engineerIT
www.engineerit.co.za
SUBSCRIBE FREE
JANUARY 2025
FOR ENGINEERS, TECHNOLOGISTS, TECHNICIANS AND ICT INDUSTRY DECISION-MAKERS

Earth may survive the Sun's demise

The data behind smart cities

LED driver for industrial power supply

The oldest satellite operating in space

AI is the spark igniting a new era

New brain implant may enable communication from thoughts alone

engineerIT
www.engineerit.co.za

CONTENTS

JANUARY 2025

EDITOR
Hans van de Groenendaal
hansv@nowmedia.co.za

SUB-EDITOR
Edith Leeson

ADVERTISING
sales@engineerit.co.za

AD COORDINATION
Cecile Scharneck

DESIGNER
Adéle Gouws

PUBLISHED BY
Travel & Trade Publishing (Pty) Ltd
32 Fricker Rd, Illovo, Johannesburg

PUBLISHER
Anton Marsh
antonm@nowmedia.co.za

Part of the NOWmedia GROUP

A VOICE FOR:

IEEE SOUTH AFRICA SECTION
IFAC INTERNATIONAL FEDERATION OF AUTOMATIC CONTROL
Information Technology Association
nmisa National Metrology Institute of South Africa
National Laboratory Association (NLA)
SOUTH AFRICAN ELECTROTECHNICAL EXPORT COUNCIL
Copper Development Association Africa
SOUTH AFRICAN COUNCIL FOR AUTOMATION AND CONTROL
arei
IITPSA
MESA AFRICA
FTTX COUNCIL
WAPA Wireless Access Providers' Association
STE SOCIETY OF TELKOM GROUP ENGINEERS
SAIMC Society for Automation, Instrumentation, Measurement and Control

EngineerIT transitions to new ownership under Estates in Africa

From January 2025, *EngineerIT* will operate under new ownership as Estates in Africa takes over the publication of the title. This marks a significant shift for the technology and engineering-focused magazine, which has been part of the Now Media Group since 2019.

The publication, well-regarded for its in-depth coverage of technology, engineering and information and communications technology trends, will continue to serve its audience with the same commitment – now under the stewardship of Estates in Africa. The change in ownership is expected to bring fresh perspectives and synergies as Estates in Africa integrates *EngineerIT* into its publishing portfolio.

The Now Media Group, known for its extensive range of trade and business-to-business publications, expressed confidence in the publication's continued success and thanked its loyal readership and advertisers for their support over the years. "*EngineerIT* has grown and adapted to a new publishing environment over the years and we are proud of the publication's journey. We trust it will thrive under its new management," said **Anton Marsh**, Managing Director of Now Media.

For more information, contact Nico Martiz at nico@eiapublishing.co.za or Justin Render at justin@eiapublishing.co.za.

DIARY OF EVENTS!

3-6 February 2025
Mining Indaba
CTICC, Cape Town.
https://miningindaba.com

1-2 March 2025
Digital Transformation Summit
Johannesburg.
https://digitransformationsummit.com/south-africa/

4-6 March 2025
Transmission Distribution Conference and Expo
CTICC, Cape Town.
https://africaenergyindaba.com/events/td-africa/

25-27 March 2025
Solar and Storage Live
Solar Africa, Nasrec, Johannesburg.
www.terrapinn.com

6-8 May 2025
13th Africa Automation Technology Fair (AATF2025)
Africa's largest security exhibition at Gallagher Convention Centre, Midrand, Gauteng.
For more information, call 011 835 1565.

8-11 June 2025
SAPICS – Innovation in Motion
Century City Conference Centre, Cape Town.
https://conference.sapics.org/

7-11 September 2026
Electra Mining Africa
Nasrec, Johannesburg.
https://electramining.co.za

To add your event to the *EngineerIT* diary, email details to justin@eiapublishing.co.za

Compact error correction: Towards a more efficient quantum 'hard drive'

University of Sydney quantum researchers Dr Dominic Williamson and Nouédyn Baspin have revealed transformative new architecture for managing errors that emerge in the operation of quantum computers.

Their innovative theoretical approach promises to not only enhance the reliability of quantum information storage but also significantly reduce the physical computing resources needed to create "logical qubits" (or "quantum switches" that can perform useful calculations). This should lead to the development of a more compact "quantum hard drive".

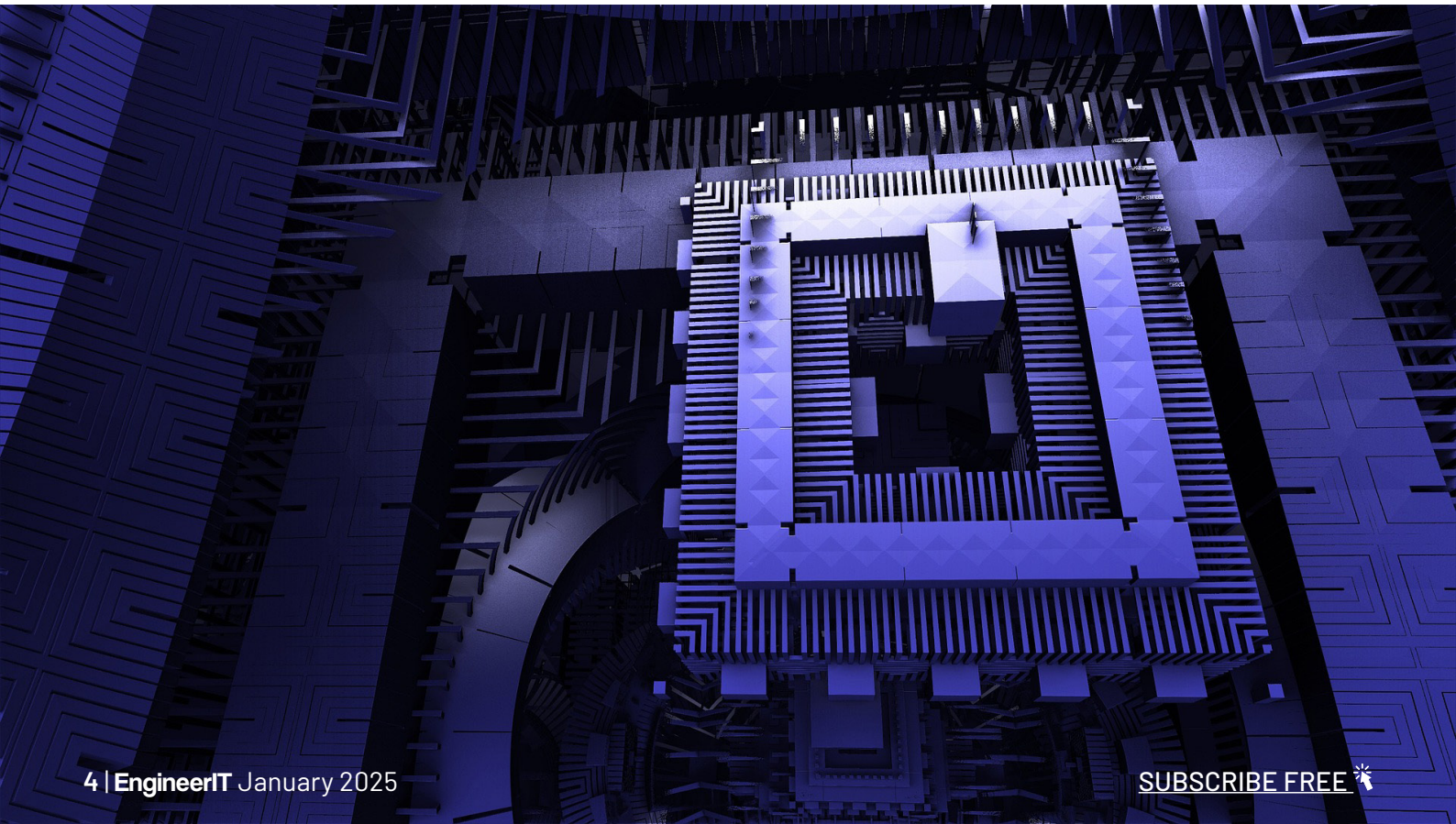
Lead author Dr Williamson, from the University of Sydney Nano Institute and School of Physics, said: "There remain significant barriers to overcome in the development of a universal quantum computer. One of the biggest is the fact we need to use most of the qubits – quantum switches at the heart of the machines – to suppress the errors that emerge as a matter of course within the technology.

