI. A combination of these two methodologies and use of a low-resistance connection to ground, will normally provide adequate isolation, eliminate unintended electromagnetic signals, both radiated and conducted, and allow all associated equipment to operate as intended.

**Compliance testing**

Electromagnetic compatibility or EMC is established through the performance of emissions testing which identifies the frequency and amplitude of EMI generated by a device, and/or immunity testing, which verifies the performance of a device or system when subjected to known levels of EMI. Emissions are measured by connecting a line impedance stabilisation network (LISN), a current probe or an antenna to an EMI receiver, scanning the desired frequency range and measuring the amplitude of the signals detected. This procedure would act much in the same way as the ‘scan’ button on an FM radio. Immunity/susceptibility testing, by comparison, connects the LISN, a current probe or an antenna to an RF amplifier and injects a signal into the system being evaluated. For this analysis, the equipment still scans for EMI signals, but now the intention is to monitor the performance of the device under test while subjected to the energy and determine what sort of response, if any, the equipment exhibits. Emissions and immunity testing are further broken down into four basic EMC tests: radiated emissions, conducted emissions, radiated immunity and conducted immunity. Radiated

---

**Figure 4. Conduction-inducing radiation.**

**Figure 5. Basic EMI compliant system.**

**Figure 6. EMI resulting from radio transmissions.**

Continued on page 28
Continued from page 27

tests utilise an antenna in the test setup, whereas conducted tests deal specifically with wires and cables and are easy to identify as there are no antennas used.

Real world considerations

Typical RF emissions limits are 100 dB or lower than typical RF immunity requirements. In other words, if all electronic devices in a given environment are limited to such low levels of emissions, then why are these same devices required to handle such high levels of immunity?

The short answer is that electronic devices must be designed to operate in the presence of both radio transmitters and radio receivers (see Figure 6 on page 27). Radio transmitters generate relatively high levels of energy so that the transmitter can be detected by radio receivers that can be miles away.

Conversely, radio receivers are designed to detect extremely low levels of energy because of the great distances involved with radio transmissions. Immunity test levels simulate the energy levels that electronic devices will be exposed to when they are operated in close proximity to radio transmitters. Emission limits reflect the maximum energy levels that electronic devices should emit when they are operated in close proximity to radio receivers, so as not to interfere with the radio receiver's operation or significantly reduce its operating range.

Standards and specifications

From a global perspective, most governments have established very specific rules and regulations related to the control of EMI and the majority take it a step further by stipulating guidelines for testing systems in an attempt to ensure an acceptable level of EMC.

The International Electrotechnical Commission (IEC), via its International Special Committee on Radio Interference (CISPR), has created globally accepted EMI and EMC rules. South Africa adopts these CISPR standards under its own set of SANS (South African National Standards) designations. The South African Bureau of Standards (SABS) is authorised to issue a certificate of compliance for products that pass applicable EMC testing at an accredited laboratory. ICASA (Independent Communications Authority of South Africa) is tasked with enforcing a regulation requiring any EMI-propagating product sold in the country to be suitably certified.

Conclusion

Electromagnetic compatibility is becoming more and more significant, especially in light of continually evolving EMC legislation, and as such has become an important aspect in the design of electronic equipment and systems. A lack of understanding when it comes to possible sources of electromagnetic interference and failure to address those situations, can potentially lead to unwanted and potentially hazardous results in critical applications.

For more information contact Electronic Industry Supplies. +27 11 726 6758, hreispy@iafrica.com.

EMC pre-compliance test system

On offer from Comtest is the latest Tektronix all-in-one solution for EMI/EMC pre-compliance testing and troubleshooting, the EMCVu.

The system gives engineers an accurate, convenient and cost-effective approach to determine if their product designs will pass EMC emission compliance testing on the first try.

With the arrival of Internet of Things (IoT) and a proliferation of electronic devices that can interfere with each other, designing products to meet EMC emission requirements is critical. According to a white paper by Intertek, in today's electronic design environment, about 50% percent of products fail electromagnetic compatibility (EMC) testing the first time.

For many engineers just starting work on new IoT devices, EMI/EMC testing can be intimidating, and failing compliance testing leads to significant cost overruns and schedule delays. Pre-compliance testing reduces failure rates but introduces its own challenges, including difficult and expensive equipment setup, testing accuracy, painful debugging and a lack of reporting tools.

