

wattnow

THE OFFICIAL PUBLICATION OF THE SOUTH AFRICAN INSTITUTE OF ELECTRICAL ENGINEERS



LIGHTNING

SAIIE

AUGUST 2025

4	SAIEE President's Message
6	Industry News
14	Student News
22	Tertiary Education Facilities in South Africa
24	Legal Matters: CEO or IT manager?
26	Lightning Detection and its Operational Uses <i>Globally, lightning causes more than 20,000 deaths annually.</i>
30	Exploring the Correlation Between Elevation and Lightning Flash Density in Southern Africa <i>Why do some areas experience more lightning than others?</i>
34	Prevention is the Best Defence Against Lightning-Related Threats <i>Effective lightning protection requires proactive measures.</i>
40	Opinion
48	SAIEE Membership
50	SAIEE Council
52	SAIEE Centres
53	SAIEE Events Calendar



Dear **watt**now Reader,

As we delve into the awe-inspiring world of weather phenomena, lightning stands out as one of nature's most striking and powerful displays. Often regarded as both a beautiful and terrifying spectacle, lightning is a reminder of the immense forces at play in our atmosphere. This natural occurrence, caused by the discharge of electricity during thunderstorms, can cause spectacular visual displays and, at the same time, represents a significant hazard to life and property.

In this edition, we explore the science behind lightning. Our first feature article, "Lightning Detection and Its Operational Uses", discusses how proper precautions can safeguard people and operations. Read more on page [26](#).

On page [30](#), we delve into "Exploring the Correlation Between Elevation and Lightning Flash Density in Southern Africa", which explores why certain areas experience more lightning than others.

Effective lightning protection requires proactive measures that go beyond addressing direct strikes. Read more in the third feature article, on page [34](#), which discusses "Prevention is the Best Defence Against Lightning-Related Threats".

The September issue features Mining, and the deadline is 15 August. Please email your contributions to minx@saiee.org.za.

Herewith the August issue - enjoy the read!

I would like to wish all the SAIEE female members a fabulous Women's Day!

EDITOR'S NOTE

MANAGING EDITOR
[M Avrabos](#)

TECHNICAL EDITOR
J Buisson-Street

EVENTS
[G Geyer](#)

TRAINING ACADEMY
[Z Sibiya](#)
[L Molepo](#)

MEMBERSHIP
[C Makhalemele](#)
[T Lefutso](#)

ADVERTISING
[Avenue Advertising](#)

SAIEE HEAD OFFICE
18A Gill Street, Observatory, JHB
T 011 487 3003
www.saiee.org.za
Office hours: 8am - 4pm



SAIEE 2025 OFFICE BEARERS
President - V Ramnarain
Deputy President - P Madiba
Senior Vice President - Prof W Cronjé
Junior Vice President - J Motladiile
Immediate Past President - P Motsoasele
Honorary Treasurer - Prof P Naidoo
Honorary Vice President - Dr M Kahn
Chief Executive Officer - L Matutoane

ISSN: 1991-0452
South African Institute of Electrical Engineers. All material is strictly copyright and all rights are reserved. Reproduction without permission is forbidden. The views expressed in this publication are not necessarily those of the SAIEE. E&OE



Veer Ramnarain
2025/6 SAIEE President

The implementation of the Identification of Engineering Work (IDoEW) by the Engineering Council of South Africa (ECSA) has enhanced the relevance of Professional Engineers, Technologists and Technicians.

The IDoEW promotes safety and the protection of the public and the environment by ensuring that only registered professionals, who have demonstrated the required competence and academic qualifications, perform or take responsibility for engineering work. Defining the engineering work that registered professionals can perform is an enormous step in professionalising the public sector. Some of the recent construction disasters in South Africa point towards substandard artistry or regulatory non-compliance. IDoEW aims to ensure public safety and environmental protection by clarifying which tasks require the competency of registered professionals within specific categories.

Accountability now rests solely with the registered professionals, and this is the ticket and empowerment that we have long been asking for. No longer will engineering decisions be taken by individuals who do not possess the appropriate technical and professional competence and accreditation. This enhances the relevance of our members

as they contribute to the development of South Africa.

On 3 July 2025, ECSA held a successful Voluntary Association President's Forum, chaired by the President of ECSA. Discussions centred around the latest developments impacting our members. On the topic of IDoW readiness, responses from organisations indicated that a high percentage of 47% of individuals undertaking engineering work are not appropriately registered. This means that there would most likely be an influx of applications to ECSA for professional registration. ECSA has acknowledged that the change in the professional registration process to the Cycle Calendar approach, implemented a few years ago, has created a bottleneck in the processing of applications. ECSA has decided to revert to the Continuous Cycle approach as of 1 July 2025. To our members who have been awaiting processing, this will bring much-needed relief.

As an ECSA-recognised Voluntary Association (VA), the South African

Institute of Electrical Engineers (SAIEE) has been playing a crucial role in promoting professional registration and providing Continuous Professional Development (CPD) activities for its members, enabling them to maintain their professional registration. SAIEE has played an active role in promoting the Road to Registration webinars through ECSA. If requested by our members, we would hold further sessions for our new members. We have a comprehensive list of CPD-validated courses and actively market those that receive a favourable response. Our centres are encouraged to undertake surveys with members to determine additional CPD courses in demand. In addition to the courses available at a fee to our members, SAIEE also provides free CPD-validated

webinars for our members. As an institute, we take pride in maintaining our Mentorship documents.

The Professional Development Committee will revive the Mentorship program, which had been lacking a driver for some time. Working closely with ECSA, we will continue to add value to our members in this new era of professionalising the public sector.

By being active in partnerships with ECSA and other Voluntary Associations, SAIEE will continue to enhance the relevance of our members and partners, enabling them to see themselves as growing and contributing to the development of South Africa. **wn**

Veer N. RAMNARAIN – Pr Eng
2025 SAIEE PRESIDENT
BSc Electrical Eng, GCC, Dip EBM, MBA, MFMP



E: president@saiee.org.za



SAIEE CGC Hosts Chairperson's Business Breakfast



From left: Pascal Motsoasele (SAIEE), Prof Johnny Dladla (PM Resources), Veer Ramnarain (SAIEE), Sibulele Dlova (GameChange Solar), Keith Katyora (SAIEE CGC), Leanetse Matutoane (SAIEE)

On 6 May 2025, the SAIEE Central Gauteng Centre (CGC) hosted its annual Chairperson's Business Breakfast, bringing together over 50 professionals, executives, and emerging engineers for a morning of insight, collaboration, and renewed purpose. Held at the University of Johannesburg's School of Electrical Engineering, the event forms part of CGC's 10th anniversary programme under the theme: **Disrupt. Evolve. Sustain.**

The keynote address was delivered by Ms Sibulele Dlova, General Manager for Sub-Saharan Africa at GameChange Solar, who spoke with clarity and conviction on the region's energy transformation. Her message focused on the role of engineering leadership in shaping Africa's solar future, the value of investing in young professionals, and the strategic imperative of adaptability in a changing global energy landscape. GameChange Solar proudly supported the event as headline sponsor.

Attendees also heard from SAIEE President Veer Ramnarain, who delivered a powerful reflection on the Institution's founding members, their legacy, and the ethos that continues to underpin SAIEE's work. He emphasised the Institution's critical role within the broader engineering ecosystem and highlighted the importance of deepening its engagement with industry stakeholders. His address called for a unified effort to strengthen the profession and reinforce SAIEE's position as a custodian of excellence.

Keith Katyora, SAIEE CGC Chairperson for the 2025/26 term, outlined the

Centre's vision for the year, with an emphasis on strategic programming, leadership development, and sector-wide collaboration. He reaffirmed CGC's role as a bridge between engineering students, professionals, and decision-makers.

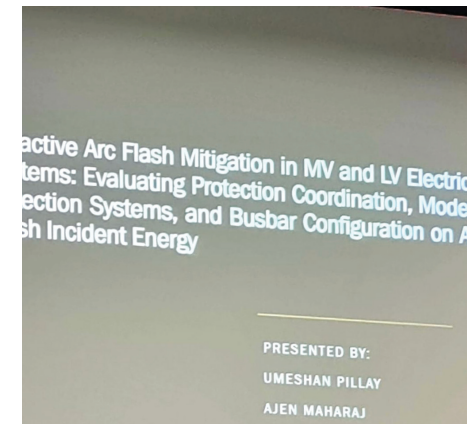
The programme concluded with closing remarks by SAIEE CEO Leanetse Matutoane, who reinforced the value of active Centres in shaping institutional outcomes and advancing the societal relevance of engineering.

Feedback from attendees was overwhelmingly positive, with many noting the quality of the programme, the depth of insights, and the value of reconnecting in a professional environment. A recurring message was the need for more physical industry events that foster dialogue, partnership, and visibility.

The Chairperson's Business Breakfast is one of several high-impact initiatives CGC will deliver this year, with upcoming engagements including the Skhaftini Sessions, Future-Fit Webinars, and the Energy Think Tank Series. **wn**



SAIEE KZN Centre – Arc Flash In-Person Lecture



We're proud to share the success of our first in-person/hybrid lecture for 2025 – the Arc Flash session held recently at the University of KwaZulu-Natal!

The event was a vibrant return to face-to-face knowledge sharing, with an enthusiastic audience, thought-provoking discussions, and brilliant insights from our esteemed speakers.

A heartfelt thank you to our guest speakers, Ajen Maharaj and Umeshan Pillay, for generously sharing their

expertise, and to the University of KwaZulu-Natal School of Electrical, Electronic and Computer Engineering for graciously hosting us.

We're energised by the turnout, after-session snacks, and engagement, and we look forward to many more enriching in-person lectures throughout the year. **wn**



A Heartfelt Thank You to UKZN - Strengthening Industry-Academia Collaboration

The SAIEE KZN Centre extends its sincere gratitude to the University of KwaZulu-Natal for its warm hospitality and continued support.

Not only did UKZN graciously host our recent in-person lecture, but they have also generously allocated a dedicated room for our committee to hold future meetings.

This gesture reflects a shared commitment to advancing electrical engineering through collaboration, mentorship, and knowledge-sharing.

A special thanks to Dr. Mohamed Fayaz Khan for making these arrangements

possible — your efforts are deeply valued.

We look forward to continuing our partnership and implementing impactful initiatives in 2025 and beyond! **wn**



GREEN Solar Academy wins SAPVIA Award



GREEN's Alexandra Hattingh, Tsakani Mashila, Amanda Dzivhani and Letlhogonolo "McDonald" Sekoa receive their award from Nicola Cencelli (left), Solar Business Development Lead at Juwi South Africa, the sponsors of the Empowerment Through Skills Development category.

GREEN Solar Academy was honoured with the Empowerment Through Skills Development Award at the inaugural 2025 SAPVIA Awards earlier this month, recognising its sustained and measurable impact in building technical capacity across the solar PV sector.

The SAPVIA Awards celebrate the significant contributions of SAPVIA members in solar PV, encompassing project development, quality installation, research, manufacturing, and the promotion of diversity. The awards aim to highlight and inspire excellence, innovation, inclusivity, and sustainable growth within South Africa's solar energy landscape.

"Everyone is an industry player and we are all working towards the same goal - the just energy transition - so the fact that SAPVIA recognises that skills development is an essential part of that, feels absolutely amazing!" said Amanda Dzivhani, COO of GREEN Solar Academy, in her remarks following the award.

She continued: "We put everything we have into ensuring that we provide quality training. That means keeping our training material up to date, working with trainers who are active in the solar sector, and making sure our content reflects what's genuinely happening on the ground."

A TRACK RECORD BACKED BY EVIDENCE

The Empowerment Through Skills Development category explicitly recognises organisations that have demonstrated exceptional commitment to enhancing workforce capabilities across the solar PV value chain. Judging criteria included the number of trained and certified individuals, the level of inclusivity, and the extent of partnership and collaboration, supported by verifiable documentation.

Since 2013, initially as Maxx Solar Academy and since 2019 as GREEN, the academy has trained nearly 10,000 individuals across South Africa and neighbouring countries. From SuperSolarSchool bootcamps to youth development projects and advanced compliance courses, GREEN offers a modular, accredited training model that caters to a broad range of learner needs, from unemployed youth to professional engineers. **wn**



POPIA non-compliance puts municipalities at risk



As South Africa's public services go digital, municipalities have become custodians of large amounts of highly sensitive information. Beyond essential services like water, electricity, and waste management, local governments now carry an even greater responsibility: protecting personal data. Despite this, only 51 out of 257 municipalities submitted their mandatory data protection and access to information reports in 2024.

The Protection of Personal Information Act (POPIA) sets strict, non-negotiable rules for how personal data must be collected, stored, used and secured.

Non-compliance not only breaches legal obligations, but it also undermines public trust. "Having the right laws in place is important, but that's just the starting point.

Real protection happens when POPIA and cybersecurity work hand-in-hand – you can't separate the two. POPIA tells you what needs to be protected, but it's solid cybersecurity that does the protecting," says Calin Cloete, Enterprise Security Solutions Lead at ESET Southern Africa.

POPIA casts a wide net, applying to all public and private bodies – municipalities included. The act mandates the prompt reporting of data breaches to the Information Regulator and immediate notification of affected individuals.

To comply, municipalities must appoint Information Officers, develop Promotion of Access to Information Act (PAIA) manuals, register their data processing activities and maintain secure systems. Despite these clear obligations, compliance remains worryingly low – underscoring the ongoing gap between policy and practice.

"This alarming lack of compliance paints a troubling picture. When municipalities lack basic IT governance or strong internal controls, they're not only failing audits but also leaving systems like billing platforms and service portals

vulnerable to attack. It's not enough to have policies on paper. Municipalities require genuine, verifiable security measures to safeguard personal data. Without them, residents' privacy and security are at risk," says Cloete.

The consequences are far from abstract. In the past three years alone, an alarming number of public institutions, including municipalities, have fallen victim to cyberattacks. Incidents have stretched across the country, bringing key services to a standstill from the KwaDukuza Local Municipality in KwaZulu-Natal to the City of Cape Town in the Western Cape.

"This year's municipal by-elections across South Africa add another layer of complexity. Securing the digital systems that support these elections is essential.

A cyberattack could compromise voter data or manipulate election information. With public confidence in institutions already fragile, even a minor security breach could have serious consequences for voter turnout and the perceived legitimacy of the results," says Cloete.

Moving forward, digital responsibility must go beyond POPIA compliance to recognising that privacy and service delivery are fundamentally linked. By securing their digital infrastructure, municipalities can enhance public confidence – whether people are accessing everyday services or participating in important events, such as elections. Cybersecurity is no longer just a background task, but a pillar of ethical, local leadership. **wn**

Water-shedding crisis raises alarm for improved firefighting solutions



Michael van Niekerk
Chief Executive | ASP Fire

As South Africa faces ongoing water shortages and the growing threat of water-shedding, concerns about the impact on firefighting efforts have emerged. ASP Fire CEO Michael van Niekerk emphasises the need for innovative solutions in areas where water supplies are compromised.