Two quantum information theorists at the University of Sydney Nano Institute have solved a decades-old problem that will require fewer qubits to suppress more errors in quantum hardware.

"Our proposed quantum architecture will require fewer qubits to suppress more errors, liberating more for useful quantum processing." Dr Williamson is currently working for 12 months as a quantum researcher at IBM.

At the heart of their theoretical architecture is a three-dimensional structure that allows for quantum error correction across two-dimensions. Current error correction architecture, also constructed within a 3D system of qubits, works to reduce errors in just one dimension along a single line of connected qubits.

Error correction is performed by writing code that operates through the qubit structure – a latticework of how the quantum switches are organised. The objective is to win an "arms race" where physical qubits are used to suppress errors as they emerge by using as few qubits as possible to reduce errors.



Dr Williamson said: "Current 3D codes in a block of dimensions L x L x L can only manage L errors. Our codes can handle errors that scale like L^2 (L x L) – a significant improvement."

It has been known for more than a decade that a three-dimensional quantum error correction architecture (L x L x L) had an upper limit of L x L but no such codes had been discovered.

PhD student and co-author Baspin said: "This means that we have discovered new states of quantum matter in three dimensions that have properties never seen before."

Quantum computers promise to solve complex problems currently beyond the reach of classical computers. However, one of the major challenges in realising practical quantum computing is the need for robust error correction mechanisms.

Traditional quantum error correction methods, such as the widely studied surface code, have limitations in terms of scalability and resource efficiency.

The research by Williamson and Baspin introduces a three-dimensional architecture that effectively manages quantum errors within two-dimensional layers. By leveraging this three-dimensional topological code, the researchers have demonstrated that it is possible to achieve optimal scaling while significantly reducing the number of physical qubits needed. This advance is crucial for the development of scalable quantum computers as it allows for a more compact construction of quantum memory systems.

By reducing the physical qubit overhead, the findings pave the way for the creation of a more compact "quantum hard drive" – an efficient quantum memory system capable of storing vast amounts of quantum information reliably.

Quantum theorist and Director of the University of Sydney Nano Institute, Professor Stephen Bartlett, said: "This advancement could help transform the way quantum computers are built and operated, making them more accessible and practical for a wide range of applications, from cryptography to complex simulations of quantum many-body systems."

The data behind 'smart cities'

While technological breakthroughs and the adoption of digital technologies have brought a new era of progress, it can sometimes be hard for the untrained eye to recognise cutting-edge innovations in every-day life. However, smart cities is a key field where new technologies, such as smart video, directly and visibly, raise living standards.

Smart cities use information and communication technologies to improve operational efficiency, share information with the public and provide a better quality of local authority services. For example, advancements in Internet of Things (IoT) technologies have enabled connected public transportation systems, which leverage real-time monitoring capabilities while tracking the locations and routes of public vehicles. Not only does this speed up service times and reduce traffic congestion, it also cuts waiting times for passengers and keeps them informed.

There's also an important security element to smart cities. "Smart" video or cameras use artificial intelligence (AI) algorithms and deep learning (DL) to analyse visual data in real-time and can dispatch orders from a hub to AI-powered devices faster than a human can process. Going further than just providing data, smart technologies can actually enable the devices to deploy intelligent insights. For example, cameras and AI-analysed traffic patterns can adjust traffic lights accordingly to improve vehicle flow, reduce congestion and pollution and, more crucially, increase pedestrian safety.

Smart video is also being deployed in connected cities to deliver critical assistance to help reduce crime. Business owners, for example, need security cameras to help protect their property, reduce shoplifting and monitor employee or customer incidents. On a larger scale, real-time video analysis is also capable of identifying and differentiating between objects – for example, distinguishing humans from animals and alerting the relevant people or systems if they are in a prohibited location or place.

The process behind smart video

Smart cameras need to "learn" to recognise objects and actions and classify the identified actions into categories such as anomalous or normal. This is where AI and DL are needed for training and learning.

DL needs to analyse a tremendous amount of data to be highly accurate. The development of higher video resolutions, such as 4K, is key here, enabling closed-circuit television cameras to capture more data in high quality and from various angles, making analysis easier and empowering the smart video future.

The smart video sector is going through a transitional phase for recording video at scale: it has moved away from recording raw data from a standard camera to conducting analysis on the AI-enabled camera. In the past, the data analysis was only possible at a centralised location such as a data centre. The rise of onboard AI chips used in smart city technology allows the analytical load to be distributed. The ability to distribute the work is crucial when working at the scale of a smart city, enabling the data to be processed more quickly at the endpoints.

As AI and 4K rise in adoption on smart video cameras, higher video resolutions are driving demand for more data to be stored on-camera. There are many more types of cameras used today such as body cameras, dashboard cameras and new IoT devices and sensors. Video data is so rich nowadays, you can analyse it and deduce a lot of valuable information in real-time instead of post-event.

The role of storage

As a result, storage is critical to the evolution and efficient working of smart video systems. Smart video architectures require innovative storage technologies, which deliver needed flexibility, performance, capacity and reliability. Robust on-board storage must be specially designed to meet the needs arising from multi-streaming devices, on-device DL systems and AI-training solutions.

Storage solutions, like Western Digital's WD Purple Pro line, have evolved to provide high data transfer and write speeds as well as the capacity to ensure world-class video capture. The company has a strong history of innovation going back to the origins of hard disk drive and flash technology. The company works closely with market and innovation leaders in smart video to develop a deep understanding of today's and tomorrow's advances in AI-enabled architectures.

WD Purple Pro is engineered with advanced capabilities needed for high-end smart video solutions, including cameras, network video recorders (NVRs) and back-end video analytics servers. It is purpose-built for 24x7 operating environments and rated for high endurance and demanding AI workloads. Western Digital provides the storage technology that protects and delivers video data to help systems prevent loss, improve situational awareness and increase business efficiency.

Storage-enabled AI

Having improved workload and performance is important in ensuring that drives can keep up with the demands of AI functionality, including pattern matching and object recognition. By combining video stream recording optimisation with top-tier durability and capacity, smart video solutions and AI analytics have the necessary foundations to operate at optimum levels for thousands of hours.

NVRs and video management systems (VMS) are getting smarter. DL algorithms go beyond simple movement detection to enable advanced capabilities to drive improvements in many industries and settings including retail, smart cities and entertainment to name a few. AI-enabled VMS are being architected for new graphic processing units and central processing units to improve overall DL capability and speed algorithms related to object identification.

NVRs with this DL require greater storage capacity and more sophisticated processing, versus individual cameras, enabling them to perform more advanced analytics such as finding a particular image from weeks or months of stored video or creation of traffic heat maps from hours of retail surveillance video.

The WD Purple Pro family is specifically designed and engineered for high performance, capacity, reliability and endurance for advanced, always-on, AI-enabled smart video recorders, appliances and servers.

Behind the innovation

Smart video plays a vital role in increasing public safety such as promoting safe driving practices by monitoring fleet movements to detecting flaws and deviations in a product line to avoid potentially dangerous products. However, the success of smart video relies on a robust and resilient storage architecture that can effectively keep up with the heavy workloads. As smart video use cases proliferate throughout security and logistics landscapes, the hidden data storage complexities shouldn't be forgotten.

LED driver for industrial power supply indication

By Reinhardt Wagner, distinguished engineer

Industrial control systems universally employ 24 V DC for their field supply voltage. The presence/absence of power supply voltage is commonly signalled by light-emitting diodes (LEDs) found on equipment, like the controller head unit, as well as I/O and communication modules. LED supply lights help to minimise installation, maintenance and downtime in industrial systems/subsystems such as programmable logic controllers (PLCs) and distributed control system (DCS) controllers, power-supply units, sensors and actuators. Supply LEDs should light up when defined conditions are met like voltage being in the required operating supply range. Despite their conceptual simplicity, real implementations are not that trivial. They require voltage comparators with hysteresis, need to be self-powered and must drive LEDs consistently.