“Meeting EMC compliance starts with good design, board layout and component selection, but even in the best of circumstances getting through compliance testing can be a gamble without pre-compliance testing,” said Kenneth Wyatt, principal consultant of Wyatt Technical Services and EMC compliance expert. “I applaud what Tektronix is doing with EMCVu to make pre-compliance testing more accessible to more engineers, even those who lack deep EMC expertise.”

At the core of the new solution are the Tektronix real-time USB spectrum analysers, including the affordable RSA306B, that offer the performance of traditional desktop instruments at a fraction of the cost. Powered through the USB connection, their small size makes it easy to perform EMI/EMC testing outside the lab environment in relatively low-noise environments, such as basements or parking garages.

The instruments are controlled by SignalVu-PC software running on a laptop or tablet. For this application, SignalVu-PC has been enhanced with optional EMCVu software to provide pre-compliance and troubleshooting capability in the same user interface.

EMCVu offers an easy-to-learn wizard with built-in support for standards, such as CISPR (International Special Committee on Radio Interference), and pushbutton accessory selection and setup. It also simplifies debugging with automated ambient noise capture, multi-failure re-measurement and harmonic markers for in-depth analysis. Users can easily save experiment results with notes and images into a configurable report in PDF or RTF formats.

The spectrum analyser and software are complemented with a comprehensive set of accessories that have all been carefully selected and thoroughly evaluated to maximise test efficiency. To ensure accurate results and save time for users, the loss or gain of the various accessories has already been captured in the software and is accounted for during measurements.

For more information contact Comtest, +27 10 595 1821, sales@comtest.co.za.
**TVS diodes for high-speed automotive data**

Two new AEC-Q101 compliant surge protection models – CDSOD323-T12C-DSLQ and CDSOD323-T24C-DSLQ – have been added to Bourns’ range for protecting high-speed interfaces in automotive applications.

The transient voltage suppression (TVS) diodes are available in an SOD323 package with bidirectional TVS for protecting communication lines. The low capacitance of 3 pF and low leakage current of 1 nA are well suited for use on high-speed interfaces and sensitive lines.

The Model CDSOD323-TxxC-DSLQ series is designed to provide ±30 kV contact discharge ESD protection per IEC 61000-4-2 and surge protection per IEC 61000-4-5. It is designed to improve the reliability of automotive and industrial systems and robustness against damage from ESD and other transient voltage events.

For more information contact Electrocomp, +27 11 458 9000, andrew@electrocomp.co.za.

**GDT lightning arrestor**

A new gas discharge tube (GDT)-type arrester with TNC female to SMA female connectors has been released by Nextek. The PTCTNFSAF20G operates from DC to 11 GHz and exhibits enhanced RF performance with a typical VSWR of only 1.3 and an insertion loss of only 0.15 dB.

The coaxial arrester has a multi-strike capability of 10 strikes at 5 kA or a single strike of up to 20 kA. The unit has maximum RF power handling of 100 W and a through current of 65 V d.c. and 5 A.

The PTCTNFSAF20G has a rugged, waterproof and compact design and it offers bidirectional protection. It is used by several military manufacturers and communication networks to protect sensitive communications systems and air navigation systems.

For more information contact Conical Technologies, +27 66 231 1900, daniel.haywood@conical.co.za.

**Protection thyristors for high-exposure environments**

Littelfuse introduced two series of SIDACtor protection thyristors optimised to protect equipment located in high-exposure environments from severe over-voltage transients.

The Pxxx0MEL 5 kA series and Pxxx0FNL 3 kA series offer enhanced reliability through multiple high-energy surge events.

Unlike many non-semiconductor-based high-power protective products, which can experience functional degradation after only a few surge events, the Pxxx0MEL and Pxxx0FNL series are semiconductor-based components, and will continue to provide protection through multiple surge events without functional degradation.

Typical applications for these protection thyristors include CATV amplifiers, telecom base station equipment, cell towers, UPS/AC high-power distribution grids, automotive battery charging systems, solar power system DC/AC inverters and uninterruptible battery backup systems.

For more information contact Jeva Narian, Altron Arrow, +27 11 923 9600, jnarian@arrow.altech.co.za.