Water-shedding in South Africa significantly impacts municipal and community firefighting capabilities. It limits the availability of water in municipal reservoirs and hydrants, making it challenging to maintain adequate water pressure and supply during firefighting operations.

With less water available, the risk of fires spreading increases, especially in dry and windy conditions. Firefighters may face delays in accessing water, which can hinder their ability to respond quickly and effectively to any fires.

"It is not just about water shedding but also the general lack of water in some areas," says van Niekerk. "I have been involved with projects where water is only available during certain hours. In such cases, building regulations suggest that the owner should assess the risk and, if necessary, provide an on-site water supply. However, there is no legal obligation to do this; it is more of a recommendation."

Van Niekerk points out that, notwithstanding the current regulations, business owners do not fully appreciate the risks of not having highly reliable, adequate water sources on hand, especially where they have high-risk operations or storage facilities, or have capital-intensive production lines, or are exposed to significant challenges related to business continuity or market loss. However, he stresses the importance of collective efforts in addressing firefighting challenges.

"A unified approach to community firefighting is lacking. For instance, setting up a communal fire tank and pump to serve multiple properties would alleviate the burden on individual owners. It would be cost-effective and provide a reliable water source for firefighting," he argues.

In rural and semi-rural areas, van Niekerk suggests leveraging existing infrastructure, such as farm Irrigation systems, to supplement water supplies for firefighting purposes. "Using existing resources, like irrigation systems on farms, to supply water for firefighting could be a viable solution in these regions."

Establishing communal water tanks in strategic locations can ensure a reliable water source for firefighting and other emergency needs. Another proactive measure is to encourage the use of rainwater harvesting systems to supplement water supply for firefighting. Lastly, investing in infrastructure improvements can enhance water storage and distribution systems, reducing the risks associated with a fire brigade rendered useless due to a lack of water. **wn**



Key sectors served by ACTOM's equipment supply and solutions offering include:

- | | | | |
|------------------|-----------------------|----------------|--------------------|
| Power Generation | Healthcare | Paper & Pulp | Renewable Energy |
| Transmission | Industrial Processing | Petro-chemical | Sugar |
| Distribution | Mining | Rail Transport | Textile |
| Utilities | Oil & Gas | Signalling | Water & Sanitation |

ACTOM, offers a winning and balanced combination of manufacturing, service, repairs, maintenance, projects and distribution of electro-mechanical equipment through its 33 outlets throughout Sub-Saharan Africa.

Your one-stop global energy solutions partner



Discussing Green Energy's Sustainability, Security, and Growth



BMF & YDE Staff.

Why is South Africa's decarbonisation journey essential for energy security, growth, and human dignity? What role does the private sector play? And how is the energy industry closing the gaps between energy producers, buyers, and public infrastructure?

Why is South Africa's decarbonisation journey essential for energy security, growth, and human dignity? What role does the private sector play? And how is the energy industry closing the gaps between energy producers, buyers, and public infrastructure?

Some of the questions raised and answered during the Energy Security and Sustainability Dialogue, a special event hosted by the Gauteng branch of the Black Management Forum (BMF) and Yellow Door Energy, an independent power producer that generates and sells energy to the South African market.

The evening, hosted at the South African Institute of Chartered Accountants (SAICA) in Sandton, provoked interesting and wide-ranging discussions, probing the minds of three expert panellists: Forbes Padayachee, the CEO of Yellow Door Energy South Africa (YDE); Hlatse Nkune, Energy Finance Principal at Nedbank; and Thembanani Bukula, CEO of power trader POWERX, a YDE customer and essential player in the aggregator and trading market in South Africa. In a discussion hosted by Ayanda Masina, they looked at the why and how of energy transitions in the country.

WHY DECARBONISE?

The shift in energy generation addresses essential economic and social realities. Padayachee gave three reasons why it's worth pursuing decarbonisation and investing in renewables.

The first is that decarbonisation and renewables reduce costs for the country

and its companies as they adopt sustainability, circular economies, and more affordable energy sources. Both also benefit from competitive access to other markets. Many regions of the world have fees tied to the output of products and services that can be mitigated with green credentials.

However, Padayachee from YDE emphasised that the most crucial issue is energy security, stating, "In South Africa, we have ancient coal-fired power plants. Those power plants will need to be decommissioned at some point, as most of them have already exceeded their useful life. It's like the cars we had when we went to university.

At some point, it will say Enough is enough. I can't go on working anymore, and then you've got to replace it. We need to replace our outdated power systems with various energy sources. However, affordability must always be a key consideration for a country. Renewable energy can play a big role in that aspect."

PRIVATE SECTOR SUPPORT

Another notable theme was the role of private sector innovation in building a resilient energy future for South Africa. Some are concerned about private sector involvement in developing energy, as it could lead to privatised energy and the lack of government-focused goals and proper regulation. However, this is not the case to date. Instead, collaboration between the public and private sectors is accelerating energy transformation and funding.



Forbes Padayachee
CEO, Yellow Door Energy South Africa.

Nkune highlighted the urgent need to upgrade the grid infrastructure to meet South Africa's energy transaction commitments. He underscored that the Transmission Development Plan (TDP) of 2024 requires approximately 30 GW to be grid-connected by 2030, 56 GW by 2034, and 14,500 km worth of transmission lines.

The Minister of Electricity and Energy has also indicated that the Government needs about R440 billion to modernise and expand transmission, and acknowledged that the Government is not in a position to provide that kind of support; hence, the introduction of the Independent Transmission Programme, which will enable private participation. According to Nkune, private sector investment is expected to play a significant role in the transmission expansion.

"Government indicated that in terms of a just transition, there is significant investment required. From a fiscal perspective, it's not something that the Government will do because it has to



Thembanani Bukula
CEO, POWERX.

prioritise other social needs that we all require. So, it is an aspect where the private sector is participating."

CLOSING THE GAPS WITH POWER TRADERS

South Africa's energy transition has little merit if it cannot reach end customers. This issue is particularly pressing for large power consumers, such as vehicle and food manufacturers, that export their goods to other markets. Specifically, they require access to green energy to meet carbon-related regulations, such as the European Union's Carbon Border Adjustment Mechanism.

POWERX's Bukula explained this mechanism. When companies ship goods produced using fossil fuels, they face duties that make them less competitive.

They can mitigate these costs through green energy sources. However, obtaining this energy poses a challenge, as many renewable sources capable of meeting their needs are not nearby. This is where power traders step in.

"Eskom and the municipalities do not have much green power in their energy mix, and have minimal abilities to build green power projects. What traders do is go to the power producers and negotiate to buy the power that they would produce. We then sell that power to the entities that require it. We do not have infrastructure—power lines and transmission lines—so we negotiate a fee to use either Eskom or municipal systems."

These sales don't necessarily deliver that power directly to the customer. Instead, they use an offset system called virtual trading, balancing out the requirements of a company's direct energy use with the green power they purchase.

In this manner, it becomes possible to address pressing power issues immediately and deliver more affordable energy to a broader audience. The process also unlocks more investment capital from financial providers.

COLLABORATING ON SOLUTIONS

The event hosted by BMF and Yellow Door Energy provided substantial insight. It provided attendees with the opportunity to ask questions and participate in the discussion. Above all, it created a platform for collaboration and the development of solutions for South Africa's energy future.

Padayachee said she looked forward to future gatherings and continuing the collaboration with the Black Management Forum. **wn**

Why Engineering Students should join the SAIEE



Engineering students in South Africa are highly encouraged to consider joining the South African Institute of Electrical Engineering (SAIEE). This prestigious organisation offers numerous benefits that significantly enhance their academic and professional development.

ABOUT THE SAIEE

Formed in 1909, the SAIEE has ±6000 members professionally engaged in various engineering activities, including academic research, manufacturing, electronics, telecommunications, measurement and control, mining, and power infrastructure services. Members make meaningful contributions to the quality of life in communities and the steady advancement of technology. Their efforts are acknowledged in many countries worldwide.

One key advantage of joining the SAIEE is access to a network of experienced professionals in the engineering field.

As members, engineering students have the opportunity to connect with industry experts who can provide valuable mentoring and career guidance. These connections can help students gain insights into the latest trends and developments in the industry, as well as potential job opportunities and internships.

Furthermore, SAIEE membership provides exclusive events, workshops, and seminars tailored to help engineering students enhance their skills and knowledge.

These events offer valuable opportunities for students to learn from experts in the field, collaborate with peers, and stay updated on the latest advancements in engineering.

The SAIEE Student membership is free from 1 December 2024, and with that, the SAIEE Student member (StM) receives the following benefits:

- **Jobs portal for WIL**
SAIEE Student Members receive preferential placing for their Work Integrated Learnership (WIL) with our SAIEE Corporate Partners
- **Mentorship**
The SAIEE has a cohort of mentors who are willing and eager to assist our student members with their studies and career guidance
- **Exclusive Networking Events**
StMs attend all SAIEE events for free and are exposed to industry decision-makers

- **CPD training discounts**

To maintain your continuous development, the StM receives significant CPD training discounts

- **Charge Reward Programme earnings**

As a StM, when attending SAIEE events, you earn Charge Reward Points, which can be claimed against paying for training courses, etc.

- **Bursary programme**

StMs receive preferential treatment when they apply for a SAIEE Bursary

- **Publication access**

Student members have access to all SAIEE publications since its inception in 1909, which include the monthly online wattnow magazine and the peer-reviewed Africa Research Journal

- **Site visits**

SAIEE Student members are invited to site visits free of charge, which is CPD accredited, where you can learn hands-on how manufacturing facilities operate

- **SAIEE Centres**

SAIEE has nine centres nationwide, and we encourage students to get involved at their local SAIEE Centre and represent your student chapter on the Centre EXCO committee.

The South African Institute of Electrical Engineering is a valuable investment for students from all engineering disciplines and tertiary establishments who are serious about advancing their careers in engineering. To learn more about joining the SAIEE, [click here](#). **wn**



Serving Since 1909

Formed in 1909, The South African Institute of Electrical Engineers sports ± 6000 engineering professionals.

Why Join Us

Our members are professionally engaged in various engineering activities, including academic research, manufacturing, electronics, telecommunications, measurement and control, mining, and power infra-structural services. Members make meaningful contributions to the quality of life in communities and the steady advancement of technology. Their efforts are acknowledged worldwide. Join us today and start making a difference!

Our Purpose

To enhance the practice of electrical engineering in South Africa and the stature of our members through knowledge, networking, influence, education and communication.



Student Bursaries

Our bursaries are for candidates who have completed a first-year study for a degree or diploma in Electrical, Electronic or Computer Engineering at an accredited South African tertiary institution.



Skills Development

One of our core objectives is to harness and foster the growth of students to study Science, Technology, Engineering, and Mathematics (STEM) subjects.



Student Activities

Becoming involved in a Student Chapter and participating in meetings can teach a student member valuable business skills. SAIEE offers mentorship, coaching and vacation work.



Contact Us

- 📍 SAIEE House, 18A Gill Street, Observatory, JHB
- ✉ 011 487 3003
- 🌐 www.saiee.org.za

EDHE-Absa Innovation Challenge Launch champions youth entrepreneurship



The launch event at the Mangosuthu University of Technology marks a bold step towards inclusive innovation and youth-driven economic transformation in South Africa's public universities.

In an educational show of collaboration and commitment to youth-led innovation, Absa, and Universities South Africa (USAf), through the Entrepreneurship Development in Higher Education initiative.

The Education (EDHE) programme officially launched the EDHE Absa Innovation Challenge on Wednesday, 25 June 2025, at Mangosuthu University of Technology (MUT) in Umlazi.

The Absa-EDHE Innovation Challenge is open to students studying at any of the 26 public universities in South Africa. It is also extended to alumni who have graduated within the last three years. The areas of competition include Healthtech, Edutech, Greentech, Agritech, and Fintech. Finalists will undergo an incubation programme and pitch at the finals in November for the grand prize of R500 000.

The event brought together leaders in higher education, entrepreneurship, and the Absa Group to mark the start of a nationwide call for entrepreneurial solutions that address fundamental societal challenges.

The launch at MUT, a historically disadvantaged institution based in a vibrant township community, underscored the significance of inclusive innovation. In her keynote address, Professor Nokuthula Sibiya, The Vice-Chancellor and Principal of MUT spoke of the university's bold vision to establish a Centre for Entrepreneurship, which will support student-led start-ups with mentorship, workspace, and early-stage investment.

On behalf of Absa, Nonhlanhla Magagula, Head of Absa's Corporate Citizenship Programmes, emphasised the transformative intent of the initiative: "This is not about supporting the next generation of small businesses. It's about unlocking the next generation of changemakers who are willing to challenge the status quo and build new realities from the ground up.

The EDHE Absa Innovation Challenge is now officially open for entries. Students and alumni are encouraged to submit applications that demonstrate creative problem-solving, practical scalability, and a profound social impact.

[Click here](#) for more information. **Wn**

WIN UP TO

R 500 000

IN CASH PRIZES AND MORE

ENTRIES ARE OPEN 25 JUNE - 8 AUGUST 2025
LEARN MORE AT WWW.EDHE.CO.ZA

EDHE Absa Innovation Challenge 2025

UJ Student Chapter toured the SAIEE Museum



On the day of the recent SAIEE Central Gauteng Centre (CGC) Annual General Meeting, the SAIEE University of Johannesburg's (UJ) Student Chapter had the privilege of being invited to a tour of the SAIEE Museum, located at the SAIEE House in Observatory, Johannesburg.

The primary objective of the museum tour was to expose the UJ students to the historical foundations, technological progress, and pioneering achievements in electrical and electronic engineering over the years. The experience was designed to inspire, educate, and deepen the students' appreciation of the profession they are studying towards.

The museum offered an engaging and visually rich timeline of technological evolution, featuring:

- Early communication systems and radios.

- Vintage electrical instruments and measuring tools.
- Telephony developments from the early 1900s.
- Historical contributions by South African engineers in global engineering milestones.

The tour was led by passionate and highly knowledgeable guides who took their time to explain each exhibit in great detail, drawing connections between past innovations and present-day technologies. The interactive nature of the visit allowed students to ask questions and relate historical concepts to their academic learning.

Following the tour, Phemelo Montsho, chairperson of the UJ Student Chapter, received overwhelmingly positive feedback from the students. Common sentiments included:

- A renewed respect for the engineering profession.
- Increased motivation to contribute meaningfully to the field.
- A sense of pride in being affiliated with an institution like the SAIEE, which preserves and honours the

legacy of engineering in South Africa.

Many students expressed how fascinating it was to see the roots of electrical engineering and were inspired by the vision and resilience of those who came before us.

Given the educational value of the museum tour, I recommend that future student leaders and engineering departments prioritise similar experiences for other cohorts. It is also advisable that such tours be formally incorporated into first-year orientation programmes or final-year transition events to reinforce the historical significance of the profession.

The SAIEE Museum tour was a truly enriching experience that left a lasting impression on our student members. It not only deepened their understanding of the engineering discipline but also reinforced the importance of preserving our professional history. We are deeply grateful to the SAIEE for the opportunity and hope to participate in more initiatives of this nature in future. **Wn**

SAIEE CGC and National AGMs



The SAIEE UJ Student Chapter members participated in the SAIEE Central Gauteng Centre (CGC) and the National Annual General Meetings (AGMs), which took place on 15 April 2025 and 24 April 2025, respectively, both hosted at SAIEE House in Observatory, Johannesburg.