Further requirements for such circuits are:

- Low power dissipation
- The light must be off when the supply voltage is under the minimum operating voltage
- The light intensity should be invariant of supply voltage
- The circuit should be tolerant to over voltages
- Robustness to miswiring like negative voltages as encountered during reverse polarity

Simple circuits can exhibit significant dependence on component, temperature and voltage variation.

Background

This LED driver circuit is based on repurposing an industrial digital input chip for a function different from its originally intended application. Industrial inputs, as commonly found in industrial control systems, are based on 24 V logic and have clearly specified input current/voltage characteristics with defined input threshold voltages. A sinking input (occasionally called a p-type input) has a pull-down current specified to be larger than 2,0 mA at the maximum input high threshold voltage of 11 V for Type 3 inputs – the most common industrial input type. In order to minimise power dissipation, today's digital input circuits limit and tightly regulate the input current to a level just slightly above the 20 mA limit.

The idea

Noticing that the 2,0 mA level coincides with common LED drive currents and that industrial digital inputs have clearly defined switching thresholds, raises the question: Would a chip, like the MAX22191 single-channel digital input, be suitable for power supply monitoring and LED driving? This industrial input device is designed to drive an opto-isolator via its OUT pin. Figure 1 shows the proposed application circuit. REXT is a current-setting resistor, allowing the OUT current to be set in the 2,0-2,6 mA range.

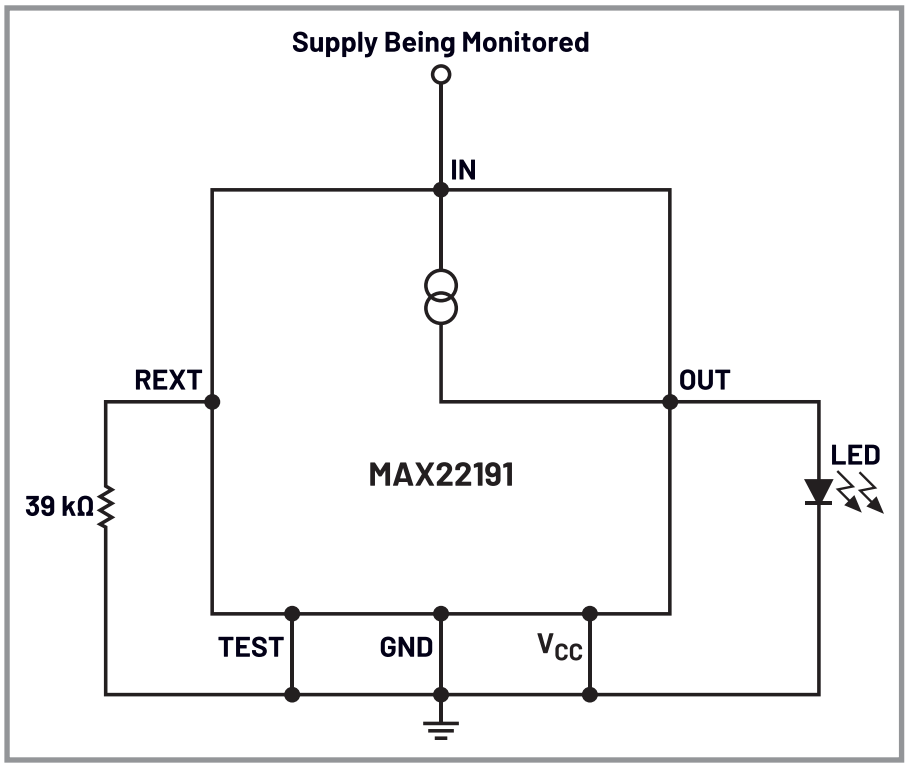


Figure 1: Supply monitoring LED driver.

The internal current source has a tolerance of ±12,5 % over temperature, input voltage and part to part, ensuring low power dissipation and negligible light intensity variation over supply voltage. With the current source specified OUT output voltage compliance of 5,5 V, it is possible to drive most modern LEDs. The device's 110 µA (typical) supply current ensures low power dissipation of the solution.

Figure 2 shows that the LED current turns on sharply at 9 V (typical) and turns off at 8 V (typical), providing 1 V hysteresis. The max-on and min-off threshold voltages are specified in the MAX22191 data sheet. Should higher threshold voltages be required, a resistor can be placed in series with the IN input (R_{IN}) as shown in Figure 3. The R_{IN} value is calculated as R_{IN} = (threshold voltage increase)/I_{IN}.

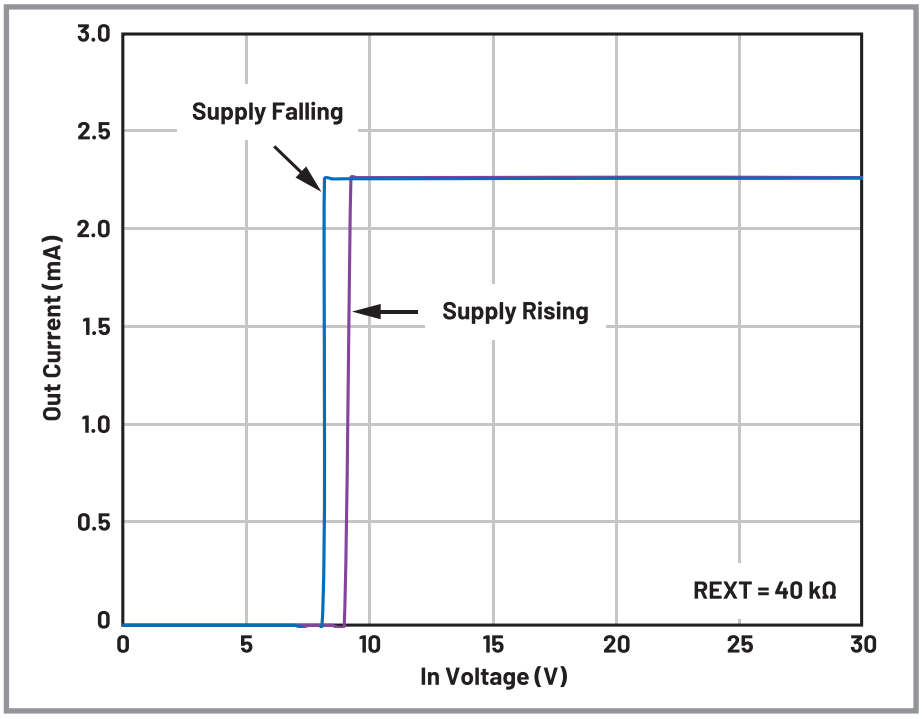


Figure 2: LED current versus supply voltage.

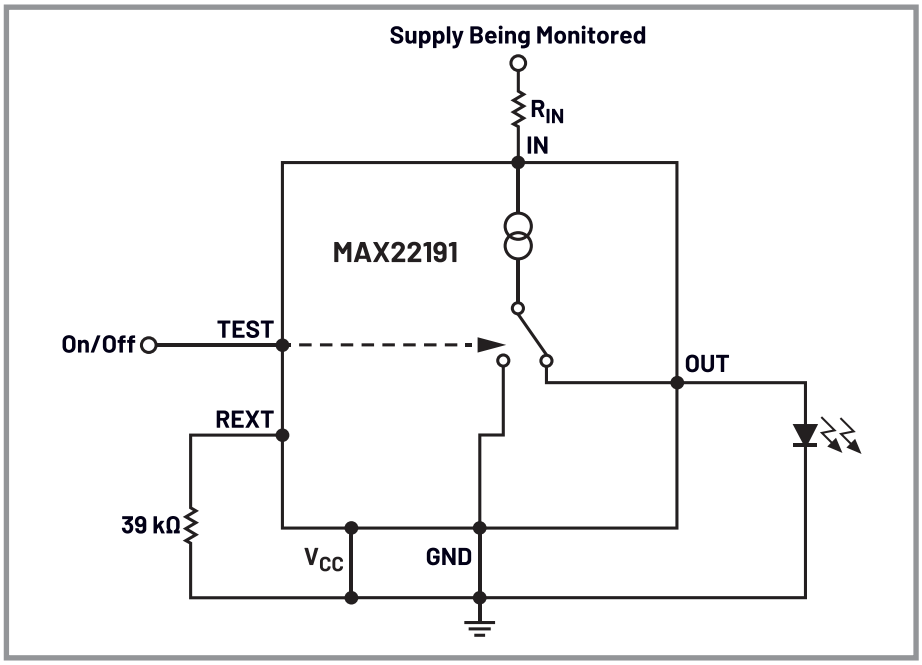


Figure 3: Circuit with on/off control and increased threshold voltage.