**Wirewound ferrite beads**

Coilcraft offers a broad range of wirewound ferrite beads in standard package sizes from 0201 (0603) to 1812 (4532). Elevated attenuation and frequency performance enable smaller solution sizes compared to traditional thick-film chip ferrite beads. These beads are used as low-pass filters to eliminate high-frequency noise while allowing low-frequency signals or DC current to pass through a circuit.

The wirewound ferrite beads feature a ferrite construction and heavy gauge wire for high current handling. They provide extremely low DCR while maintaining high filtering impedance across a wide bandwidth – up to GHz band. These features enhance the performance of the choke circuit while potentially reducing board space by replacing a larger chip ferrite bead with an equivalent or higher-performing wirewound ferrite bead.

Coilcraft offers 11 families of wirewound ferrite beads, all of which are RoHS-compliant and halogen free. Three models (0603LS, 0805LS and 1008LS) are qualified to AEC-Q200 Grade 3 standards (-40°C to +85°C ambient), making them suitable for automotive and other harsh-environment applications.

For more information contact Andrew Hutton, RF Design, +27 21 555 8400, andrew@rfdesign.co.za.
Radiall has developed a new series of microwave components, including terminations up to 2 W and attenuators up to 15 W equipped with Nex10 connectors, for outdoor applications such as telecom base station integration.

Nex10 terminations are available at low power (2 W) from 4 to 6 GHz maximum frequency in order to meet a range of requirements and provide outstanding electrical performance. The design is suitable for outdoor applications, has passed several environmental test requirements (vibrations, shocks and more), and is IP67 rated.

Attenuators are available up to 15 W with 6 GHz maximum frequency. The robust design allows attenuators to be used in severe environmental conditions, and they are IP67 rated.

For more information contact Hiconnex, +27 12 661 6779, info@hiconnex.co.za.
Programmable 3-channel power supplies

Comtest has announced the introduction of the Keithley Series programmable, low-noise, three-channel power supplies that deliver up to 375 W in a compact 2U high, half-rack-wide enclosure.

Designed for flexibility, accuracy and low noise when testing high-power, multi-voltage circuits such as LED drivers, automotive and power-IC circuits, the power supplies’ three channels are isolated, independent and individually programmable with remote sensing for each channel.

The 2230G-30-3 provides 195 W with two 30 V, 3 A channels and a 5 V, 3 A channel, while the 2230G-30-6 and 2230G-60-3 provide up to 375 W, with two 30 V, 6 A channels and two 60 V, 3 A channels, respectively. Both 375 W versions also have a 5 V, 3 A third channel. For higher voltages or currents, 30 V channels can be combined in series to get up to 60 V, and two or three channels can be connected in parallel to deliver up to 15 A from the 2230G-30-6. All channels are simultaneously displayed on the front-panel display.

To minimise the effects of noise on the device under test (DUT), the triple-output power supplies use a linear design with less than 1 mV rms ripple and noise. The linear design also ensures the supplies don’t add to ambient noise and affect other sensitive instrumentation being used for test. Using the supplies’ remote sensing capability, the user can set and monitor output voltages with a 0,03% basic accuracy and a resolution of 1 mV. Load current can be monitored to 0,1% basic accuracy and 1 mA resolution.

The power supplies include both front and rear access to the power outputs for orientation flexibility in test setups, while minimising required lead lengths to reduce noise pickup, minimise losses and keep the test setup neat. The 2230G series come with three standard interfaces options for PC-based control: USB, GPIB and RS-232.

For more information contact Comtest, +27 10 595 1821, sales@comtest.co.za.

Sealed connector system

Molex recently released the Squba 1,80 mm pitch, sealed wire-to-wire connector system, designed to fit in small spaces and provide protection against liquid, dust and dirt.

The connectors carry up to a 6,0 A current and provide an IP67 NEMA rating on the seals. Seals are retained with caps to provide manufacturers of sensors, lighting, vending machines and liquid dispensers with a durable barrier from moisture and dust.

This Molex product is highly flexible, with options for 2 to 10 circuits, operating temperature limits ranging from -40°C to +105°C, and 30 N of terminal retention. The positive latch is low-profile and is designed to prevent wires from getting caught or damaged.