SAIEE CGC AGM

Following a successful and enlightening tour of the SAIEE Museum, our students attended the SAIEE CGC AGM. The meeting was a significant moment for the region, as Engineer Keith Katyora was officially appointed as the new Chairperson of the Central Gauteng Centre, succeeding Engineer Pascal, who gracefully stepped down after his term.

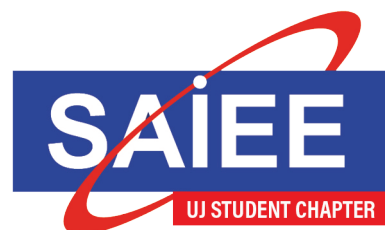
Additional members were also welcomed into the CGC Committee, and attendees were presented with various future projects and strategic plans. These included outreach initiatives, professional development programmes, and efforts to increase student engagement across institutions.

Students found the AGM both educational and inspiring, especially seeing the level of structure and leadership involved in the functioning of SAIEE. Those who were not yet members expressed a strong interest in registering and becoming active participants in SAIEE's student and professional community.

SAIEE NATIONAL AGM

A week later, our students were also allowed to attend the SAIEE National AGM, where broader updates concerning the Institute's national direction, structure, and achievements were presented. The meeting further deepened students' understanding of SAIEE's influence and role within the South African engineering industry.

Both AGMs were valuable experiences for our students, offering exposure to real-world engineering leadership, governance, and professional engagement. We extend our gratitude to SAIEE for the opportunity and for covering transport costs. These engagements not only motivated students academically and professionally but also encouraged many to consider more active participation in SAIEE in the future. **wn**



SAIEE UJ Student Chapter Career Expo



The Engineering Career Expo, hosted at the University of Johannesburg on May 9, 2025, in collaboration with various engineering student chapters, was a huge success. These included representatives from the Electrical/ Energy, Mechanical, and Civil Engineering departments. As the SAIEE UJ Student Chapter, we were proud to help lead this impactful initiative that sought to connect students directly with industry professionals.

The Career Expo was organised to expose engineering students to professionals and experts from the corporate world, allowing them to engage, learn, and ask relevant questions about life after graduation.

The event provided a valuable platform for:

- Gaining insight into industry expectations and career pathways.
- Understanding graduate recruitment and internship opportunities.
- Building networks with established professionals in various fields.

Invited participants included companies from across the Electrical/Energy, Mechanical, and Civil Engineering sectors.

These guests ranged from industry engineers to graduate recruitment representatives and project managers. In addition, we were honoured to have invited the SAIEE UNISA Student Chapter to form part of the SAIEE exhibitor group.

Their participation further strengthened the spirit of collaboration between institutions and helped showcase SAIEE's student engagement on a broader scale.

To ensure smooth operations and an enjoyable experience for all involved,

student chapters collectively contributed to event logistics, covering:

- Venue preparation
- Marketing and communication materials
- Catering (lunch and refreshments)

Each participating chapter contributed a total of R2,386.44, which was used to ensure a professional, welcoming, and informative event for both guests and students.

The Engineering Career Expo, held on May 9, 2025, was a remarkable success that showcased the power of student leadership, inter-chapter collaboration, and strong industry engagement.

The involvement of the SAIEE UNISA Student Chapter added further value to the event and reinforced our shared mission to equip students with relevant knowledge and networks.

As the SAIEE UJ Student Chapter, we are proud to have co-hosted an event that left a meaningful impact on our student body and look forward to initiating similar collaborations in the future. **wn**

SAIEE UKZN and IQRAA Trust Inspire Future Engineers Through Hands-On STEM Outreach



Top student receives a prize for outstanding participation during the session.

The SAIEE UKZN Student Chapter, in collaboration with IQRAA Trust, recently hosted a dynamic STEM outreach workshop for Grade 11 learners from Brettenwood High School.

The session took place at the IQRAA Knowledge Centre at Hunt Road Secondary School in Durban.



Students with the UKZN SAIEE Committee.

Learners were introduced to electrical, electronic, and computer engineering through an interactive Arduino Uno workshop. Through guided activities in basic coding and circuit building, participants gained practical exposure to the tools and thinking that define modern engineering.

The session focused on turning theory into application. Learners were encouraged to explore, experiment, and solve problems-developing critical thinking and teamwork skills along the way. One standout participant was recognised with a prize for exceptional engagement and innovative thinking.

The initiative was supported by IQRAA Trust, whose focus on educational

upliftment continues to create impactful learning opportunities. The University of KwaZulu-Natal contributed Arduino kits and learner gifts, helping to create a meaningful and memorable experience.

By introducing high school learners to engineering in a hands-on, accessible format, the collaboration aims to spark early interest in STEM and open pathways to future careers in science and technology.

This outreach highlights the value of partnerships between academia, industry organisations, and community stakeholders in driving educational impact and shaping tomorrow's innovators. **wn**



Students with UKZN SAIEE Committee and Dr. Mahmoud Youssef Baker (Executive Chairman of Iqraa Trust).



Students building circuits.

The SAIEE UKZN introduces new committee



From left to right: Mihir Singh (Communications Director), Shankara Naidoo (Events Co-Ordinator), Saaliha Paruk (Administrative Director), Tumelo Sibiyi (Activities Co-Ordinator), Ntuthuko Zulu (Chairperson), Muhammad Buckus (Treasurer), Nombulelo Ngidi (Vice Chairperson), and Dr. Mohamed Fayaz Khan (Vice Chairperson of SAIEE KZN Centre).

The SAIEE Student Chapter at the University of KwaZulu-Natal has officially elected its Executive Committee for 2025.

This dedicated team of professionals and students is passionately committed to enhancing professional development, fostering industry engagement, and creating valuable networking opportunities for students enrolled in the School of Electrical, Electronic, and Computer Engineering.

Our mission centres around cultivating a vibrant and inclusive community that not only attracts new members but also establishes meaningful partnerships with industry leaders and academic peers. This collaborative approach aims

to advance both education and research within the diverse fields of electrical, electronic, and computer engineering.

To achieve these goals, we organise a variety of activities, including hands-on technical workshops that provide practical skills and knowledge, as well as collaborations with industry experts that offer insights into the latest trends and technologies. We invite you to stay updated on our ongoing efforts and initiatives, as we work passionately to enhance the overall student experience at the University of KwaZulu-Natal! **wn**

Universities in South Africa



It is only through education that people are able to improve themselves. One of the most important factors for escaping from poverty is education. The only way a society can continue to grow and prosper is through proper education at all levels.

Cape Peninsula University of Technology
Call Centre: +27 21 959 6767

Central University of Technology
Bloemfontein: +27 (0)51 507 391
Welkom: +27 (0)57 910 3500

Durban University of Technology
Switchboard: 031 373 2000

Mangosuthu University of Technology
Call Centre : 031 907 7111

Nelson Mandela University
Call Centre : 041-504 1111

North-West University
Call Centre : 0860 169698

Rhodes University
Call Centre : +27 46 603 8111

Sefako Makgatho Health Sciences University
Call Centre : (012) 521-4111

Sol Plaatje University
Call Centre : 053 491 0000

Stellenbosch University
Call Centre : +27 21 808 911

Tshwane University of Technology
Call Centre : +27 21 808 911

University of Cape Town
UCT switchboard: +27 (0)21 650 9111

University of Fort Hare
East London: 043 704 7000
Bhisho Campus : 040 608 3407
Alice Campus: 040 602 2011

University of Johannesburg
Call Centre : +27 11 559 4555

University of KwaZulu-Natal
DBN: +27 31 260 1111
PMB: +27 33 260 5111

University of Limpopo
Switchboard: (015) 268 9111
(015) 268 3332 / (015) 268 3276

University of Mpumalanga
Switchboard: (013) 002 0001
info@ump.ac.za

University of Pretoria
Switchboard: +27 (0)12 420 3111
info@up.ac.za

University of South Africa
Switchboard: 012 441 5888
study-info@unisa.ac.za

University of the Free State
Bloemfontein Campus: +27 51 401 9111
Qwaqwa Campus: +27 58 718 5000
South Campus: +27 51 401 9111

University of the Western Cape
Call Centre : +27 21 959 2911

University of the Witwatersrand
General enquiries : +27 (0)11 717 1000
Admission enquiries: +27 (0)11 717 1888

Vaal University of Technology
Call Centre : +27 (0)861 861 888
Admission enquiries: +27 (0)16 950 9356

University of Zululand
Switchboard : +27 (0)35 902 6000

Walter Sisulu University
Mthatha Campus : 047 502 2844

University of Venda
Call Centre: 015 962 8000

A single flaw can break an entire system

IN ENGINEERING, PRECISION IS NON-NEGOTIABLE.
THE SAME PRINCIPLE SHOULD APPLY
TO YOUR DATA SECURITY AND PRIVACY PROTOCOLS.



Don't let a compliance gap put your business at risk. As an official legal panel member for the SAIEE, Fairbridges Wertheim Becker, provides expert legal services to ensure your business stays compliant.

POPIA Compliance: Expert guidance to ensure your business meets the requirements of the Protection of Personal Information Act.

Data Privacy Reviews: Thorough assessments to identify gaps and mitigate risks.

Training & Workshops: Tailored training to equip your team with the knowledge to manage data privacy effectively.

CONTACT US FOR A DISCUSSION REGARDING YOUR NEEDS TODAY



Jodi Poswelletski
DIRECTOR
SPECIALIST IN DATA PRIVACY AND POPIA

Phone: +27 11 593 3724
Mobile: +27 71 224 4665
Email: jodi.p@fwblaw.co.za

Clifton Motshepe
ASSOCIATE

Phone: +27 11 268-0250
Mobile: +27 71 889 7473
Email: clifton.m@fwblaw.co.za



CEO or IT Manager?

WHO TAKES THE FALL FOR A DATA LEAK UNDER POPIA?



It's the headline nobody wants to read: "Engineering group fined R10 million; CIO charged over patient-monitoring data leak." Swap in "CEO" or "Project Director" and the message stays the same: under South Africa's Protection of Personal Information Act, Act 4 of 2013 (POPIA), liability is no longer a faceless, corporate problem.

By: Jodi Poswelletski
Fairbridges Wertheim Becker

Decision-makers can be held personally accountable when personal information escapes their control, even if they never had direct access to the compromised server.

For SAIEE-member businesses that juggle drawings, IoT telemetry and staff files, it pays to know precisely where the legal buck stops when the network lights flash red.

HOW POPIA PINS RESPONSIBILITY

POPIA begins with the concept of a "responsible party" - the person or organisation that determines why and how personal information is collected, processed, and stored.

On paper, that party is usually the company itself, but directors are not immune to liability. Sections 100-109 of POPIA impose fines and even prison sentences (of up to ten years) on individuals who wilfully or negligently fail to secure personal information, obstruct an Information Regulator investigation, or ignore an enforcement notice. Add the Companies Act's "delinquent director" provisions and the boardroom suddenly looks a lot less bulletproof.

WHERE THE REAL EXPOSURE SITS IN AN ENGINEERING ENVIRONMENT

Responsibility in a typical engineering firm travels along a chain, and any weak link can snap that chain, and point the finger:

- The CEO or Managing Director approves budgets and strategic data initiatives. If security funding

has been repeatedly deferred in favour of other priorities, the CEO may face accusations of reckless trading or negligence once a breach occurs.

- The Information Officer (often the company secretary, compliance head or CIO or anyone from senior management) is required to be registered with the Information Regulator, maintain processing records of personal information and report breaches of personal information "without undue delay". Failure to do the same could attract penalties and administrative fines, and not just a corporate embarrassment.
- The IT Manager or Head of Operational Technology implements firewalls, backups and access controls. If those controls were poorly configured or ignored, civil claims for professional negligence (and internal disciplinary action) will follow swiftly.
- Project leads and senior engineers routinely handle client specifications, site photographs, contractor details, and sometimes patient data in medical device projects. Saving that data on an unencrypted laptop or sharing it through unsecured links can trigger both POPIA penalties and internal misconduct proceedings.

In short, liability is a relay baton. If one runner drops it, everyone-from engineer to executive-may feel the burn.

TURNING THEORY INTO PROTECTION

Good governance, rather than blame-shifting, remains the best shield. Executives can take five intertwined actions that protect the company and themselves without adding layers of bureaucracy.

First, place POPIA on every board agenda and keep minutes that show genuine debate, budgets and deadlines. Courts are more lenient towards directors who can demonstrate that they took privacy seriously before disaster struck.

Second, give the Information Officer real teeth. Registration is the easy part; authority is the more challenging part.

Delegate the power to insist on policy changes, staff training and third-party POPIA audits, then demand quarterly POPIA compliance reports.

Third, map your data flows. Network diagrams explain where cables run;

they do not reveal where personal information lives. Track the entry points (HR onboarding, subcontractor portals), storage locations (cloud SCADA, BIM servers), and exit routes (RFQ packs, marketing lists). Without such a map, you cannot secure the terrain.

Fourth, rehearse data-breach drills. Treat them like blackout simulations: who isolates the compromised laptop, who uploads the incident to the Information Regulator's e-portal, who drafts the notification letter to affected data subjects? A time-boxed dry run exposes gaps and serves as proof of proactive governance.

Finally, embed privacy commitments in both contracts and key performance indicators. Supplier agreements should impose POPIA-level safeguards, while executive bonuses should be linked to hard security metrics. When career advancement depends on zero critical vulnerabilities, priorities sharpen quickly.

THE UNCOMFORTABLE TRUTH

Many boards still rate "loss of IP" above "loss of personal data." POPIA flips that calculation: a stolen CAD file can harm competitiveness, but leaked employee health records can trigger statutory fines, civil suits, and career-ending headlines. Regulators and courts rarely care whether the breach originated with a misconfigured PLC or a phishing e-mail - they care whether leadership could, and should, have prevented it.

The question is not whether a data incident will reach your organisation; it is who will carry the can when it does. A CEO who treats privacy as "just IT's problem" courts personal liability.

An IT manager who ignores board-level directives does the same. Only shared vigilance, clear accountability and rehearsed response plans provide real insulation. In a POPIA world, the fall guy could be anyone—unless everyone plays their part. **wn**

20 **comtest** **years**
measure with confidence

NEW accessory
NEW application
NEW Price

The Fluke Acoustic Imager and SB140 Sound Beacon - a powerful duo for pinpoint accuracy.

The ii500 Acoustic Imaging Camera. NOW more affordable than ever!