The LED current is flat with input voltage variation in the on state, as seen in Figure 2. This contrasts to the use of a simple bipolar/MOS transistor for driving the LED, which shows significantly higher current-voltage dependence due to the transistor's early voltage.

LED control

For application cases where the LED needs to be turned on/off under logic control, the test input can be conveniently used, as shown in Figure 3. This allows implementing auxiliary functions like power-up delays, blinking or other status feedback.

Robustness

The solution is specified for use over the -40°C to +125°C operating temperature range. The IN supply voltage is tolerant to a wide voltage range of -70 V to +60 V, which provides headroom for surge protection and robustness to reverse polarity miswiring. In the event of reverse connection, the circuit has a low 1 µA input current in case of a negative input voltage.

Conclusion

The MAX22191 provides a simple means for LED power supply indication applications. Its SOT23 package and low power current-setting resistor constitute a small solution size.

About the author

Reinhardt Wagner is a distinguished engineer with Analog Devices in Munich, Germany. Originally with Maxim Integrated and now in ADI's Industrial Automation Group, his 21-year tenure primarily involved the product definition of new industrial chips in the areas of communication and input/output devices, like IO-Link, fast digital I/Os, Beyond-the Rails™ analogue switches and digital isolation.

How businesses solve the attack surface dilemma

By Camille Campbell
Director of Wireless WAN and Security Product Marketing, Ericsson

The rise of Internet of Things (IoT) has transformed industries, connecting everything from manufacturing equipment to video camera systems and kiosks. However, unique security challenges raise a key question: How can businesses secure their IoT ecosystems without widespread in-person intervention?

The attack surface dilemma posed by widespread enterprise IoT is a complex challenge but businesses are finding ways to fight back. From zero trust principles to micro-segmentation and artificial intelligence (AI)-driven threat detection, organisations are evolving their IoT security practices to stay ahead of threats.

No single solution can eliminate all IoT risks. IoT security requires layered security strategies – combining proactive management, robust security technologies and vendor collaboration. As IoT adoption continues to grow, investing in these best practices today is crucial for protecting the networks and connected devices of tomorrow.

Why is IoT so at risk from a security perspective?

IoT devices are inherently more vulnerable to security threats than traditional IT systems for several reasons. Many IoT devices operate with limited computing power, which restricts their ability to support robust encryption or security protocols. Additionally, in regulated industries, many of these devices run on outdated firmware or can't be regularly patched, leaving them exposed.

IoT devices frequently lack standardised security practices with manufacturers prioritising functionality and ease of deployment over security. This inconsistency creates gaps that attackers can exploit. Also, the sheer number and diversity of IoT devices in enterprise environments – ranging from cameras and sensors to heating, ventilation and air-conditioning systems – make it challenging to monitor and secure all. Compounding the issue is the fact that IoT devices often come with default passwords that sometimes aren't changed, their data is generally not encrypted and they connect to broader networks. This enables attackers to use IoT devices as entry points for lateral movement, threatening critical systems and sensitive data.

Are specific types of IoT devices most vulnerable?

Imagine the havoc hackers could cause a nation by systematically targeting its power grid. Consider the implications of criminals taking control of a city's network of video cameras. Even worse: a hacker taking over a commercial airplane en route.

While some of these risk scenarios may seem exaggerated, the fact remains: IoT security threats are real and hackers can easily access and control many of our day-to-day devices, homes and vehicles. In fact, months ago, we learned that millions of vehicles could be easily hacked, tracked and controlled, thanks to a simple website bug. According to WIRED, researchers found a flaw in a Kia web portal that let them virtually scan any internet-connected Kia vehicle's licence plate, use it to track millions of cars, unlock the doors and even start the engines. Scary!

While the list of vulnerabilities and IoT devices that could potentially be hacked is massive, here is a list of the 10 most vulnerable IoT devices (according to *IoT World Today*):

- Industrial facilities
- Cars
- Video cameras
- Power grids and utilities
- Buildings
- City infrastructure and transportation networks
- Medical devices and hospitals
- Airplanes
- Retail stores
- Databases

How have organisations provided security for enterprise IoT?

Organisations have employed various strategies to secure IoT environments and each has its own strengths and limitations:

- **Virtual private networks (VPNs):** Many businesses use VPNs to secure communication between IoT devices and central systems. VPNs provide an encrypted channel, preventing eavesdropping on data in transit.

However, VPNs are increasingly seen as inadequate for IoT because they rely on a perimeter-based security model, which assumes that devices and users inside the network can be trusted. If compromised, VPNs can grant attackers broad access to the network.

- **Carrier-delivered private access point names (APNs):** Some organisations use carrier-delivered private APNs to enhance IoT security by creating isolated, private communication channels within mobile networks. Carrier-delivered private APNs allow IoT devices to connect directly to enterprise systems without using the public internet, reducing exposure to external threats. This isolation strengthens security by segmenting IoT traffic and restricting access to predefined enterprise networks. However, carrier-delivered private APNs also have their limitations. They do not inherently protect against insider threats or vulnerabilities within IoT devices such as outdated firmware or weak authentication.
- **Device authentication, network access control and secure boot:** Implementing device authentication protocols only allows authorised devices to connect to the network while secure boot mechanisms verify the integrity of IoT devices' firmware during startup. These measures enhance security but require ongoing firmware updates and strict enforcement to remain effective.

What are best practices in IoT security today?

To effectively keep enterprise IoT data and a company's overall network secure, organisations need layers of IoT security measures. Current strategies to keep in mind include:

- **Zero trust alternatives to VPNs:** Transitioning from VPNs to zero trust solutions ensures every connection request, whether from an IoT device or a remote user, is authenticated, authorised and encrypted. Zero trust networks provide granular access controls and isolate compromised devices, limiting their ability to spread threats across the network.
- **Physical isolation and air gapping:** For highly sensitive environments, physically isolating IoT devices or employing air gapping can provide an extra layer of protection. While not practical for all scenarios, this method is still a strong defence for critical infrastructure or industrial systems.
- **Microsegmentation:** A key network security technique to help implement a broader zero-trust approach at a granular level within the network is microsegmentation. It isolates workloads, applications and compromised areas within specific segments, which helps limit the spread of potential breaches. This approach is not typically at router level. Instead, it is often implemented by using host-based firewalls or software-defined networking, which essentially create secure zones where each segment can be secured individually with specific policies.
- **Robust device identity and management:** Implementing unique, immutable identities for IoT devices and enforcing secure boot processes ensures only authenticated devices are permitted on the network. Regularly updating firmware and applying patches is essential to maintaining device security.
- **AI-driven threat detection:** Automated tools that use machine learning to monitor IoT traffic for suspicious behaviour can proactively identify threats. By analysing device patterns and flagging anomalies, these systems provide early warnings and enable rapid incident response.
- **Endpoint protection for IoT:** Lightweight endpoint security solutions tailored for IoT devices can provide protection against malware and unauthorised access. This is particularly valuable for IoT systems in healthcare or finance where data privacy is critical.
- **Vendor collaboration:** Organisations should work closely with IoT manufacturers to ensure devices meet security standards, including secure firmware updates and compliance with established security protocols. Partnering with vendors committed to security reduces risks across the device life cycle.

The future of IoT security

The future of IoT security will hinge on integrating advanced technologies like AI and machine learning to address the ever-expanding attack surface. AI-driven systems will play a pivotal role in real-time threat detection, analysing vast amounts of IoT data to identify anomalies and potential breaches faster than human teams could.

That said, AI is also a double-edged sword when it comes to IoT security. It will be a valuable tool in detecting and preventing breaches but it will also increase the frequency and sophistication of attacks on IoT devices.

Predictive analytics will also enable enterprises to anticipate vulnerabilities and proactively address them while blockchain technology could enhance device authentication and secure data exchanges.