The seal and seal caps protect against on-the-job damage and guard against shipping and handling abuse as well as the possibility of puncturing the seals during assembly. Compared to similar sealed connector products, the Squba system offers a narrower pitch and a larger range of circuit sizes, and is both waterproof and dust-resistant.

For more information contact TRX Electronics, +27 12 997 0509, info@trxe.com.
ON Semiconductor released the new NCS21x series of bidirectional current sense amplifiers. They include integrated, highly matched precision resistors that offer an accurate, compact system design for measuring small differential voltages. The devices are able to detect common mode voltages in the range -0,3 to 26 V, making them ideal for both high-side and low-side current sensing. The zero-drift architecture of the NCS21xR provides a low input offset voltage (as low as 35 µV) and low offset drift (as low as 0,5 µV/°C). Together with integrated gain setting components, these devices are capable of sensing smaller voltage drops across the shunt, providing a higher gain accuracy and superior temperature performance.

Altron Arrow, +27 11 923 9600.

Quectel’s MC90 is a quad-band GSM/GPRS/GNSS/Wi-Fi module using LCC castellation package. The module features low power consumption and supports dual-SIM single standby function. Thanks to the hybrid positioning technology, the MC90 supports position tracking in both indoor and outdoor environments. GNSS, Cell ID and Wi-Fi positioning ensures that the module can track position even in areas with weak or no signal. It also supports EPO technology which provides predicted Extended Prediction Orbit to speed up time to first fix (TTFF) without the need of any extra server. Based on EPO data, the QuecFastFix Online function further reduces TTFF in cold start. A built-in LNA provides improved RF sensitivity and acquisition/tracking performance even in weak signal areas.

EBV Electrolink, +27 21 402 1940.

ams announced the release of a new XYZ ‘tri-stimulus’ colour sensor – the AS73211 – which provides enhanced optical characteristics because of its filter-on-glass technology. It offers light and colour measurements closely matching a typical human eye’s perception of light. The sensor measures colour accurately at light levels from 0,4 lux up to 208 klux – a wide dynamic range of 250 000 000:1, enabling effective operation in widely varying lighting conditions, from moonlight to bright sunshine. The high sensitivity of the AS73211 makes it particularly suitable for precise measurements of dark objects and materials, such as black pixels on a display screen, dark skin, black paint or soil, even in low-light conditions.

Future Electronics, +27 21 421 8292.

With 26 V maximum gate-drive output voltage and optional separate turn-on/turn-off outputs or integrated active Miller clamp, STMicroelectronics’ STGAP2S single-channel galvanic isolated gate driver can control silicon-carbide (SiC) or silicon MOSFETs and IGBTs across a range of switching topologies. The device has 4 A rail-to-rail outputs for crisp, efficient switching, even with high-power inverters. Input-to-output propagation delay is within 80 ns for precise PWM control at the high switching frequencies suited to SiC devices. High dV/dt common-mode transient immunity prevents energy-sapping spurious switching.