FLUKE

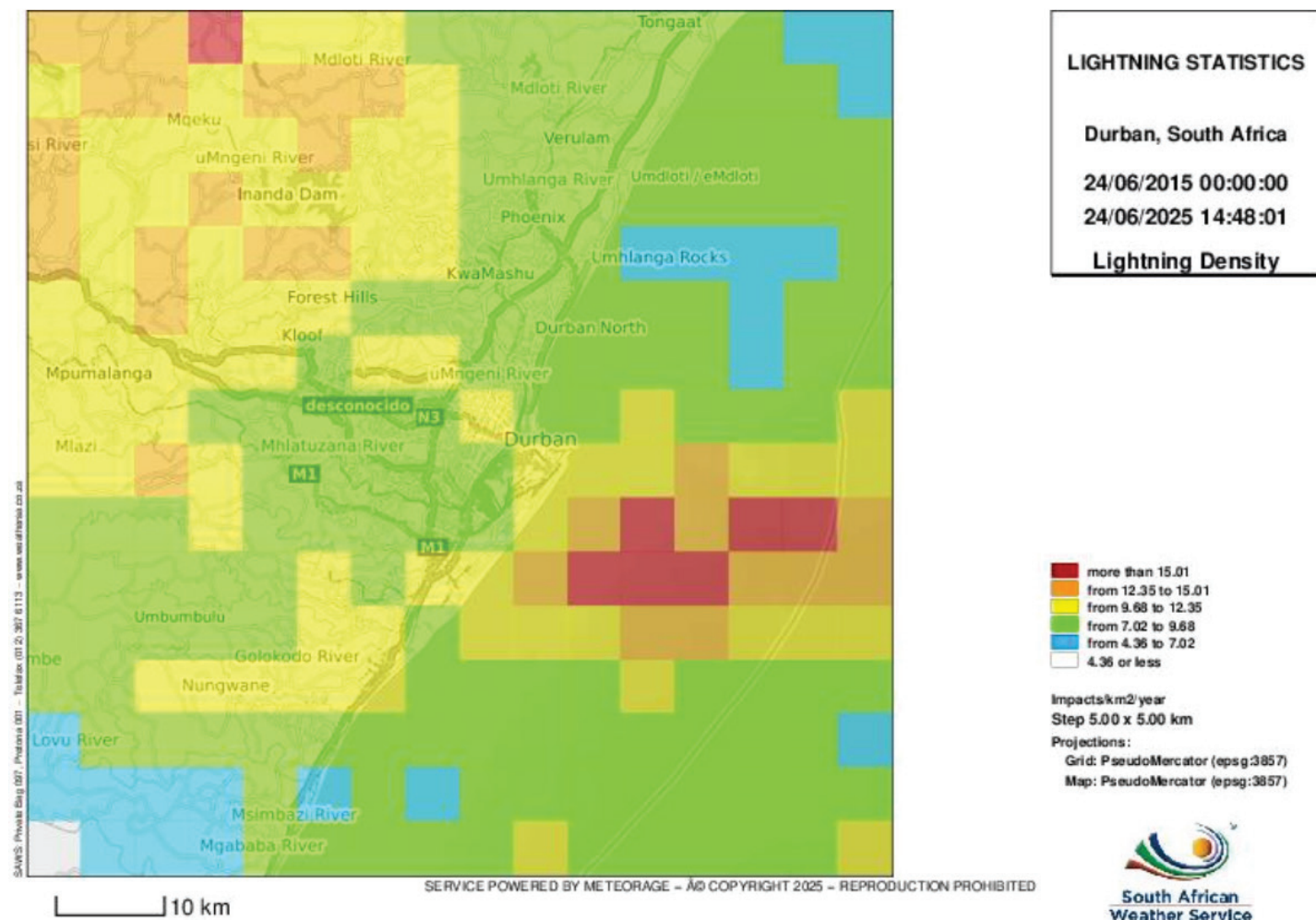




*BY: Solal Bordenave,
Anouk Inial,
Rydall Jardine,
Michelle Hartsliet*

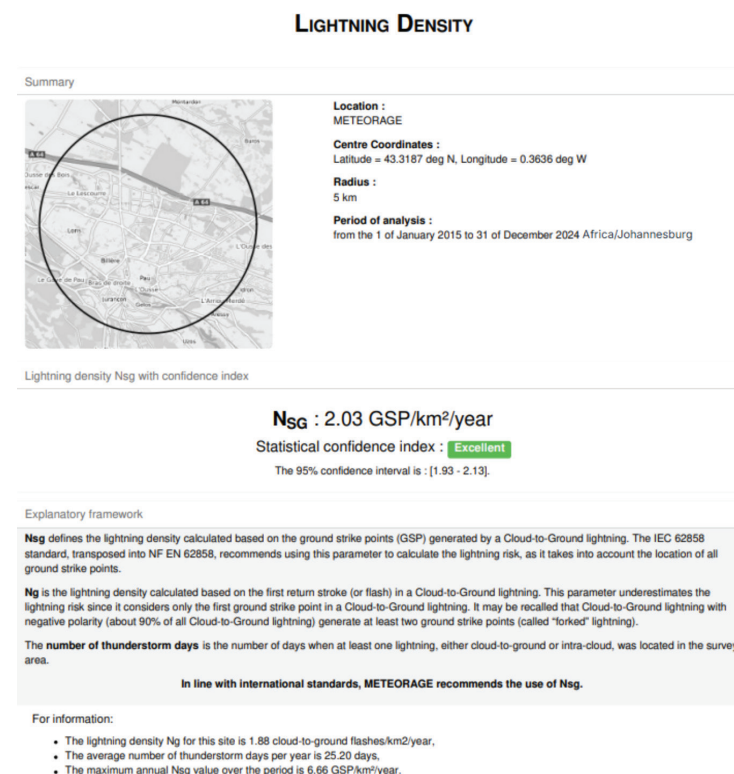
This high-resolution, real-time data provides essential support for lightning risk mitigation strategies.

- Meets national requirements for ground flash density under the SAWS Act 8 of 2001,
- Aligns with the IEC 62858 international standard, which recommends at least 10 years of data to evaluate lightning exposure, and
- Supports the development of risk assessments and infrastructure planning in high-risk zones.



Lightning Density map

After a storm, users can request (or automatically obtain) lightning reports that confirm strike locations — useful for insurance claims, asset inspections, or investigating disruptions.



Lightning Density value



4. STATISTICAL RISK EVALUATION

Historical SALDN data is used to generate user-specific lightning risk assessments, including:

- o Lightning Density Maps
- o Strike Frequency Tables
- o Seasonal or temporal analyses
- o Tailored site studies that combine a spatial lightning distribution, temporal patterns, and electrical characteristics (e.g., peak current distribution). These comprehensive reports support infrastructure planning, regulatory compliance, and lightning protection design.

COLLABORATION WITH METEORAGE

In an exciting development, SAWS has partnered with METEORAGE, a French lightning detection and risk management company, to enhance the services offered through SALDN. METEORAGE brings decades of global expertise in lightning data and applications.

Mr. Ishaam Abader, CEO of SAWS, noted: "As the South African Weather Service, we are pleased to join hands with METEORAGE, a global authority where matters of lightning detection are concerned."

This collaboration will go a long way to enhance our safety efforts against lightning strikes for our citizens, as well as for industries that are critical to our economy, such as aviation, energy, insurance and others."

CONCLUSION

Lightning is a powerful and persistent threat, but with accurate detection and informed decision-making, its risks can be significantly reduced. The South African Lightning Detection Network plays a central role in this effort by providing real-time data, long-term insights, and tools to safeguard both people and infrastructure. Through local expertise, international collaboration, and a commitment to innovation, SAWS continues to lead the way in building a more lightning-resilient South Africa.

THE AUTHORS

Solal Bordenave is the Head of Marketing & International Sales at METEORAGE, the operator of the European Lightning Locating System. Building on past experiences in the metrology and renewables sectors, he supervised international capacity-building projects for several national meteorological services. He developed an expertise in lightning data uses throughout the diversity of market segments affected by thunderstorms.

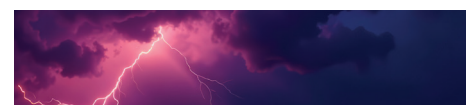
Anouk Inial is currently the International Sales Manager at METEORAGE. Anouk Inial brings experience from previous roles at METEORAGE and LIGUE DE L'ENSEIGNEMENT - FEDERATION DES OEUVRES LAIQUES DE L'AVEYRON. Anouk Inial holds a 2019 - 2021 Master's in Commercial Negotiation from the Université Sorbonne Nouvelle.

Rydall Jardine is the South African Weather Service (SAWS) Technical Service Manager, overseeing the Southern African Lightning Detection Network (SALDN). He has over 27 years of work experience within the Meteorological Environment, of which 20 years are on the lightning location technology.

He holds a Bachelor's Degree in Electrical Engineering from Tshwane University of Technology and is pursuing his Master's in Electrical Engineering at the University of Witwatersrand. He currently serves as the Deputy Chairperson of the Lightning Chapter for the South African Institute of Electrical Engineers (SAIEE).

Michelle Hartsliet is the Senior Commercial Manager at the South African Weather Services (SAWS) and has been deeply involved in the development and implementation of an evolving Commercial Strategic Plan, generating revenue in excess of R35 million annually for the short-term sustainability and long-term viability of SAWS.

An experienced, articulate innovator, with the capacity to identify, analyse and take independent action to enhance strategic imperatives and build capabilities. **wn**



OLDMUTUAL

GIVE YOUR CHILD THE EDUCATION THEY DESERVE

Understand your options when it comes to paying for their education. Get in-touch with me to invest in your child's future.



Misheck Mdala

Executive Financial Adviser
mmdala@oldmutual.com
082 546 1674



DO GREAT THINGS EVERY DAY

Old Mutual Life Assurance Company (SA) Limited is a licensed FSP and Life Insurer

Exploring the Correlation Between Elevation and Lightning Flash Density in Southern Africa



Southern Africa is known for having frequent and intense thunderstorms. But why do some areas experience more lightning than others, even when they lie in areas of similar rainfall?

BY: Andrew Britz

Hugh Hunt

Johannesburg Lightning Research Laboratory,
University of the Witwatersrand

This question lies at the heart of a study conducted by researchers at the Johannesburg Lightning Research Laboratory. Their work examines the complex relationship between lightning activity and topography — specifically, elevation — across parts of South Africa, Lesotho, and Eswatini.

Drawing on thirteen years of lightning data from the South African Lightning Detection Network (SALDN), the study offers the most comprehensive regional analysis to date of how elevation influences lightning flash density in the region. The findings offer not only scientific insights but also valuable guidance for engineers, meteorologists, and planners working in lightning-prone regions.

ELEVATED INSIGHTS

The study area encompasses a wide swathe of eastern southern Africa, from the Indian Ocean coastal plain, to South Africa's central plateau to the elevated Drakensberg Mountains, covering altitudes ranging from sea level to over 3,000 metres.

This makes it an ideal region of study for investigating how lightning activity responds to changes in terrain.

After compiling over a decade's worth of cloud-to-ground (CG) flash data and mapping it onto a 1 km² resolution digital elevation model, the researchers calculated the correlation between flash density and elevation across the region.