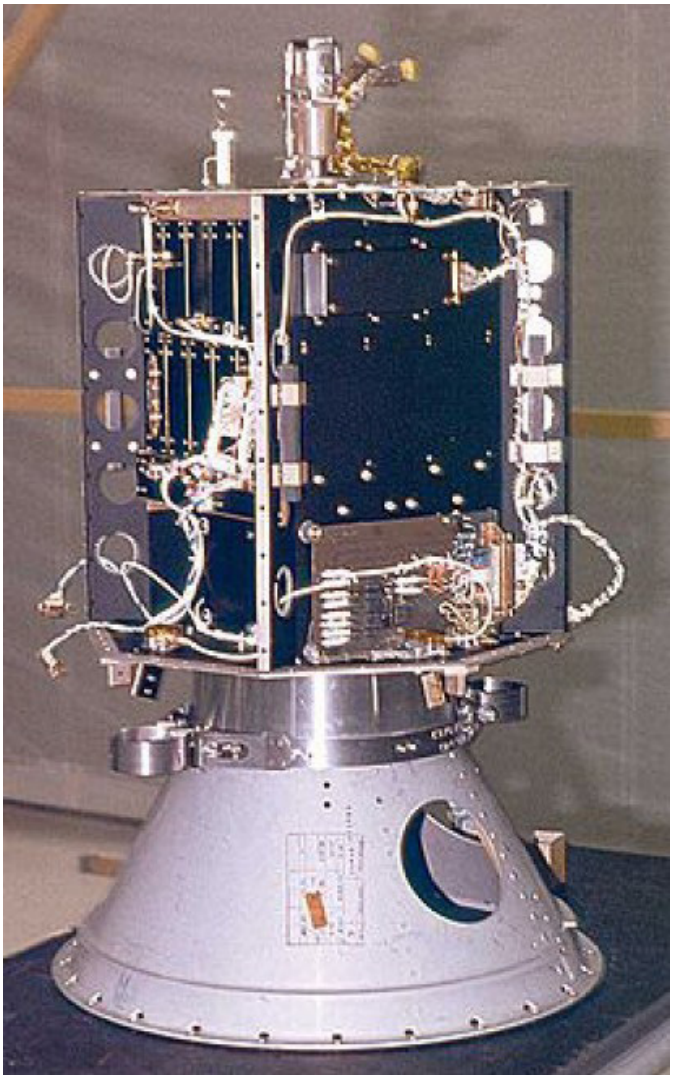
As IoT ecosystems grow more complex, more and more businesses will need to continue adopting zero trust architectures to verify device identities and enforce granular access controls. With these innovations, approaches and strategic collaborations with vendors, enterprises can be ready and more likely to evolve from reactive to proactive security strategies. As a result, many organisations will be able to help ensure robust protection against the dynamic challenges of IoT networks in coming years.

The oldest satellite operating in space

By Hans van de Groenendaal*

It is generally believed that the oldest spacecraft still operating in space are JPL space probes Voyager 1 and 2. They were launched in 1974. But are they, indeed, the oldest functioning spacecraft? Is it conceivable that the oldest working satellites in space were not designed or operated by NASA, USAF or any other space agency? Could it be that the satellite was designed and constructed by radio amateurs with the final assembly in a basement makeshift laboratory at someone's house?

On November 15, 1974, a 29 kg Smallsat was launched. Today, after 50 years, it is still providing communication services to the world's amateur radio fraternity – enthusiasts who have the same passion with which the world's oldest functioning satellite was designed, constructed and built – AMSAT OSCAR 7 (AO-7).



Amateur radio satellites are developed and built by many AMSAT (Amateur Radio Satellite Association) groups around the word and launched as secondary payloads on commercial launches. Once successfully orbiting the earth, these satellites are given OSCAR (orbiting satellite carrying amateur radio) designations like AO-7.

It is often said that, in any system, the batteries are the weakest link. AO-7 proved that point when the batteries failed in 1981. AO-7 went to sleep for 21 years and woke up in 2002 when, miraculously, the short circuit across the battery cells disintegrated and the solar panels were able to deliver power directly to the transponders. The satellite now operates when it is in sunlight.

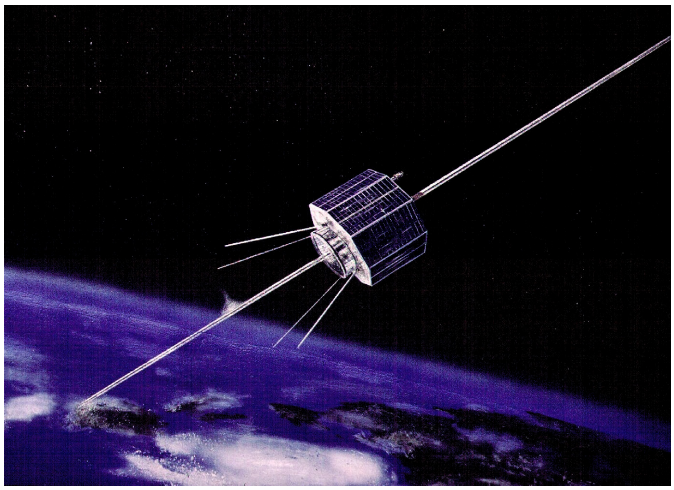
NiCad batteries – star of the show

One fascinating programme that flew from NASA/GSFC was called Radio Astronomy Explorer (RAE) conducting radio astronomy measurement around the moon. The spacecraft used six standard nickel-cadmium (NiCad) cells. The battery pack donated for AO-7 was the engineering test battery pack of RAE-2, which had accumulated many hours under load. After removal, it was installed in AO-7 as the primary energy source. As they accumulate more cycles, NiCad battery cells increase their series resistance. This causes the voltage of each cell to sag under load. This behaviour worsens with increasing duty cycles, especially with a higher drain depth. AO-7's battery did its best but, in mid-1981, it failed. Jan King W3GEY, who is the AO-7 Project Manager, said he and his team of volunteers accepted that this was the end. "We accepted the fact but were happy that, over the six years, we had managed to do all our experiments."

Communicating across space

One of the most interesting features of AO-7 was that, under certain conditions, it communicated through space with AO-6 (no longer operational today) to create a high-frequency (HF) downlink. The downlink spectrum of AO-7's ultra (UHF)/very (VHF) transponder overlapped with AO-6's VHF-to-HF transponder. The overlap of the two was approximately 50 kHz wide. The two orbits were almost the same. AO-7's mean motion was slightly higher than that of AO-6, which means, once every year or so, AO-6 will "lap" its younger sibling in space. During the time when the two spacecraft were in closer proximity, it was already known to be theoretically possible (if AO-7 has its UHF/VHF transponder on) for one user to communicate through two spacecraft in succession with the downlink of AO-7's transponder being relayed through AO-6's VHF/HF transponder uplink and then with the doubly relayed signal arriving on 29,5 MHz to another user on the ground. This could be done, in certain geometries, in both directions, making two-way double-hop communications possible.

The first successful Earth-space-Earth relay of this type took place on January 6, 1975. This happened early in AO-7's "first" lifetime and during the first occasion when AO-6 approached AO-7 in their very similar orbits. The two stations were both located over the state of Texas – one in Dallas and one in Richardson. This method of communication was also conducted and reported by 55 other user stations from 12 countries during 1975. These events were documented in the Institute of Electrical and Electronics Engineers proceedings in October 1975.



CodeStore breaking new ground

There has always been a fascination among radio amateurs in digital modes of communications. In thinking about where this spacecraft sits in electronic history, it is all too easy to forget that it was designed at least three years before the appearance of the first eight-bit microprocessor. The notion of packet communications was still nearly 10 years into the future. The team wanted to demonstrate that they could store data at will on a spacecraft in transit across the sky and then download it at another location. They wanted to demonstrate non-real-time digital communications to themselves and to the world.

CodeStore probably was not the best choice then. The team selected the command frequency for the uplink, which meant it would only be available to authorised command stations.

CodeStore was the brainchild of, and designed and fabricated by, John Goode W5CAY. In one small module, he housed an AFSK decoding system, which allowed uplink data to be clocked into a "long" shift register containing 896 bits. This was done with the memory ICs of the day. What one could manage then was 14 ICs each containing 64 bits of serial data storage. The contents of the shift register was sequentially downlinked first-in-first-out (FIFO) to the selected beacon when CodeStore was commanded to RUN mode.