ICORP Technologies, +27 11 781 2029.
<table>
<thead>
<tr>
<th>Company</th>
<th>Telephone</th>
<th>e-mail</th>
<th>Website</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Altron Arrow</td>
<td>+27 11 923 9600</td>
<td><a href="mailto:info@arrow.altech.co.za">info@arrow.altech.co.za</a></td>
<td><a href="http://www.arrow.altech.co.za">www.arrow.altech.co.za</a></td>
<td>6,9*,13,14,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>20,22,29,30,32</td>
</tr>
<tr>
<td>AREI</td>
<td>+27 11 462 3256</td>
<td><a href="mailto:arei@icon.co.za">arei@icon.co.za</a></td>
<td><a href="http://www.arei.co.za">www.arei.co.za</a></td>
<td>14*</td>
</tr>
<tr>
<td>Avnet South Africa</td>
<td>+27 11 319 8600</td>
<td><a href="mailto:sales@avnet.co.za">sales@avnet.co.za</a></td>
<td><a href="http://www.avnet.co.za">www.avnet.co.za</a></td>
<td>25,32</td>
</tr>
<tr>
<td>Comtest</td>
<td>+27 10 595 1821</td>
<td><a href="mailto:sales@comtest.co.za">sales@comtest.co.za</a></td>
<td><a href="http://www.comtest.co.za">www.comtest.co.za</a></td>
<td>28,31</td>
</tr>
<tr>
<td>Conical Technologies</td>
<td>+27 66 231 1900</td>
<td><a href="mailto:daniel.haywood@conical.co.za">daniel.haywood@conical.co.za</a></td>
<td><a href="http://www.conical.co.za">www.conical.co.za</a></td>
<td>17,29</td>
</tr>
<tr>
<td>EBV Electrolink</td>
<td>+27 11 236 1900</td>
<td><a href="mailto:saro.murabito@ebv.com">saro.murabito@ebv.com</a></td>
<td><a href="http://www.ebv.com">www.ebv.com</a></td>
<td>4,6</td>
</tr>
<tr>
<td>EBV Electrolink</td>
<td>+27 21 402 1940</td>
<td><a href="mailto:capetown@ebv.com">capetown@ebv.com</a></td>
<td><a href="http://www.ebv.com">www.ebv.com</a></td>
<td>OFC*,10,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>12,22,32</td>
</tr>
<tr>
<td>Electrocomp</td>
<td>+27 11 458 9000</td>
<td><a href="mailto:andrew@electrocomp.co.za">andrew@electrocomp.co.za</a></td>
<td><a href="http://www.electrocomp.co.za">www.electrocomp.co.za</a></td>
<td>29</td>
</tr>
<tr>
<td>Electronic Industry Supplies</td>
<td>+27 11 726 6758</td>
<td><a href="mailto:hreispty@iafrica.com">hreispty@iafrica.com</a></td>
<td><a href="http://www.eispty.co.za">www.eispty.co.za</a></td>
<td>26,27,28,30*</td>
</tr>
<tr>
<td>Farnell element14</td>
<td>0800 111 057</td>
<td><a href="mailto:info-za@farnell.com">info-za@farnell.com</a></td>
<td><a href="http://export.farnell.com/">http://export.farnell.com/</a></td>
<td>15,16</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>welcome-south-africa</td>
<td></td>
</tr>
<tr>
<td>Forsatt SA</td>
<td>+27 11 469 3598</td>
<td><a href="mailto:sales@forsatt.co">sales@forsatt.co</a></td>
<td><a href="http://www.forsatt.co">www.forsatt.co</a></td>
<td>6,0BC*</td>
</tr>
<tr>
<td>Future Electronics</td>
<td>+27 21 421 8292</td>
<td><a href="mailto:marian.ledgerwood@futureelectronics.com">marian.ledgerwood@futureelectronics.com</a></td>
<td><a href="http://www.futureelectronics.com">www.futureelectronics.com</a></td>
<td>32</td>
</tr>
<tr>
<td>Gemcon South Africa 2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hammond Manufacturing</td>
<td>+1 519 822 2960</td>
<td><a href="mailto:robhammond@hammfg.com">robhammond@hammfg.com</a></td>
<td><a href="http://www.hammondmgf.com">www.hammondmgf.com</a></td>
<td>23*</td>
</tr>
<tr>
<td>Hiconnexion</td>
<td>+27 12 661 6779</td>
<td><a href="mailto:info@hiconnexion.co.za">info@hiconnexion.co.za</a></td>
<td><a href="http://www.hiconnex.co.za">www.hiconnex.co.za</a></td>
<td>30</td>
</tr>
<tr>
<td>Hi-Q Electronics</td>
<td>+27 11 894 8083</td>
<td><a href="mailto:callie@hi-q.co.za">callie@hi-q.co.za</a></td>
<td><a href="http://www.hi-q.co.za">www.hi-q.co.za</a></td>