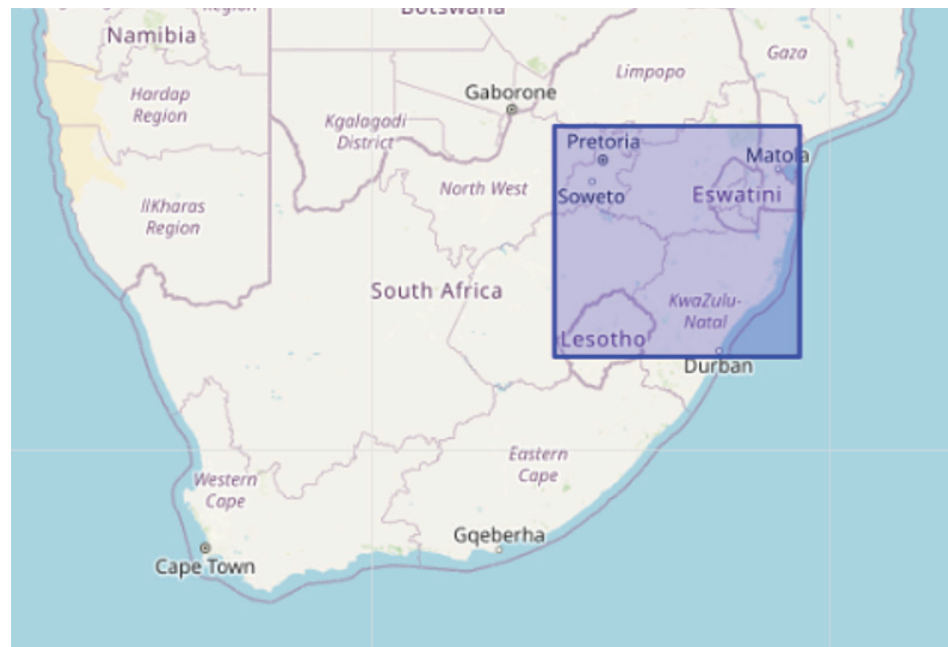


Figure 1: Region of Study

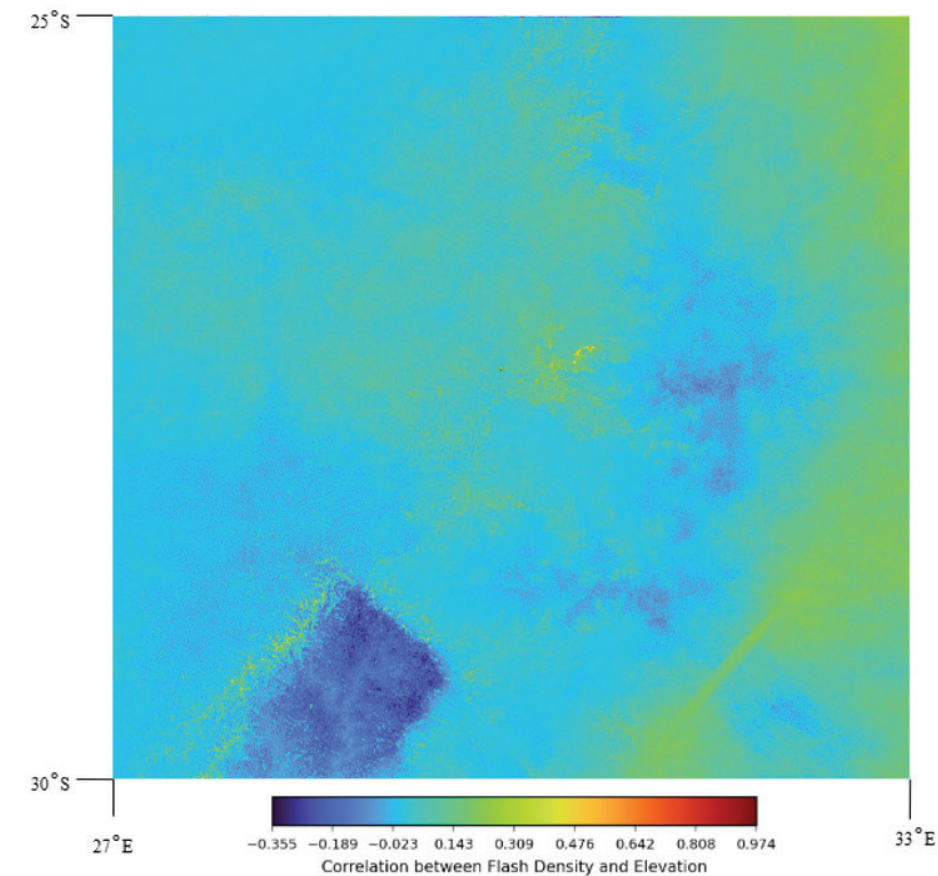


Figure 2: Map of Correlation Between Flash Density and Elevation

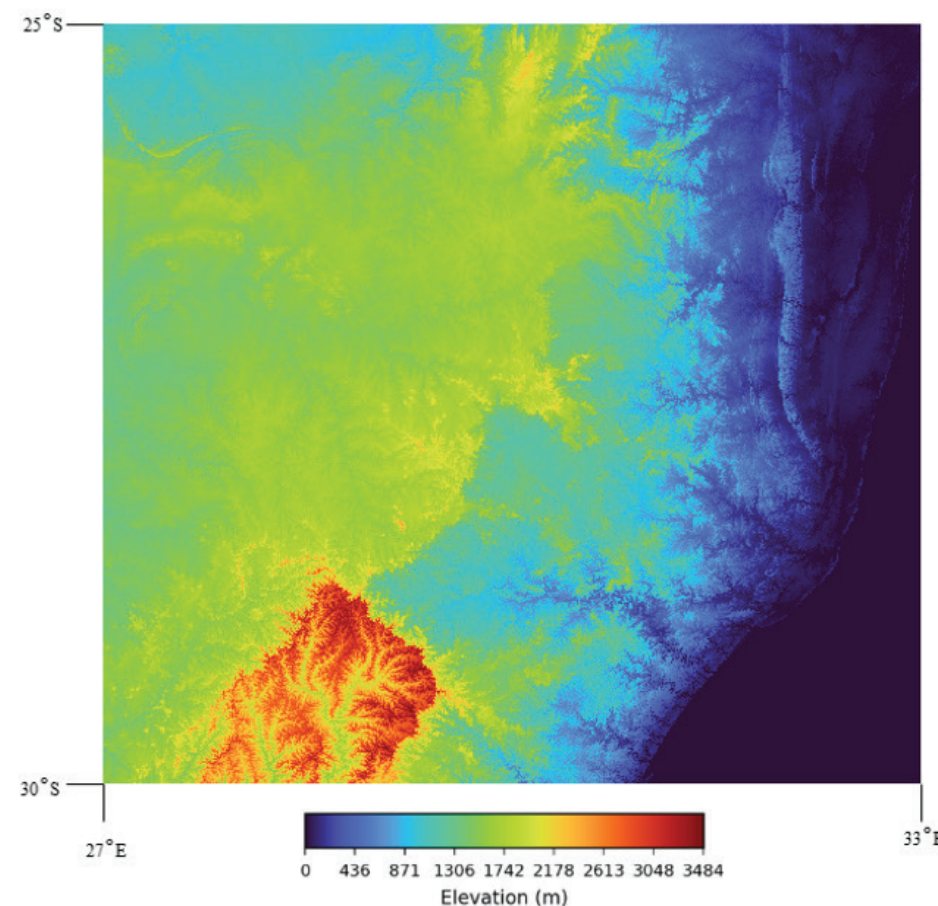


Figure 3: Elevation Map of the Region

The result: a moderate positive correlation ($r \approx 0.441$), indicating that lightning activity generally increases with altitude — up to a point. Flash density peaks at elevations between 1,300 and 1,400 metres, after which it declines steadily at higher elevations, particularly over the Drakensberg and Lesotho Highlands.

This finding aligns with previous studies in Brazil, Austria, and the United States, which similarly observed a plateau or decline in lightning occurrence above mid-altitude ranges.

METHODOLOGY

Lightning data from the South African Lightning Detection Network (SALDN) was filtered to include only cloud-to-ground events and grouped into flashes according to international standards (IEC 62858). This ensured statistical accuracy in computing flash density, measured in flashes per square kilometre per year.

Elevation data was sourced from the USGS's GTOPO30 global digital elevation model, with a spatial resolution of 30 arcseconds — approximately 1 km² at this latitude. The researchers overlaid lightning and elevation data, then generated correlation and density maps that revealed how flash activity clusters with geographic features.

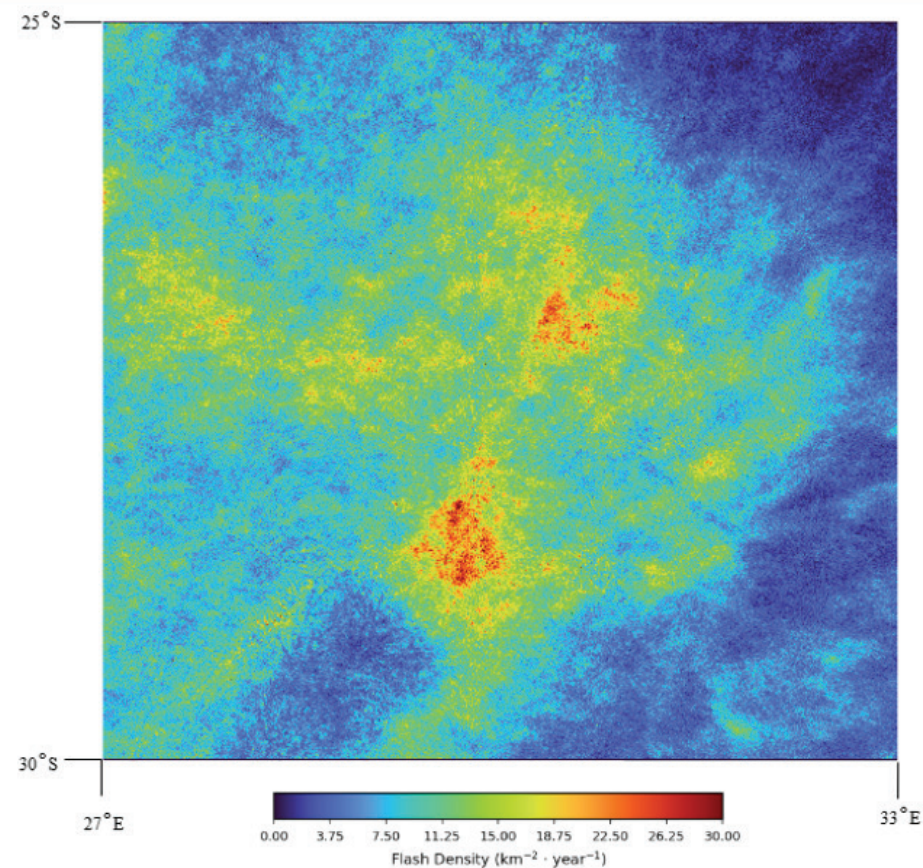


Figure 4: Lightning Flash Density Map of the Region

REGIONS OF HIGH LIGHTNING FLASH DENSITY

Highest lightning flash density was observed to occur in valleys adjacent to South Africa's eastern escarpment (the area of contrast between lime green and light blue as well as dark red and light blue in Figure 3).

This phenomenon is largely attributed to orographic uplift. As moist air from the Indian Ocean moves inland, it encounters steep terrain that forces it upwards, triggering convection and cumulonimbus cloud formation. These uplift zones serve as hotspots for thunderstorm initiation and charge separation, increasing the likelihood of lightning discharges.

Regions of Low Lightning Flash Density Flash density was found to be lowest near sea level and at altitudes exceeding

1,400 metres, as indicated by the darker regions in Figure 4.

While the overall correlation between flash density and elevation in these zones was generally weak, certain terrain features consistently displayed elevated lightning activity and stronger localised correlations. In particular, ridges descending from regions of high elevation to lower elevations emerged as notable hotspots. Notably, several of these ridges are present above 2,000 metres yet still exhibit heightened flash densities — challenging the broader regional trend of reduced lightning activity at higher altitudes.

The authors note that storms forming along these ridges may benefit from an optimal balance of uplift, moisture, and instability, enabling taller storm towers and more efficient charge separation,

however, this is research that requires further investigation.

IMPLICATIONS FOR INFRASTRUCTURE AND FORECASTING

The study's findings have practical implications for infrastructure design, risk assessment, and storm forecasting. Understanding where lightning is most likely to occur can help mitigate its risks to electrical networks, telecommunications infrastructure, and rural housing — particularly in highland communities.

From an engineering perspective, local topography should be considered alongside general elevation when designing lightning protection systems. Areas with steep slopes and descending ridges may warrant enhanced shielding or early warning mechanisms due to their elevated lightning exposure.

CONCLUSION

This study provides a comprehensive analysis of how elevation influences lightning flash density across a topographically varied and storm-prone region of southern Africa. While a moderate positive correlation was observed between elevation and lightning activity, the relationship is not uniform. Flash density peaks at mid-elevations (~1,300–1,400 m) but declines at higher altitudes — a trend consistent with global observations.

However, this elevation-flash density relationship is strongly modulated by local topography. In particular, descending ridges and steep terrain adjacent to escarpments emerge as consistent zones of intensified lightning activity, even at elevations exceeding 2,000 metres. These features likely enhance convective development through orographic uplift and favourable thermodynamic conditions.

The findings highlight that terrain structure — not just altitude — plays a crucial role in shaping lightning climatology. For infrastructure planners, engineers, and meteorologists, this underscores the importance of incorporating local terrain data into lightning risk models and protection strategies. Regions exhibiting sharp elevation gradients may warrant prioritised mitigation efforts.

ACKNOWLEDGEMENTS

This research was supported by the National Research Foundation of South Africa (Thuthuka programme), DEHNAFRICA, and the South African Weather Service (SAWS). The authors extend special thanks to Morné Gijben,

Rydall Jardine, and Michelle Hartsliet for providing and supporting the SALDN lightning data used in this study.

ABOUT THE AUTHORS

Andrew Britz obtained his BSc Eng (Information Engineering) from the University of the Witwatersrand and is pursuing his Master's degree by research at the same institution where his research focuses on lightning mapping and analysis, specifically investigating the correlation between lightning ground strike point densities and South Africa's topography.

Hugh Hunt is a Senior Lecturer in the School of Electrical and Information Engineering at the University of the

Witwatersrand. He earned his PhD from the University of Witwatersrand, investigating the use of lightning location system data in forensic investigations.

Dr. Hunt has extensive experience with the South African Lightning Detection Network and the RINDAT system in Brazil. He has authored over 35 research articles in the fields of lightning and high-voltage engineering. Currently, Dr Hunt leads the Johannesburg Lightning Research Laboratory. **wn**

YOUR 24/7 SERVICE PARTNER

Repairs, maintenance and customised manufacture of all electrical and mechanical rotating machines.

ELECTRICAL SERVICES

Medium and low voltage, Ex certified, AC and DC motors, transformers, generators, alternators and ancillary power generation equipment up to 373 MVA.

MECHANICAL SERVICES

Full range of rotating machinery mechanical services. Machine shop capabilities including dynamic balancing up to 32 tons, large machining up to 40 tons, micro welding and hydraulic presses up to 1000 tons.

24 HOUR ON-SITE SERVICES

Breakdown repairs, removal, re-installation, on-site testing, dynamic balancing, alignment, vibration analysis, root cause analysis, condition monitoring, preventative and predictive maintenance, motor management programmes and maintenance contracts.

CUSTOMISED ELECTRICAL AND MECHANICAL DESIGN

Reliability improvements/enhancements, efficiency improvements, performance upgrades and root cause analyses.



Marthinusen & Coutts
A division of ACTOM (Pty) Ltd

+27 (0) 11 607 1700 | support@mandc.co.za

53 Hospital Street, Cleveland 2094, JHB

www.mandc.co.za



Prevention is the Best Defence Against Lightning-Related Threats



Lightning strikes present a serious threat to critical facilities, leading to costly downtime, hazardous working conditions, and potentially irreversible damage to operations and stakeholder relationships. Effective lightning protection requires proactive measures that go beyond addressing direct strikes also to mitigate the broader range of lightning-related hazards, including induced surges and ground potential rise.

*Paper courtesy of
[Lightning Eliminators](#)*

Lightning Defence encompasses two key approaches: Lightning Protection and Lightning Avoidance (such as Charge Transfer technologies). This paper examines the nature of lightning-related risks, strategies for mitigating these threats, the unique advantages offered by LEC solutions, and best practices for designing, installing, and maintaining a comprehensive and effective Lightning Defence system.

TRADITIONAL LIGHTNING PROTECTION

Franklin Rods, commonly known as “lightning rods,” have been the standard method of lightning protection for over 250 years. These devices function by creating a “preferred collection point” on a structure to attract a lightning strike and channel its energy—ideally, safely to the ground through a conductive wire.

However, this approach is not without flaws. Historically, one significant risk arose from the physical attachment of lightning rods to structures. In many cases, the immense energy from a lightning strike ignited fires or caused severe structural damage. While advancements in techniques have reduced this risk over time, other critical vulnerabilities have emerged.

A fundamental issue lies in the very purpose of lightning rods: to attract lightning. This design means lightning rods can sometimes draw strikes into areas that might have otherwise remained unaffected. Paradoxically, in attempting to protect a structure, a lightning rod can create a risk where

none previously existed, introducing lightning into the very zone it is intended to safeguard. Fortunately, Lightning Defence technology has advanced since the introduction of the Franklin Rod.

LIGHTNING RISKS AND SCENARIOS

Modern operations and processes depend heavily on electronic equipment and telecommunications systems. Traditional lightning “protection” methods, such as lightning rods, can inadvertently bring dangerous lightning energy uncomfortably close to critically sensitive environments—often involving explosive materials—and the electronic systems responsible for monitoring and controlling these operations.

An equally significant, but frequently overlooked risk, lies in the secondary effects of lightning. Even when a direct strike is avoided, the residual effects—such as earth currents, atmospheric transients, secondary arcing, electromagnetic pulses (EMP), and ground potential rise (GPR)—can severely degrade system components. These secondary effects can result in equipment failure, operational downtime, or even false and erroneous system behaviour, compromising safety and reliability.

A wide range of facilities and operations face risks from both direct lightning strikes and their secondary effects. These risks may stem from the nature of the materials or commodities involved—such as flammable or explosive substances—or the critical missions they

Industries particularly vulnerable to lightning-related threats



Oil and Gas

Petrochemical plants, refineries, produced water facilities, and upstream/midstream operations are vulnerable to fires, explosions, and operational disruptions caused by lightning.



Energy and Utilities

Power plants, transmission, and distribution infrastructure face risks of outages and equipment damage.



Time-Sensitive Critical Processes

Industries like overnight delivery require systems that prevent operational downtime.



Healthcare

Hospitals and clinics rely on continuous power for critical medical equipment.



Telecommunications

Data centers, cell towers, and network facilities depend on uninterrupted service and are at risk of lightning strikes or secondary power surges.



Transportation

Airports, railways, shipping ports, and logistics hubs require robust infrastructure to avoid disruptions.



Process Industries

Wastewater treatment plants and pulp mills must protect against environmental and operational risks.



Public Services

Emergency response agencies and military installations need uninterrupted functionality to maintain public safety.