Today radio amateurs are still involved in satellite communication. In South Africa, AMSATSA is constructing a CubeSat called AfriCUBE. The one-unit CubeSat (10 x 10 x 10 cm) has a dual band software-defined transponder, a camera, telemetry system and an experimental board for student projects.

*hans@intekom.co.za

Powering South Africa's future – the era of smart grids and intelligent equipment

By Sy Gourrah
Senior General Manager: Smart Technologies at ACTOM

Adoption of Internet of Things (IoT) and artificial intelligence (AI) technologies is driving a profound transformation in South Africa's electromechanical equipment sector. This transformation is giving rise to smart grids and optimisation of energy generation, distribution and consumption. Key to this digital transformation is demand for intelligent equipment capable of remote monitoring and control – ushering in unprecedented efficiency and resilience.

Uptake of digital transformation within the industrial sector has been rapid with leading equipment manufacturers realising the importance of giving their equipment a "voice" through IoT. As a result, this sector is seeing significant development towards becoming smart by leveraging real-time data for condition monitoring. This is key to enhancing the performance and efficiency of equipment and enabling remote monitoring that benefits manufacturers and clients – downtime can be prevented by tracking the health and other parameters of components and infrastructure.

Smart grids

Similarly, smart grids that leverage AI and IoT bring numerous advantages to the country's power system as they can monitor an entire electrical system in its totality. This can determine power losses, the best sources of generation at any given time and actual power consumption as data is logged in real time. Additionally, AI enables generation of algorithms to optimise consumption and monitor production or generation and theft, vandalism and losses in the system. Smart grids can ultimately improve system performance, determine energy use, monitor performance and enable condition monitoring of equipment, among others.

However, amid the local electromechanical equipment sector's digital transformation, it must still ensure inclusivity and accessibility while embracing smart grids. Despite meeting the demands of digital transformation through the use of IoT devices and AI, there is huge potential within South Africa to equip people with the skills to deploy these new technologies, manufacture IoT devices, develop AI and programme and code the solutions for AI. Moreover, the country needs to move with the times and introduce these emerging technologies during early childhood development as part of school curriculums.

Yet, to ensure inclusivity and accessibility in adopting smart grid technologies across South Africa, the industry would have to overcome several challenges. These include resistance to change, fear of losing jobs, South Africa's current regulatory framework and pushback from labour unions. Additionally, Eskom could also prove to be a hurdle as it currently has a controlling stake in the generation and transmission grids without much competition in those sectors.

Economic and environmental benefits

Ultimately, transitioning to smart grids in South Africa could potentially yield numerous significant economic and environmental benefits. This is largely due to smart grid initiatives enabling increased energy efficiencies, reduced carbon emissions, greater grid reliability and reduced peak demands. Furthermore, smart grids can lower the costs of operational, maintenance and management resources. All of this would serve to bring down energy costs and use.

Smart grids can also contribute to enhancing energy efficiency and resilience in the face of evolving energy demands and climate change as they monitor real-time data – meaning they can enhance real-time interaction and interconnectivity between energy producers and consumers. This would optimise the use of energy through improved automation and remote switching. In addition, smart grids can also monitor temperature, humidity, water content and illuminance and assist with the reduction of greenhouse gas emissions and other pollutants. This would be a significant positive step to combat climate change while improving energy efficiency.

Leading equipment manufacturers such as ACTOM are recognising the importance of developing intelligent solutions. The company has already begun adding condition monitoring capabilities to its equipment as well as digital substation implementations.

Globally, the shift to smart grids is inevitable and moving at a very fast pace. As a country, South Africa cannot afford to be left behind so we must make a head start and begin the transition to smart grids. This digital transformation, which includes intelligent IoT devices and smart grids, has potential to ensure visibility and achieve greater efficiencies in our power management systems.

New brain implant may enable communication from thoughts alone

A speech prosthetic brain implant – developed by a collaborative team of Duke neuroscientists, neurosurgeons and engineers – can translate a person's brain signals into what they're trying to say.

The new brain implant technology might one day help people unable to talk due to neurological disorders regain the ability to communicate through a brain-computer interface. The current tools available to allow them to communicate are generally very slow and cumbersome.

Imagine listening to an audiobook at half speed. That's the best speech decoding rate currently available, which clocks in at about 78 words per minute. People, however, speak around 150 words per minute.

Compared to current speech prosthetics with 128 electrodes, Duke engineers have developed a new brain implant device that accommodates twice as many sensors in a significantly smaller footprint.

The lag between spoken and decoded speech rates is partially due to the relatively few brain activity sensors that can be fused onto a paper-thin piece of material atop the surface of the brain. Fewer sensors provide less decipherable information to decode.

To improve on past limitations, Cogan teamed up with fellow Duke Institute for Brain Sciences faculty member Dr Jonathan Viventi whose biomedical engineering lab specialises in making high-density, ultra-thin and flexible brain sensors and implants.

For this project, Viventi and his team packed an impressive 256 microscopic brain sensors onto a postage stamp-sized piece of flexible, medical-grade plastic, making a novel brain implant. Neurons just a grain of sand apart can have wildly different activity patterns when coordinating speech so it's necessary to distinguish signals from neighbouring brain cells to help make accurate predictions about intended speech.

After fabricating the new brain implant, Cogan and Viventi teamed up with several Duke University Hospital neurosurgeons who assisted in recruiting four patients to test the implants.

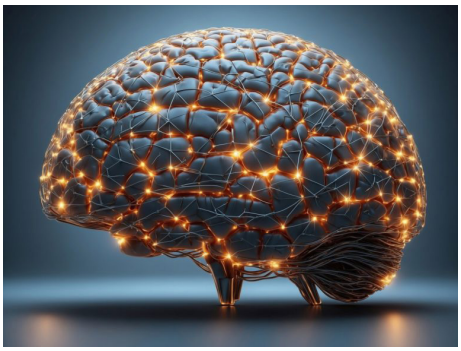
The experiment required the researchers to place the brain implant device temporarily in patients undergoing brain surgery. Time was limited for Cogan and his team to test drive their device in the operating theatre.

"I like to compare it to a NASCAR pit crew," Cogan said. "We don't want to add any extra time to the operating procedure so we had to be in and out within 15 minutes. As soon as the surgeon and the medical team said 'Go!', we rushed into action and the patient performed the task."

The task was a simple listen-and-repeat activity. Participants heard a series of nonsense words like "ava", "kug" or "vip" and then spoke each aloud. The device recorded activity from each patient's speech motor cortex as it coordinated nearly 100 muscles that move the lips, tongue, jaw and larynx.

Afterwards, Suseendrakumar Duraivel, a biomedical engineering graduate student at Duke, took the neural and speech data from the surgery suite and fed it into a machine learning algorithm to see how accurately it could predict the sound being made, based only on the brain activity recordings.

For some sounds and participants, like /g/ in the word "gak", the decoder got it right 84% of the time when it was the first sound in a string of three that made up a given nonsense word.



Accuracy dropped, though, as the decoder parsed out sounds in the middle or at the end of a nonsense word. It also struggled if two sounds were similar like /p/ and /b/.

Overall, the decoder was accurate 40% of the time. That may seem like a humble test score but it was quite impressive, given that similar brain-to-speech technical feats require hours or days' worth of data to draw from. The speech decoding algorithm Duraivel used, however, worked with only 90 seconds of spoken data from the 15-minute test.

Duraivel and his mentors are excited about making a cordless version of the brain implant device with a recent US$2,4 million grant from the National Institutes of Health.

"We're now developing the same kind of recording devices but without any wires," Cogan said. "You'd be able to move around and you wouldn't have to be tied to an electrical outlet, which is really exciting."

While their work is encouraging, there's still a long way to go for Viventi and Cogan's speech prosthetic brain implant to hit the shelves anytime soon.

"We're at the point where it's still much slower than natural speech," Viventi said in a recent *Duke Magazine* article about the technology "but you can see the trajectory where you might be able to get there".

Earth may survive the Sun's demise

A distant white dwarf hosts an Earth-like planet in an orbit that might be like Earth's if it survives the Sun's red giant phase

By Damond Benningfield

Earth's future is bleak. At best, our planet will become a burned-out cinder as the Sun expands at the end of its life. At worst, it will be engulfed by the Sun, leaving no trace that it ever existed.