<td>20</td>
</tr>
<tr>
<td>ICORP Technologies</td>
<td>+27 11 781 2029</td>
<td><a href="mailto:enquiries@icorpotechnologies.co.za">enquiries@icorpotechnologies.co.za</a></td>
<td><a href="http://www.icorpotechnologies.co.za">www.icorpotechnologies.co.za</a></td>
<td>32</td>
</tr>
<tr>
<td>Microchip</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microtronix Manufacturing</td>
<td>+27 11 792 5322</td>
<td><a href="mailto:info@microtronix.co.za">info@microtronix.co.za</a></td>
<td><a href="http://www.microtronix.co.za">www.microtronix.co.za</a></td>
<td>13*</td>
</tr>
<tr>
<td>NuVision Electronics</td>
<td>+27 11 608 0144</td>
<td><a href="mailto:gdekker@nuvisionelec.co.za">gdekker@nuvisionelec.co.za</a></td>
<td><a href="http://www.nuvisionelec.com">www.nuvisionelec.com</a></td>
<td>17</td>
</tr>
<tr>
<td>Phoenix Contact</td>
<td>+27 11 801 8200</td>
<td><a href="mailto:info@phoenixcontact.co.za">info@phoenixcontact.co.za</a></td>
<td><a href="http://www.phoenixcontact.co.za">www.phoenixcontact.co.za</a></td>
<td>18,23,24,25</td>
</tr>
<tr>
<td>Radio Data Communications</td>
<td>+27 11 452 1471</td>
<td><a href="mailto:terry.v@radiodata.co.za">terry.v@radiodata.co.za</a></td>
<td><a href="http://www.radiodata.co.za">www.radiodata.co.za</a></td>
<td>4,6</td>
</tr>
<tr>
<td>RAPDASA</td>
<td></td>
<td><a href="mailto:tebogor@resolutioncircle.co.za">tebogor@resolutioncircle.co.za</a></td>
<td><a href="http://www.rapdasa.org">www.rapdasa.org</a></td>
<td>7*</td>
</tr>
<tr>
<td>RF Design</td>
<td>+27 21 555 8400</td>
<td><a href="mailto:andrew@rfdesign.co.za">andrew@rfdesign.co.za</a></td>
<td><a href="http://www.rfdesign.co.za">www.rfdesign.co.za</a></td>
<td>17*,18,29,30</td>
</tr>
<tr>
<td>RS Components</td>
<td>+27 11 691 9300</td>
<td><a href="mailto:sales.za@rs-components.com">sales.za@rs-components.com</a></td>
<td><a href="http://www.rscomponents.com">www.rscomponents.com</a></td>
<td>17,18</td>
</tr>
<tr>
<td>Sivan Electronic Supplies (SES)</td>
<td>+27 11 887 7879</td>
<td><a href="mailto:elecsupp@global.co.za">elecsupp@global.co.za</a></td>
<td><a href="http://www.semcc.co.za">www.semcc.co.za</a></td>
<td>20</td>
</tr>
<tr>
<td>Supreme Electro Magnetics</td>
<td>+27 10 591 3500</td>
<td><a href="mailto:info@semcc.co.za">info@semcc.co.za</a></td>
<td><a href="http://www.semcc.co.za">www.semcc.co.za</a></td>
<td></td>
</tr>
<tr>
<td>Technews Publishing</td>
<td>+27 11 543 5800</td>
<td><a href="mailto:nicole@technews.co.za">nicole@technews.co.za</a></td>
<td><a href="http://www.technews.com">www.technews.com</a></td>
<td>19*</td>
</tr>
<tr>
<td>Tempe Technologies</td>
<td>+27 11 455 5587</td>
<td><a href="mailto:willem.hijbeek@tempetech.co.za">willem.hijbeek@tempetech.co.za</a></td>
<td><a href="http://www.temptech.co.za">www.temptech.co.za</a></td>
<td>32</td>
</tr>
<tr>
<td>TRX Electronics</td>
<td>+27 12 997 0509</td>
<td><a href="mailto:info@trxco.com">info@trxco.com</a></td>
<td><a href="http://www.trxe.com">www.trxe.com</a></td>
<td>11*,31</td>
</tr>
<tr>
<td>Würth Elektronik eiSos</td>
<td>+27 71 259 9381</td>
<td><a href="mailto:jason.page@we-online.com">jason.page@we-online.com</a></td>
<td><a href="http://www.we-online.com">www.we-online.com</a></td>
<td>IFC*</td>
</tr>
</tbody>
</table>

* denotes advertisement
40VA Power Supply

Peak Power offers power supplies that are easy to install, offering a safe low voltage power source for residential, commercial and industrial applications.

Features
- 40VA with lighting protection
- Dual Output 16.0VAC or 18.0VAC
- Power on LED
- Molded SA plug with 60cm mains cable
- IEC 60950-1 safety certified