Broadcasting and Media

Lightning can disrupt television and radio communication, leading to significant operational interruptions, loss of revenue, as well as expensive and time-consuming repairs.



Manufacturing

Industries such as electronics, paper mills, and pharmaceuticals face operational and financial losses from lightning-related shutdowns.

support, including essential services and infrastructure.

THE IMPORTANCE OF LIGHTNING DEFENCE FOR MITIGATING RISK

Lightning Defence is crucial for safeguarding assets, maintaining operational continuity, and ensuring personnel safety. An effective Lightning Defence strategy mitigates risks and ensures the sustainability of critical operations.

BUSINESS RISKS OF LIGHTNING EVENTS

1. Operational Downtime

- **Equipment Damage:** Lightning can physically damage machinery, servers, and production lines.
- **Power Outages:** Disruptions halt productivity and lead to revenue losses.
- **Communication Disruptions:** Damaged networks and systems impair coordination.

2. Safety Hazards

- **Personnel Injuries:** Direct strikes or secondary effects jeopardise onsite safety.
- **Liability Issues:** Legal consequences arise from injuries to workers or visitors.

3. Financial Loss

- **Repair and Replacement Costs:** Infrastructure repairs are costly.
- **Insurance Premiums:** Inadequate protection systems may result in higher premiums or claims denial.
- **Revenue Loss:** Operational halts affect customer satisfaction and profitability.

4. Reputational Damage

- **Customer Trust:** Frequent disruptions erode client confidence.
- **Brand Impact:** Negative coverage damages public perception.

5. Environmental Impact

- **Fires and Explosions:** Lightning-induced incidents harm ecosystems

and cause regulatory challenges.

- **Compliance Issues:** Violations due to environmental damage result in fines.

6. Regulatory and Legal Risks

- **Code Violations:** Non-compliance with standards like NFPA 780 incurs penalties.
- **Legal Exposure:** Claims of negligence arise from insufficient protection.

7. Data and Intellectual Property Loss

- **Data Corruption:** Surges damage data storage systems.
- **IP Loss:** Compromised proprietary information affects competitiveness.

8. Supply Chain Disruptions

- **Vendor Delays:** Strikes at one facility can cascade through supply chains.
- **Inventory Loss:** Damaged storage areas result in significant losses.

9. Long-Term Infrastructure Damage

- **Structural Weakening:** Repeated lightning strikes degrade infrastructure.

LIGHTNING DEFENCE SYSTEM DESIGN CONSIDERATIONS

Several interrelated factors contribute to a facility's unique lightning risk profile. Primary considerations include:

1. Site-Specific Factors

- Geographic location, storm frequency, and soil resistivity influence system design.
- Topographic features and environmental conditions must be accounted for.

2. Structural and Operational Considerations

- Facility type, material composition, and layout determine the level of protection required.

3. Electrical and System Characteristics

- Proper grounding and surge protection are critical.

- Integration with existing systems ensures operational continuity.

4. Operational Requirements

- Facilities with critical functions require advanced prevention systems.
- Personnel safety is a key priority in all designs.

5. Regulatory and Industry Guidelines

- Compliance with NFPA 780 and other industry-specific requirements is essential (e.g., API 545 for the oil and gas industry).

6. Environmental and Sustainability Concerns

- Reducing environmental impact and using durable materials promote sustainability.

7. Maintenance and Monitoring

- Regular testing and real-time monitoring ensure system reliability.

SOLUTIONS FOR MINIMISING LIGHTNING RISK

Lightning defence risk mitigation strategies fall into two primary categories: Lightning Protection and Lightning Avoidance, briefly summarised below.

LIGHTNING PROTECTION

Lightning Protection refers to strategies designed to minimise the damage caused by a lightning strike after it occurs. The primary objective is to protect structures, equipment, and personnel from the destructive effects of lightning. One of the most widely recognised technologies is the lightning rod (or Franklin Rod), which attracts lightning strikes and channels their energy safely to the ground.

As previously mentioned, however, because lightning rods are designed to attract lightning, they can inadvertently imperil the very areas they are intended to protect.

Less understood is the fact that lightning can cause significant damage even if a strike occurs some distance away, sometimes up to a mile. Under specific ground and soil conditions, the electrical charge from a strike can travel considerable distances underground, posing a threat to nearby facilities and systems.

When lightning strikes a structure equipped with a Lightning Protection system, the system provides a controlled pathway for the electrical current to disperse into the ground. This minimises risks such as fires, structural damage, operational disruptions, and other hazards.

Standard Lightning Protection solutions include Franklin Rods, surge protection devices, grounding systems, mesh and Faraday cage systems, and air terminals. Each plays a critical role in managing the energy of a strike and reducing its impact.

LIGHTNING AVOIDANCE

In contrast to Lightning Protection, Lightning Avoidance technologies (i.e., Charge Transfer Systems or CTS) aim to reduce the likelihood of a lightning strike altogether. The primary goal of Lightning Avoidance is to alter atmospheric or ground (static) conditions, discouraging or diverting lightning strikes away from vulnerable areas such as critical infrastructure (e.g., mail sorting hub, crude oil storage facilities, etc.) or densely populated regions or venues (e.g., sports stadiums, schools, etc.).

Lightning Avoidance technologies focus on charge transfer, which lowers the electric field within the protected area to below lightning-collection thresholds. For example, the Dissipation Array® System (DAS®) from LEC works by



reducing the static field in the protected zone, encouraging lightning to terminate outside the area.

By proactively preventing strikes in this manner, DAS systems help to minimise downtime, preserve valuable assets, and enhance safety for personnel working in lightning-prone environments.

BEST PRACTICES FOR LIGHTNING DEFENCE

In this section, we cover the recommended practices for assessing lightning risk and developing an effective Lightning defence strategy for your operations.

ASSESS YOUR LIGHTNING RISK

Now that we have covered the types of lightning risks and lightning prevention strategies, we will now focus on the best practices planners and operators can use to develop an effective risk mitigation strategy for their specific risk profile and needs.

Engage an Expert. Lightning Defence is a specialised body of knowledge that has accumulated over 200 years, making it critical to secure an experienced and knowledgeable expert in lightning protection. A qualified lightning expert can help you assess your specific risk profile and develop a comprehensive protection strategy aligned with your budget.

Perform a Site Survey. A qualified Lightning Defence consultant can help survey your operations to identify likely physical risk factors. A site survey should include a detailed review of the structure(s) requiring protection, including materials, location, and other physical properties (i.e., height, depth, shape, etc.), environmental surroundings, soil composition and other factors.

Identify Critical Assets and Vulnerabilities. Identifying equipment that is vulnerable to lightning, either because of its location, connection to power systems, and/or reliance on power, is an essential element of developing an effective Lightning Defence strategy. Particular attention should be given to equipment that may be time-consuming to replace. In most cases, insurance can cover the cost of replacement, but in the case of specialised equipment or assets customised to a particular facility, extra protection is warranted.

Risk Mapping. Based on a site survey, create a visual representation of risk zones, highlighting areas of high strike probability, zones requiring surge protection, and paths for potential lightning-induced currents.

Operational Assessment. Make a critical analysis of the impact of a lightning-related interruption on your business. This includes downtime, loss of revenue and profits, time required to restart a process, and potential environmental impacts of a spill or overflow scenario along with associated fines, loss of business to competitors, and other operational factors.

Compliance Standards and Guidelines. Adherence to industry standards and guidelines (e.g., NFPA 780, API 545) is essential, but these standards often represent only the baseline for protection. In our view, relying solely on compliance may expose your operations to a higher level of lightning risk than your business can afford.

Cost/Benefit Analysis. We recommend analysing both the quantitative and qualitative costs of a lightning-related

business interruption, given different scenarios ranging from a short period of downtime to extended periods for more catastrophic situations. Handicap each scenario based on an assessment of its probability of occurrence, and then determine the appropriate level of budget to mitigate the risks.

TAKE A COMPREHENSIVE APPROACH

Once you have assessed the lightning risk profile of the facility under evaluation and the costs of a lightning-related business or process interruption, we recommend taking a comprehensive approach to developing a Lightning Defence strategy. Consider both Lightning Protection and Lightning Avoidance technologies in your defence initiative to minimise the risks and costs.

Meeting compliance objectives is essential, but compliance generally means achieving only a minimum level of lightning defence. In many cases, the risk and cost of a process upset or lengthy downtime can be significantly reduced by using Lightning Avoidance solutions that go above and beyond compulsory compliance. **wn**



BECOME A SAIEE KZN MENTOR

The South African Institute of Electrical Engineers (SAIEE) in KwaZulu-Natal is launching a Mentorship Programme to support aspiring engineers in achieving professional registration with the Engineering Council of South Africa (ECSA).

We invite you to become a Mentor and play a vital role in guiding candidates through technical development and professional growth in line with ECSA's requirements.



kznc@saiee.org.za

www.saiee.org.za



Why Become a Mentor?



Access

Webinars, lectures, and training courses on technical and professional topics.



Networking

Involvement in SAIEE Centres, Sections, Chapters, and industry-related initiatives.



Publications

Access to the wattnow Magazine, Africa Research Journal, and the Chronicle.



CPD

CPD credit accumulation through active participation.

How to Apply

If you're interested in becoming a SAIEE Mentor in the Electrical Discipline, please submit the following documents:

- Completed Mentor Application Form
- Your Curriculum Vitae (CV)
- ECSA Registration Certificate
- SAIEE Membership Certificate

Mentorship is currently VOLUNTARY, while SAIEE explores future remuneration options.

Click here for the Application form

Email your application to:
mentorship@saiee.org.za

Application Deadline
15 August 2025

Cybersecurity at a crossroads

- WHY AI DEMANDS A NEW PLAYBOOK



There's a growing unease in boardrooms, data centres, and cabinet offices across South Africa. It's not just about economic headwinds or political uncertainty; it's about something quieter, more technical, and yet just as dangerous: the rising tide of cyber threats.

*By Boland Lithebe
Security Lead for Accenture, Africa*

From phishing, scams, to ransomware and deepfakes, attacks are growing more sophisticated, more frequent, and more expensive. And the truth is, most organisations aren't ready.

That's not a guess. It's the clear picture emerging from our latest State of Cybersecurity 2025 research that shows just 36% of technology leaders acknowledge that AI is outpacing their security capabilities – yet a staggering 90% of companies lack the maturity to counter today's AI-enabled threats.

Cyber threats are evolving faster than enterprise defences can adapt, and generative AI is widening the gap. With unprecedented speed and scale, AI is enabling attackers to bypass legacy systems and overwhelm security teams. Traditional defences are no longer sufficient.

This is not merely a technical issue; it is a strategic risk. The cyber threat landscape is being reshaped not only by technology but by geopolitics. Heightened global tensions, changing trade dynamics and shifting regulations are compounding cyber exposure. Furthermore, a severe cybersecurity talent shortage presents a significant challenge. While awareness of AI-related risks is increasing, security measures are simply not keeping pace. As companies respond by adjusting supply chains and data strategies, many are unknowingly introducing new cyber risks, especially when security assessment, compliance and risk protocols fail to keep pace.

These revelations should ring alarm bells in Sandton, Pretoria, and every other place where digital decisions are being made. While AI adoption races ahead, security is playing catch-up. Speed and innovation continue to eclipse safety, with less than half (42%) of organisations striking a balance between AI development and security investment. Just 28% of organisations embed security into transformation initiatives from the outset, forcing many to scramble to retrofit defences later, often under duress. This reactive approach places growing pressure on already stretched security teams.

We surveyed 2,286 security and technology executives – 80% CISOs, 20% CIOs – from \$1 billion-plus enterprises across 24 industries and 17 countries, including South Africa. Their insights offer a sobering view of the current state of cybersecurity – and a clear call to action for what must come next.

Let's be blunt: too many of our organisations still treat cybersecurity as an afterthought. Something that gets squeezed into the budget if there's money left over or addressed after an attack has already happened. Meanwhile, cybercriminals are evolving, innovating, and automating. This is an arms race, and we are not winning it.

The findings show that only 34% of organisations have a mature cyber strategy. Fewer still – just 13% – possess the advanced cyber capabilities needed

to defend against modern, AI-driven threats. The vast majority remain exposed, underprepared and at risk of falling behind as AI-powered threats accelerate.

But there's a path to safety, a high ground we call the Reinvention-Ready Zone. Only 10% of companies have reached this level. These companies demonstrate maturity in both strategy and capability with a proactive, adaptive and resilient security posture that continuously evolves to counter emerging threats. The payoff?

Compared to those in the most vulnerable zone, which we refer to as the Exposed Zone, this group of companies are 69% less likely to be hit by an advanced attack such as an AI-powered cyberattack. They also see 1.6 times higher returns on their AI investments and reduce technical debt by 1.7 times, fuelling faster, more secure innovation. These companies report building stronger customer trust, 1.6 times more than those in the Exposed zone, a critical factor in sustaining long-term business success.

Our economic modelling of security outcomes reveals that a 10% increase in security investment, strategically directed toward Reinvention-Ready

Zone practices, can enable organisations to detect, contain and remediate cyber threats 14% faster. We recommend four decisive actions for companies to achieve Reinvention-Ready Zone status. These actions not only protect AI investments but also leverage AI to enhance cybersecurity defences and resilience.

Develop and deploy a fit-for-purpose security governance framework and operating model accounting for the realities of an AI-disrupted world. Establish clear accountability and align AI security with regulatory and business objectives.

Design the digital core to be generative AI-secure from the outset. AI must be developed, deployed and operated with security integrated at every stage, yet only 37% of organisations assess AI security before deployment.

Maintain resilient AI systems with secure foundations and proactive threat management. Emerging AI-based cyberattacks – including AI worms like Morris II – can embed malicious prompts into AI models, allowing attackers to hijack AI systems and compromise sensitive data.

Reinvent cybersecurity with generative

AI to scale security capabilities, strengthen cyber defences and detect threats earlier. With an estimated 4.8 million cybersecurity positions unfilled worldwide¹³, AI presents an opportunity to bridge the cybersecurity talent gap by amplifying security professionals.

Organisations that bake security into their AI-powered transformations will not only survive but thrive, gaining a crucial competitive edge, cementing customer loyalty and building unshakable resilience. Ascending to the Reinvention-Ready Zone – where robust security is deeply embedded in both strategy and capability – requires focused effort, strategic investment and leadership from the top down.

The Reinvention-Ready Zone is within reach – but it requires decisive action. By adopting a secure governance framework, building resilient AI systems, leveraging generative AI for security and embedding security into every stage of AI development, companies can close the security gap and confidently navigate an era of accelerating cyber threats.

The path forward is clear: Security is not just a safeguard – it is a strategic enabler of innovation, trust and long-term success. **wn**

High Voltage & Earthing Engineering Conference

22nd & 23rd October 2025 | Sandton, South Africa

Call for Speakers



Quantum computing and its impact on data security

- A DOUBLE-EDGED SWORD FOR THE DIGITAL AGE



Quantum computing is poised to redefine the boundaries of data security, offering groundbreaking solutions while threatening modern encryption's foundations. For third-party IT providers, this duality presents both a challenge and an opportunity to lead organisations through one of the most significant technological transitions in decades.