Astronomers have found a clue as to which path Earth might follow in a star system about 4 300 light-years away. There, a rocky planet orbits the remains of an once Sun-like star at a distance similar to where Earth could park if it survives our own star's death throes.
The system "may offer a glimpse into the possible survival of planet Earth in the distant future," according to a new study published in *Nature Astronomy*.

The system, KMT-2020-BLG-0414L, was discovered in 2020 by the Korea Microlensing Telescope Network, a set of three automated 1,6 metre telescopes in the Southern Hemisphere.

The network looks for gravitational lensing events, those in which a star or planet passes between Earth and a background star. The gravity of the intervening object acts as a lens, making the background star appear much brighter. The length, intensity and other details of the event, along with before-and-after observations, allow scientists to calculate the details of the lensing object.

Early analysis suggested that the system (abbreviated as KB200414) consists of a low-mass star, an Earth-mass planet and a third object many times the mass of Jupiter.

A lucky alignment

Astronomers tried to get a clearer look at the system with the 10-metre Keck II Telescope in Hawaii but those observations did not detect the lensing system's host star.

"This system is part of a larger sample of microlensing planets," said Keming Zhang, an astrophysicist now at the University of California, San Diego and first author of the study. "This is the only one for which we don't detect the expected host brightness."

Zhang and his colleagues considered several scenarios that could explain that finding. They concluded that instead of being a bright main sequence star, the star must be a dimmer white dwarf about half as massive as the Sun. "There is some luck involved because you would expect only around one in 10 microlensing planets to have white dwarf hosts," Zhang said.

The researchers' analysis also showed that the rocky planet orbiting that star is nearly double Earth's mass and more than twice Earth's distance from the Sun. It is the first possible Earth-like world discovered orbiting a white dwarf. Other studies have revealed white dwarfs orbiting gas giant planets, along with bands of rubble that are thought to be the remnants of rocky planets, but nothing comparable to Earth.

The third object in the system appears to be a brown dwarf – a "failed star" that's not massive enough to shine as a true star. It's about 27 times the mass of Jupiter and orbits the white dwarf at about 22 times the Earth–Sun distance, according to the researchers, which would put it beyond Uranus in a comparison to our solar system.

A glimpse at Earth's future?

During its time in the main sequence, a star fuses the hydrogen in its core to create helium. As that process ends, the star expands, becoming a red giant. The Sun, which is 4,6 billion years old, is expected to enter that phase in about 6-7 billion years, puffing up to dozens of times its current diameter. It will remain in this red giant phase for a billion years, after which it will expel its outer layers, leaving only its hot, dense, now-dead core: a white dwarf like the one at the centre of KB200414.

When the Sun becomes a red giant, it will engulf Mercury and Venus. Mars and the outer planets almost certainly will survive.

Earth's fate is more difficult to foretell, however, because of the complicated nature of the Sun's final days. One possibility is that as the Sun loses mass and its gravitational grip on Earth weakens, our planet will migrate outward (though its oceans and atmosphere will have boiled away billions of years earlier). As it becomes a white dwarf, the Sun will lose half its mass, and Earth, if it survives, may expand its orbit to twice its current size, Zhang said. That's about as far as KB200414's rocky planet, suggesting it met a similar fate.

The scenario will be further complicated by the motions of the Sun's other planets, especially Jupiter and Saturn, which can act as wrecking balls.

"Our solar system is relatively boring and stable today," said Carl Melis, also an astrophysicist at the University of California, San Diego, who was not involved in the study but has collaborated with some of its authors in the past. "But when the Sun begins to die, all bets are off," he added. "There are many studies of what will happen dynamically, and it's not pretty."

In the case of KB200414, the brown dwarf would have "wreaked absolute havoc" on other planets in the system as it moved away from the red giant, Melis said. "The brown dwarf would excite all kinds of weird things. I can't even imagine what it would do to the planet."

For that and other reasons, Melis doesn't consider the architecture of the system proposed by Zhang and his colleagues settled. "It is a possible solution – even a reasonable solution. But it's not 100% conclusive," he said. "My personal take is they need to keep cracking."

Extremely large ground-based telescopes, which are expected to come online early in the next decade, should reveal the white dwarf itself, allowing astronomers to confirm their scenario, Zhang said. And NASA's Nancy Grace Roman Space Telescope, due to launch in 2027, should find many additional white dwarf planetary systems, he said. Those discoveries could provide additional clues to the bleak fate of Earth.

Should we be worried? Not in a million years.

AI is the spark igniting a new era

By John Roese
Chief Technology Officer, Dell Technologies

The year is 2025 and we're witnessing the technological equivalent of the "big bang" with artificial intelligence (AI) at the epicentre of how we live, work and play. Just as the universe expanded rapidly after its inception, technology is exploding into new realms, redefining industries and reshaping our future. Whether you're a tech enthusiast, business professional, innovator or student, understanding these shifts is vital to navigating this brave new world.

The rise of agentic AI architecture

"Agentic" will be the word of the year in 2025. The birth of agentic AI architecture marks a new chapter in human-AI interaction. Generative AI (GenAI) tools are evolving to enable AI agents, which are poised to revolutionise how we engage with AI systems.

In the consumer world, we've seen early agent approaches with virtual assistants, chatbots and navigation apps. In 2025, a new, more advanced set of agents will emerge. These agents will operate autonomously, communicate in natural language and interact with the world around them, including working in teams of other agents and humans. They will also be fine-tuned and optimised to perform assigned, specific skills like coding, code review, infrastructure administration, business planning and cybersecurity.

AI agent systems will feature diverse cognitive, orchestration and distribution architectures tailored to specific tasks. As complexity grows, multi-agent systems will emerge, requiring the rapid evolution of tech stacks to support agentic systems effectively.

To realise AI's full potential and the rise of agentic architecture, enterprises must upgrade infrastructure – everything from data centres to AI personal computers (PCs). This distributed infrastructure, optimised for agentic AI, can address security, sustainability and capacity considerations by distributing the AI workload across the entire IT infrastructure (cloud, data centre, edge and device).

Scaling enterprise AI from concept to reality

Enterprises are poised to take AI from ideation to scale. Enterprise AI is simply the application of AI technology to a company's most impactful processes in its most important areas to improve the productivity of the organisation. It requires customers to answer two important questions:

1. **What problem am I trying to solve?** Developing a framework to prioritise AI efforts in the most important, impactful areas is critical.
2. **How do I solve that problem?** AI solutions implemented as random projects on random tools do not scale. Instead, enterprises must determine the minimum set of AI systems needed to build a reusable and scalable AI foundation. This allows them to solve the first set of critical AI problems and then leverage that investment to solve all future AI problems.

At Dell, for instance, our priority areas are our global supply chain, our services capability, our sales engine and our research and development capacity. Any impact on these areas results in significant return on investment (ROI) over other areas like human resources, finance and facilities.

Next, enterprises should look at specific processes in its priority areas. For example, if process analysis uncovers an opportunity – not in how sales people interact with customers but in how much time they spend gathering content for the customer meeting – that's a clear AI project. GenAI can be used to automate and accelerate content discovery and creation work. In this case, the ROI is clear: shift sellers' time back to customer-facing activities and increase revenue.

To execute prioritised projects, enterprises today have multiple off-the-shelf tools from which to choose. So, in 2025, the preferred path is to buy and implement AI tools in their private infrastructure. They can also buy tools that accelerate data modernisation (data meshes, for example).

In 2025, we have clear, repeatable approaches for prioritisation and more turnkey and well-defined AI platforms and AI infrastructure options. 2025 is a year when it simply becomes easier to know what to do and how to do it when adopting AI in the enterprise space.

Sovereign AI accelerates global adoption

Sovereign AI efforts are accelerating AI adoption worldwide. This concept revolves around a nation's ability to create AI value and differentiation using its own infrastructure and data – designing an ecosystem aligned with local culture, language and intellectual property. In an era when data security is paramount, countries are opting for sovereign AI strategies and solutions – often with strong collaboration between the public and private sectors.

Instead of AI systems exclusive to governments, some countries are developing national AI resources to serve government and local private industry, providing access to compute power and data capacity. Others are implementing a coherent national strategy where governments do not necessarily build new infrastructure but instead proactively and collaboratively co-design and encourage private industry to modernise and lead AI ecosystems.