*By Amrithesh Anand, Vice President & MD
Technology Services Group at In2IT Technologies.*

THE QUANTUM THREAT: SHATTERING CLASSICAL ENCRYPTION

At the heart of quantum computing's disruptive potential lies its ability to solve complex mathematical problems exponentially faster than classical computers. Algorithms like Shor's algorithm could crack RSA and elliptic curve cryptography (ECC), cornerstones of today's internet security, in minutes.

This capability isn't theoretical; it's a looming reality. Imagine a future where encrypted financial transactions, classified government communications, or sensitive healthcare data stored today could be retroactively decrypted once quantum computers mature. For industries relying on long-term data confidentiality, this creates a race against time to adopt quantum-resistant solutions.

THE SILENT COUNTDOWN TO CRYPTO-COLLAPSE

Governments and cyber adversaries are well aware of the ticking clock. Some states have already begun quantum research arms races, with some rumoured to be investing in "harvest now, decrypt later" strategies, collecting vast amounts of encrypted data in anticipation of future quantum breakthroughs.

The trend poses an existential risk to industries like legal, finance, and healthcare, where long-term confidentiality is non-negotiable. Third-party IT providers must help clients

understand that quantum threats are not years away; they are data decisions made today with consequences tomorrow.

BUILDING UNBREAKABLE DEFENCES

While quantum computing undermines classical encryption, it also pioneers novel security paradigms. Quantum Key Distribution (QKD), for instance, uses the principles of quantum mechanics to create theoretically unhackable communication channels.

Any attempt to intercept a QKD-secured message disrupts its quantum state, alerting both parties to eavesdropping. Similarly, post-quantum cryptography (PQC) leverages mathematical problems believed to be unsolvable even by quantum machines, such as lattice-based or hash-based algorithms.

Hybrid approaches, combining classical encryption with PQC, offer transitional security, ensuring data remains protected even if one layer is compromised.

BRIDGING THE EXPERTISE GAP

Most organisations lack the in-house expertise to navigate this transition alone. Third-party IT providers are not just a resource, but a crucial ally in this journey, uniquely positioned to offer:

Cryptographic audits and risk assessments: They help identify the vulnerabilities in existing systems, such as reliance on RSA or ECC, and prioritise high-risk data for immediate remediation.

Implementation of quantum-resistant frameworks: Deploying hybrid encryption models (e.g., AES for bulk data paired with PQC-secured keys) and integrating QKD into network infrastructure.

Crypto-agility solutions: Building adaptable systems that can seamlessly transition to new algorithms as standards evolve, future-proofing investments against rapid technological shifts.

For example, a healthcare provider might partner with IT experts to encrypt patient records using lattice-based cryptography, ensuring decades of compliance with privacy laws despite advancing quantum capabilities.

TAILORED QUANTUM ROADMAPS

Not every organisation will require the same path to quantum readiness. A telecom firm handling real-time data may prioritise QKD networks, while a law firm may focus on PQC for archival integrity. Third-party providers are key in crafting customised quantum migration plans, factoring in industry regulations, data sensitivity, system dependencies, and operational timelines. These roadmaps align technological shifts with business priorities, ensuring that security enhancements are supported and do not disrupt ongoing operations.

OVERCOMING PRACTICAL CHALLENGES

Transitioning to quantum-resistant security isn't without hurdles. Many PQC algorithms demand more computational resources, straining Internet of Things

(IoT) devices or legacy systems. Third-party providers can mitigate this by optimising implementations for efficiency, such as leveraging hardware accelerators for lattice-based operations or designing phased rollout plans that balance security and performance.

Additionally, they can orchestrate supply chain collaboration, ensuring partners and vendors adopt compatible encryption standards to prevent weak links.

PROACTIVE ADAPTATION

The quantum threat is not a distant sci-fi scenario. It is a reality, with some corporations already stockpiling encrypted data for future decryption. Organisations must act now to:

Educate leadership: Securing executive buy-in for quantum readiness initiatives, emphasising regulatory and reputational risks.

Adopt hybrid encryption: Layering classical and quantum-resistant methods to safeguard critical assets today.

Invest in quantum literacy: Training IT teams to manage emerging tools like QKD and QRNGs (Quantum Random Number Generators), which enhance key generation security.

THE COMPETITIVE EDGE OF EARLY ADOPTION

Beyond risk mitigation, early movers in quantum-resilient security gain a reputational edge. As data breaches grow costlier, clients and partners

will increasingly favour businesses that can demonstrate post-quantum preparedness. From securing customer trust to meeting future compliance mandates, quantum readiness is more than technical hygiene – it is its strategic positioning.

For IT providers, this opens new opportunities to create value-added service offerings built around quantum security audits, compliance certifications, and secure communication protocols.

SECURING THE FUTURE, TODAY

Quantum computing's impact on data security is inevitable, but its risks are manageable with foresight and collaboration.

Third-party IT providers will be pivotal in guiding organisations through this transition, demystifying quantum mechanics, implementing robust defences, and fostering crypto-agile ecosystems.

By embracing quantum-resistant strategies today, businesses can turn a potential crisis into a competitive advantage, ensuring trust and resilience in the quantum era. **wn**



Ransomware isn't going away



Ransomware continues to be one of the most disruptive and costly threats facing organisations today. With attacks capable of halting operations, damaging brand reputations, and draining financial resources, the risk is not only real; it's escalating.

*By Nemanja Krstić,
Operations Manager
Managed Security Services at Galix*

In this climate, businesses must shift from reactive firefighting to a more strategic, proactive approach that minimises vulnerabilities, strengthens recovery strategies, and encourages collaboration across the board.

START WITH THE BASICS: VULNERABILITY AND PATCH MANAGEMENT

At the heart of every robust cybersecurity strategy is a surprisingly simple yet frequently overlooked element: vulnerability and patch management. Cybercriminals often exploit known vulnerabilities in outdated software, making regular updates a critical first line of defence. But patching isn't just about installing the latest software version; it requires a consistent, structured process to identify and address weaknesses across the IT environment.

When appropriately executed, patch management forms the backbone of a broader vulnerability management strategy. It might not carry the glamour of cutting-edge AI tools or advanced threat detection systems, but its role in reducing risk exposure is foundational.

By closing off well-known entry points, organisations immediately reduce their appeal as easy targets.

BACKUPS: YOUR BUSINESS'S SAFETY NET

Once systems are patched and secure, the next step is ensuring you have a solid backup strategy. Backups act as a vital safety net in the event of a ransomware attack. Best practice is to maintain multiple copies of data, stored in geographically separate locations—

including cloud or off-site environments that are isolated from the main network.

But backups are only adequate if they work. Regular testing is essential to ensure data can be restored quickly and accurately. In this regard, cloud platforms have become indispensable, offering secure, scalable, and accessible disaster recovery options. A well-tested, resilient backup system can be the difference between a swift recovery and a devastating data loss.

GOOD CYBER HYGIENE: EVERYDAY SECURITY WINS

While infrastructure plays a crucial role, so do the people who use it. Day-to-day cybersecurity habits across an organisation are just as crucial as technical safeguards. Practices like Multi-Factor Authentication (MFA), secure password policies, and advanced endpoint protection create layers of security that slow attackers down—or keep them out entirely.

Many organisations already have access to powerful cybersecurity tools, but underutilisation is a common issue. It's essential to understand the full capabilities of existing solutions and ensure they are properly configured. These everyday actions often serve as the first and most reliable barrier against opportunistic threats.

CONTROL ACCESS, CONTROL RISK

User privilege management is another key line of defence. Attackers often target privileged accounts, especially admin-level users, because of the broad access they provide. Applying the Principle of Least Privilege (PoLP), giving users

only the access they need, dramatically reduces the potential damage in the event of a breach.

Administrative accounts, in particular, should be tightly controlled and monitored. Enabling MFA, reviewing access rights regularly, and auditing account usage can prevent both internal misuse and external compromise. These controls not only limit damage but also reduce the time it takes to detect and contain a breach.

WHY PAYING RANSOM IS A RISKY GAMBLE

In the chaos of an attack, the idea of paying a ransom may seem like the fastest route to recovery. However, this approach is fraught with risk. There is no guarantee the data will be returned, nor that the attackers won't come back, or sell the information elsewhere.

What's more, paying up contributes to the larger ransomware ecosystem, fuelling more attacks. Organisations also face regulatory and legal challenges if they fail to report or handle breaches properly, especially under laws like GDPR or POPIA. A well-prepared, prevention-focused strategy remains the most responsible and sustainable path forward.

STAY ONE STEP AHEAD WITH THREAT INTELLIGENCE

Knowledge is power in cybersecurity. Leveraging threat intelligence from reputable sources can help organisations anticipate emerging risks and adjust their defences accordingly. These insights provide details on how attackers operate—what tactics, techniques,

and procedures they're using, allowing security teams to act pre-emptively.

Sharing this intelligence within industry groups is equally powerful. The financial sector, for instance, has long benefited from information-sharing initiatives that foster collective defence. By participating in such networks, businesses can align on standards, reduce duplicated effort, and respond faster and more effectively to evolving threats.

PLANNING FOR THE WORST: INCIDENT RESPONSE

Even with the strongest defences, no system is entirely foolproof. That's why a well-crafted Incident Response Plan (IRP) is essential. This isn't just an IT concern; it must involve legal teams, communications personnel, and senior leadership. Clear roles and backup communication methods are crucial, especially if primary systems are compromised.

Regular tabletop exercises and simulations are vital to refining your response. These drills help identify gaps and prepare teams to act swiftly under pressure. Tailored playbooks for specific scenarios like ransomware or phishing attacks make the response more structured and effective.

Downtime from ransomware can quickly snowball into lost revenue, productivity setbacks, and reputational harm. Testing and refining recovery strategies, supported by investments in cloud-based backups and partnerships with Managed Security Service Providers (MSSPs), significantly shortens recovery times.

LEARNING AND ADAPTING POST-INCIDENT

Recovery doesn't end with restoring data. A post-incident review is essential to understand what went wrong, what went right, and how to improve. Updating policies, retraining staff, and adapting the IRP based on lessons learned helps build a culture of constant vigilance.

This ongoing refinement transforms every challenge into an opportunity for growth, making the organisation more resilient with each incident. It's a continuous cycle of learning that's critical in today's fast-changing cyber landscape.

A LAYERED DEFENCE FOR LONG-TERM RESILIENCE

There's no silver bullet for stopping ransomware. But a layered approach, starting with basic hygiene like patching and backups, progressing through access control and response planning, and ending with collaboration and threat intelligence, creates a strong defence.

By investing in preparedness and working together across industries, businesses can stay ahead of attackers, protect their assets, and ensure continuity no matter what comes their way. In the world of cybersecurity, resilience isn't a destination; it's an ongoing journey. **Wn**



Bridging the Divide

- ACTIVATING THE "S" IN ESG THROUGH IMPACT-DRIVEN ESD



In many boardrooms, the "S" in ESG in the context of MSME enablement has become the most abstract pillar on the ESG scorecard, often overshadowed by environmental metrics tracked to decimal points and governance standards guided by frameworks like King IV and JSE requirements. When quarterly reports are presented, the small business empowerment-related social indicators often distil into a familiar line: "R130 million spent with black-owned suppliers."

By Mpopi Khupe, Managing Director at Zevoli Growth Partners

While this sounds impressive, it masks a more profound, uncomfortable truth. That line item rarely reveals the actual value delivered. How much of that spend created sustainable enterprises? How many jobs were supported beyond the life of a single contract? Did any of it translate into a long-term increase in household incomes in the mine's host communities?

More importantly, can anyone in the organisation answer those questions with certainty?

FROM COMPLIANCE TO CREDIBILITY

Mining companies already navigate a dense web of compliance frameworks - B-BBEE scorecards, Social and Labour Plans, Mining Charter obligations, and global ESG disclosure demands. It's no wonder that many treat the social element of ESG as just another risk and compliance reporting requirement to appease the relevant stakeholders.

But this compliance and reporting-driven approach is rapidly becoming a liability. Global investors now scrutinise the authenticity of social empowerment and impact claims. Lenders apply higher margins to perceived social risk. Communities, once quiet recipients of development spending, are increasingly vocal about the lack of lasting transformation and impact.

A transactional relationship with socio-economic development, one where impact isn't tracked or verified, is no longer enough. ESD managers find themselves at the frontlines of this

reckoning. And the most strategic ones are beginning to reframe the role of ESD from a legislative burden to a powerful lever for sustainable social and economic impact.

A NEW ROLE FOR ESD IN ESG STRATEGY

ESD, long seen as a B-BBEE requirement, can and should serve as an integral part of the engine that powers the "S" in ESG. When thoughtfully designed and executed, ESD can and should do more than implement quick-win initiatives to secure points. It should be optimally leveraged to build sustainable small businesses. It should enable the achievement of diversified value chains. It should strengthen social licence in ways that no cheque or clinic ever could. To do this, however, requires a clear departure from business as usual and a willingness to change the lens through which we view the "why" of transformation initiatives.

The first shift is a move from spend to outcomes. Measuring the Rand value of contracts is no longer sufficient. What matters now is whether those contracts contribute to real MSME growth, improved business resilience, and local job creation. This is often initiated by impactful, bold decisions such as a shift from off-contract, short-term opportunities to on-contract, long-term opportunities.

The second shift is from compliance to inclusion. Procurement should actively seek out suppliers that are not only black-owned but also represent diversity across gender, geography, and industry

sectors, particularly those from rural and peri-urban areas where economic activity is limited.

The final shift is toward integration. Community development, ESD programmes, local and preferential procurement, and even SLP infrastructure projects must work together under a unified strategy. When these elements are aligned, mining houses can credibly and transparently demonstrate that their "S" pillar delivers measurable value to people and small businesses in the communities in which they operate.

Demystifying ESG and SDG Alignment
A common question among executives and ESD managers alike is whether they should align with ESG or the Sustainable Development Goals.

The answer is: both. ESG is investor-driven and risk-focused. SDGs are aspirational and development-driven. When paired, they offer a comprehensive framework for defining, executing, and measuring social impact.

For example, onboarding 100 local MSMEs and growing their collective revenue supports both ESG metrics like percentage local procurement and SDG goals, such as decent work and industry innovation. Similarly, increasing the share of women-owned businesses in the supply chain delivers against ESG diversity metrics and SDG 5 on gender equality.

The value lies not in choosing one framework over another, but in ensuring that your ESD outputs are intentionally mapped to both.

WHAT THIS MEANS FOR ESD MANAGERS

As an ESD manager, your role is more critical than ever. You are the link between board-level ESG ambitions and real-world transformation. But activating that potential requires a strategic mindset and a deliberate approach.

Start by assessing whether your current ESD programme is built to deliver outcomes or simply satisfy compliance. Are you tracking the survival rate of SMEs after contract award? Are you

measuring income uplift in your host communities? Are your service providers equipped to support businesses beyond the programme "what" - technical training, with mentorship, access to markets, and funding facilitation, by also equally addressing its "why" - entrepreneur mind shift change, operational excellence principles, and technical mastery practices?

If the answer is no, or you're unsure, there's an opportunity to reframe your ESD programme as a core contributor to ESG performance.

This also means engaging differently with your implementation partners. The most impactful programmes are co-designed with Entrepreneur Support Organisations who understand the local context and can bring diagnostic insights, blended support models, and robust data collection systems to the table.

When the right partners are selected, ESD evolves from an expenditure line to a strategic investment in enterprise resilience and community stability. **WN**



MEMBERSHIP FEES EFFECTIVE 1 DECEMBER 2024

The Council meeting held on 6 September 2024 approved subscription & entrance fees as from 01 December 2024 as per schedule indicated below.

PLEASE NOTE: In terms of Bylaw 3.2 annual subscriptions are due on 1st December 2024

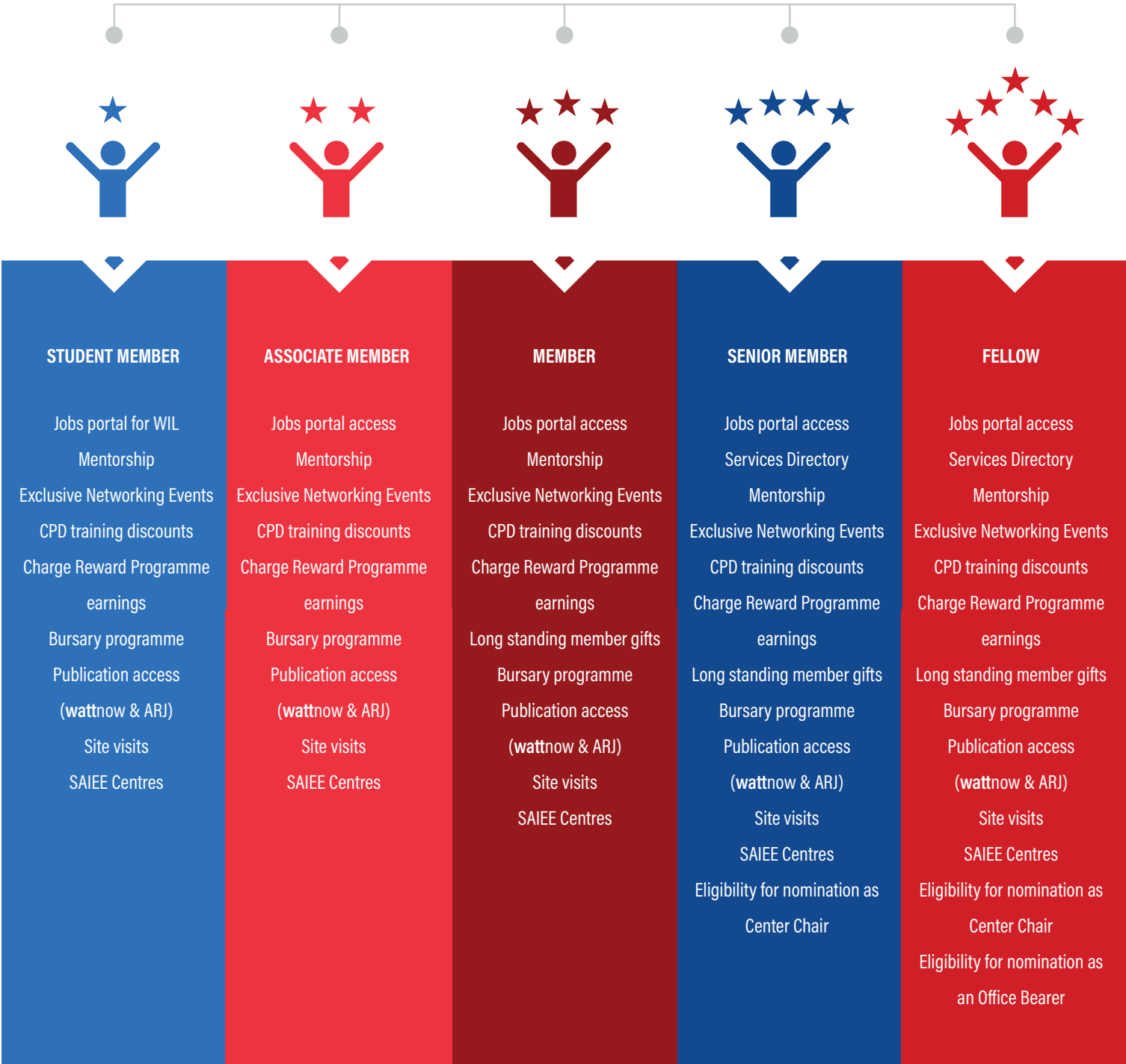
MEMBERSHIP FEES CAN BE PAID IN MONTHLY RECURRING PAYMENTS

Council agreed to a discount for fees paid before 31 March 2025. Members are therefore encouraged to pay promptly to minimize increase impact.

Grade of Membership	Annual Subscriptions paid before 31 March 2025		Annual Subscriptions paid after 31 March 2025		New Members FEES * see Notes 1 & 4 below.	
	RSA incl VAT (R)	Outside RSA excl VAT (R)	RSA incl VAT (R)	Outside RSA excl VAT (R)	RSA incl VAT (R)	Outside RSA excl VAT (R)
Student	nil	nil	nil	nil	nil	nil
After 6 yrs study	1 890	1 644	2 268	1 972	2 268	1 972
Associate	1 890	1 643	2 268	1 972	2 268	1 972
Member	2 089	1 816	2 507	2 180	2 507	2 180
after 6 years	2 441	2 122	2 929	2 547	2 929	2 547
after 10 years	2 555	2 221	3 065	2 666	3 065	2 666
Senior Member	2 555	2 221	3 065	2 666	3 065	2 666
after 6yrs/age 40	2 768	2 407	3 322	2 889	3 322	2 889
Fellow	2 768	2 407	3 322	2 889	3 322	2 889
Retired Member (By-law B3.7.1)	1 174	1 021	1 409	1 225	n/a	n/a
Retired Member (By-law B3.7.3)	nil	nil	nil	nil	n/a	n/a

1. The fee for all new applications is R3457.00 which includes an entrance fee of R950.00. On election to the applicable grade of membership the new member's account will be adjusted accordingly and refunds/additional payment made on request.
2. Transfer fee to a higher grade is free for all grades of membership.
3. Members are encouraged to transfer to a higher grade when they qualify. It will be noted that the fees of Member and Senior Member grades after 10 and 6 years respectively are equal to the fees at the next higher grade.
4. Members elected after May 2025 pay a reduced subscription fee.
5. By-law B3.7.1 reads "Where a member in the age group of 55 to 70 years has retired from substantive employment in the engineering profession, such member may make written application to Council for recognition as a retired person and a reduced membership fee".
6. By-law B3.7.3 reads "any member complying with the conditions of B3.7.1 but who has been a member of the Institute for not less than 25 consecutive years, shall be exempt from the payment of further subscriptions." Members who comply with the requirements of By-Law B3.7.3 may make written application to Council for exemption from paying subscriptions".
7. By-law B3.9 reads "any member in good standing who has been a member for fifty (50) consecutive years shall be exempt from the payment of further subscriptions."
8. Members not in good standing by failing to pay their subscriptions by end of June of each year will, subject to Council decree, be struck-off the SAIEE membership role.
9. Members in good standing and no longer in substantive employment and do not receive payment or salary for work done may apply to Council for a reduction in their annual subscriptions.
10. The members monthly magazine ("wattnow") is available on line and members who require a hard copy may acquire same on request and for a nominal fee subject to minimum uptake numbers.
11. Members who wish to pay their membership fees in recurring payments should activate the payments on their banking portal. Members will receive the early bird discount only if their fees are fully paid by 31 March 2025.

2025 SAIEE MEMBER BENEFITS



MEMBERSHIP UPGRADE DISCOUNT STRUCTURE

LENGTH OF MEMBERSHIP	DISCOUNT UPON UPGRADE
10 - 19 years	5%
20 -39 years	10%
40+ years	15%



Become a member today and start earning the rewards!

The South African Institute of Electrical Engineers | T: 011 487 3003 | www.saiee.org.za



SAIEE OFFICE BEARERS



V RAMNARAIN
2025 SAIEE PRESIDENT



P MADIBA
DEPUTY PRESIDENT



PROF W CRONJE
SENIOR VICE PRESIDENT



J MOLADIILE
JUNIOR VICE PRESIDENT



P MOTSOASELE
IMMEDIATE PAST PRESIDENT



PROF P NAIDOO
HONORARY TREASURER



DR M F KHAN
HONORARY VICE PRESIDENT

2025 OFFICE BEARERS

President	V Ramnarain	Deputy President	P Madiba
Senior Vice President	Prof W Cronjé	Junior Vice President	J Motladiile
Immediate Past President	P Motsoasele	Honorary Treasurer	Prof P Naidoo
Honorary Vice President	Dr M Kahn		

PAST PRESIDENTS

G Debbo, Prof J de Kok, Dr H Geldenhuys, S Gourrah, Dr A Hay, J Machinjike, I McKechnie, P Moyo, A Mthetwa, Prof P Naidoo, P van Niekerk

FELLOWS

J Buisson-Street, I Fick, Prof C Gomes, Dr M Kahn, C Matlala, S Mollo, J Motladiile, A Mtshali, Prof D Nicholls, K Setlhapelo, Dr L Staphorst,

SENIOR MEMBERS

Y Brijmohan, T Cornelius, Dr L Masisi, Dr F Manganye, C Mohloki, P O'Halloran, M Rikhotso, V Shikoana, R Singo, W Stucke

MEMBERS

O Bosaletsi, T Gabriel, K Katyora, S Mabuza, V Mahlasela, L Modiselle, Dr F Nelwamondo, S Nkosi, M Ramutumbu

SECTION CHAIRPERSONS:

Building Services	A Chivaurah	bssection@saiee.org.za
Electronics & Software	M Taljaard	essection@saiee.org.za
Historical Section	C Mohloki	hs@saiee.org.za
Power & Energy	M Soni	pesection@saiee.org.za
Rotating Machines	F Steyn	rmsection@saiee.org.za
Systems	T Ramagofu	systemsection@saiee.org.za
Telecommunications	TBA	telsection@saiee.org.za

CHAPTER CHAIRPERSONS:

Cybersecurity Chapter:	M Taljaard	csc@saiee.org.za
Entrepreneurship Chapter:	Y Mabuto	entrepreneurchapter@saiee.org.za
Financial Chapter	M Mdala	financialchapter@saiee.org.za
Lightning Chapter	H Hunt	lightningchapter@saiee.org.za
Load Research Chapter:	M Dekenah	lrchapter@saiee.org.za
Nuclear Chapter:	D Nicholls	nuclearchapter@saiee.org.za
Railway Chapter	R Kopa	railwaychapter@saiee.org.za
Renewable Energy Chapter	T Mhondiwa	re@saiee.org.za
Women in Engineering:	M Phoshoko	wie@saiee.org.za





Eastern Cape Centre

Chairman | Philip Nicholson
E | ecc@saiee.org.za



Free State Centre

Chairman | Motoloki Lephoi
E | fsc@saiee.org.za



Central Gauteng Centre

Chairman | Keith Katyora
E | cgc@saiee.org.za



Kwa-Zulu Natal Centre

Chairman | Krystle Nageshar
E | kznc@saiee.org.za



Mpumalanga Centre

Chairman | Vacant
E | mpc@saiee.org.za



Northern Cape Centre

Chairman | Vacant
E | ncc@saiee.org.za



Southern Cape Centre

Chairman | Vacant
E | scc@saiee.org.za



Vaal Centre

Chairman | Vacant
E | vc@saiee.org.za



Western Cape Centre

Chairman | Heinrich Rudman
E | admin.wcape@saiee.org.za

AUGUST 2025

05/08/2025	Photovoltaic Solar Systems
07/08/2025	SAIEE Business Breakfast
12/08/2025	Design Thinking and Innovation for Engineering Professional
13/08/2025	SAIEE President's Invitation Lecture
13/08/2025	Earthing & Lightning Protection
13/08/2025	An Introduction to Artificial Intelligence for Professionals
19/08/2025	Lightning Protection of Structures, Low Voltage and Signal Systems
19/08/2025	LV/MV/HV Switch gear Operation, Safety, Maintenance and Management
26/08/2025	Professional Registration with ECSA for Mature Candidates
27/08/2025	KZN Centre presents: Green Hydrogen webinar
27/08/2025	Writing Good Technical Specifications
28/08/2025	SAIEE Rotating Machines Site Visit to LHM Fan Division

SEPTEMBER 2025

03/09/2025	Arc Flash
05/09/2025	Road to Registration for Engineering Candidates
10/09/2025	Incident Investigation and Management (Root Cause Analysis)
16/09/2025	Fundamentals of Medium Voltage Protection
16/09/2025	Planning Feasibility Studies: An Engineer's Perspective
25/09/2025	High Voltage Measurement and Testing
29/09/2025	FIDIC Tendering and Contracts for Engineers



View past events & webinars on SAIEE TV [here](#).

SAIEE Sections, Chapter & Centre Events

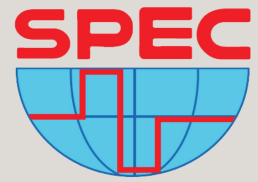
SAIEE Academy Online Training

SAIEE Academy Classroom Training

IEEE SPEC 2025

CALL FOR PAPERS

DECEMBER 1-4 | Wits University, JHB



pels



IEEE

SAIEE



IEEE SPEC 2025 (the 10th Southern Power Electronics Conference) will take place in Johannesburg, South Africa, from December 1 to 4, 2025. SPEC 2025 offers a valuable opportunity for researchers, engineers, academics, and students worldwide to showcase the latest technological advances and applications in Power Electronics to the Southern Hemisphere.

IMPORTANT DATES

31

AUGUST 2025

Digest Submission

30

SEPTEMBER 2025

Notification of Acceptance

30

OCTOBER 2025

Final Paper Submission

AREAS OF INTEREST

- Wireless EV charging
- Alternative capacitive & ultrasonic wireless power transfer technologies
- Energy harvesting and wireless power network
- Converter topologies, control and modulation
- Renewable & alternative energy power electronics systems
- Critical power and energy storage systems
- Aerospace energy conversion systems
- Space power electronics
- Grid-forming technologies
- High power converters
- Multilevel converters
- Permanent magnet & reluctance machines: design, control and applications
- AC machines: design, control and applications
- Sensorless motor drives
- Smart, AC, DC and micro/nano grids
- Power electronics in HVDC, HVAC and FACTS
- Power quality issues, harmonic problems and solutions
- High-density power converters
- Active and passive devices for power electronics
- Fault-tolerant and diagnostic techniques and applications
- Power electronics in mechatronics and robotics
- Power electronics in transportation and mobility
- Power electronics in bio-medical applications
- Emerging topics in power electronics
- Big data and artificial intelligence in energy conversion
- Energy conversion for information technology and communication systems
- Cybersecurity issues in power conversion systems
- Digital twins, cloud design and simulation techniques for energy conversion systems

IEEE SPEC 2025



CLICK HERE FOR MORE INFORMATION