Sovereign AI empowers nations to increase accessibility, protect critical infrastructure, drive economic growth and enhance global competitiveness. By fostering the development of AI, it accelerates its adoption. We're seeing growing investments directed toward infrastructure, data management, talent cultivation and ecosystem development – and we fully expect to see this trend continue in years ahead.

AI and the fusion of emerging technologies

AI's true potential lies in its connections with other emerging technologies. While AI is transformative, its impact multiplies when combined with quantum computing, intelligent edge, zero trust security, 6G technologies and digital twins to name a few. This fusion creates a dynamic environment ripe for innovation and addressing existing challenges.

For instance, quantum computing in collaboration with AI will significantly impact most industries by providing the computing capability needed to scale AI to domains where classical computing struggles like complex material science, drug discovery and complex optimisation problems.

AI and telecom are already coming together to transform how cellular networks operate and how fundamental elements of these systems, like spectrum optimisation, work. Even the future of the PC is influenced by AI as we now see the AI PC not just as a client device but part of the end-to-end AI infrastructure. With agentic architectures, we expect to shift agents out of the data centre and onto the edge or to the AI PC.

Zero trust security and AI are also intersecting. Zero trust architectures are the best path to a better, more secure world and implementing zero trust in brownfield legacy IT is hard. In contrast, AI infrastructure is new and greenfield. We expect customers to adopt zero trust by default in new AI factories for optimal security. Given the criticality of AI, that is a good thing for all of us.

AI becomes an essential skill for everyone

AI will become an indispensable tool across professions and industries. Much like past technological advancements, AI is poised to transform the job market. Routine, task-oriented roles may diminish but new opportunities will arise such as software composers, AI content editors and prompt engineers.

Recent surveys reveal 72% of IT leaders identify AI skills as a critical gap requiring immediate attention. Organisations must invest in developing their workforce's AI fluency. AI skill development will be focused on defining the AI-human relationship where AI completes more of the tasks but people define what needs to be done. This allows professionals to focus on higher-level tasks, critical thinking and complex problem-solving.

With AI, it's not just about the work that goes away, it's about the new roles humans play in shaping, directing and leading AI work. AI-enabled businesses can use the evolution of the human-machine relationship to accomplish tasks in different ways and expand the art of the possible.

AI is tech's grand evolution

Just as the big bang set the stage for the development of galaxies, stars and planets, the rapid growth of AI is creating new opportunities, industries and ways of living and working.

As we approach 2025, we predict enterprise AI adoption will accelerate dramatically in the coming year. We're seeing better processes, better tools and a stronger ecosystem. For chief information officers, staying informed and adaptable will be essential. Organisations must prioritise AI fluency, invest in talent development and explore innovative solutions to remain at the forefront of this tech revolution.

The future belongs to those who can harness the power of AI. Whether you're a business executive, tech enthusiast or innovator, the time to act is now. The impact will be profound.

ARTICLES FROM OUR BI-WEEKLY NEWSLETTERS YOU MAY HAVE MISSED

***EngineerIT* publishes a newsletter twice a week. Here are highlights from the newsletter...**

Giving robots superhuman vision using radio signals

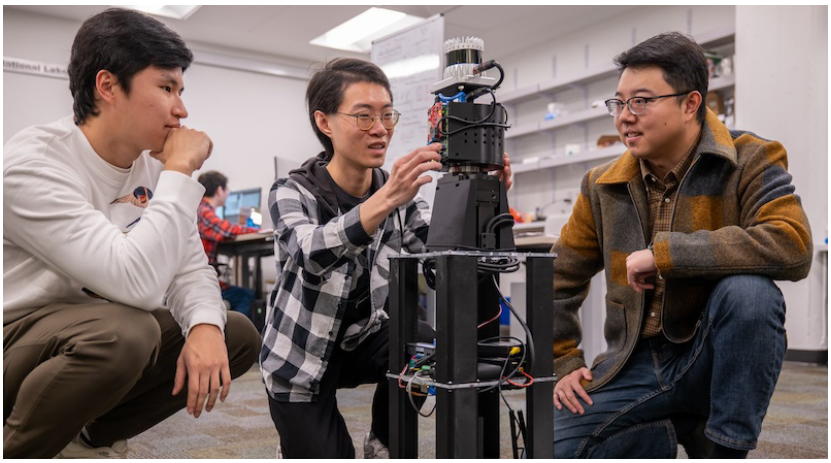
In the race to develop robust perception systems for robots, a persistent challenge is operating in bad weather and harsh conditions. For example, traditional, light-based vision sensors, such as cameras or light detection and ranging (LiDAR), fail in heavy smoke and fog.

However, nature has shown that vision doesn't have to be constrained by light's limitations – many organisms have evolved ways to perceive their environments without relying on light. Bats navigate using the echoes of sound waves while sharks hunt by sensing electrical fields from their prey's movements.

In a paper presented at the 2024 International Conference on Mobile Computing and Networking (MobiCom), Zhao and his team from the Wireless, Audio, Vision and Electronics for Sensing (WAVES) Lab and the Penn Research in Embedded Computing and Integrated Systems Engineering (PRECISE) Centre describe how PanoRadar leverages radio waves and artificial intelligence to let robots navigate even the most challenging environments like smoke-filled buildings or foggy roads.

Radio waves, with wavelengths longer than light waves, can better penetrate smoke and fog and even see through certain materials – all capabilities beyond human vision. Yet robots have traditionally relied on a limited toolbox: they either use cameras and LiDAR, which provide detailed images but fail in challenging conditions, or traditional radar, which can see through walls and other occlusions and produce crude, low-resolution images.

Researchers from the University of Pennsylvania School of Engineering and Applied Science (Penn Engineering) have developed PanoRadar – a new tool to give robots superhuman vision by transforming simple radio waves into detailed, 3D views of the environment. Read on



Advanced technology makes mining safer and more efficient

The Mandela Mining Precinct – a public-private partnership between the Department of Science, Technology and Innovation and the Minerals Council South Africa – hosted a showcase event at the CSIR International Convention Centre on November 18. The theme of the event – "Accelerating Mining RDI: Integrating Research Excellence with Mining Innovation" – highlighted innovative mining modernisation tools and solutions, people-centred approaches to technological change and human capital development programmes. Read on

Major changes as SAIMC and MESA Africa adapt to industry transformation

One of the most notable changes is the blurring of traditional dividing lines between the various ISA-95 layers. The ISA-95 model, which has long served as a framework for integrating enterprise and control systems, is now being reinterpreted to accommodate the seamless integration of processes across all levels of enterprise automation.

The Society for Automation, Instrumentation, Mechatronics and Control (SAIMC) board has approved the inclusion of computer engineering, mechatronics engineering, factory automation and process automation in the SAIMC and structural reorganisation of the Manufacturing Enterprise Solutions Association (MESA) Africa, resulting in the formation of two distinct additional advisory councils of the SAIMC: the Computer Engineering Advisory Council and the End User Advisory Council. This change is designed to enhance focus and effectiveness in addressing diverse stakeholders' unique needs and challenges. Read on

2025 cybersecurity outlook

KnowBe4, a cybersecurity platform that comprehensively addresses human risk management, has released its 2025 cybersecurity outlook from its team of global industry experts.

In 2024, the world witnessed cyber threats evolve faster than ever primarily due to the rise in the number and popularity of artificial intelligence (AI) tools. These tools assist cybercriminals in refining and making attack tactics more sophisticated and more difficult to recognise while helping cybersecurity professionals defend against attacks more effectively.

KnowBe4's global team of security awareness advocates, who are experts with decades of experience in the cybersecurity field, share their six main concerns:

1. AI-enabled tools for cyber defence and attacks will continue to improve.
2. Ransomware attacks will remain a problem.
3. The human factor in cybersecurity will become more of a focus.
4. Improvement of deepfake detection technologies.
5. Adoption of a zero-trust mindset and cyber-mindfulness.
6. Exploitation and the overlap of cybersecurity and human trafficking in Africa.

"The cybersecurity landscape is rapidly evolving and the dynamic between defenders and attackers has never been more complex," said Stu Sjouwerman, CEO of KnowBe4. "As we enter 2025, we must embrace the potential of AI to enhance our defences and protect organisations globally. Read on