

wattnow

THE OFFICIAL PUBLICATION OF THE SOUTH AFRICAN INSTITUTE OF ELECTRICAL ENGINEERS



CABLES



- 4 SAIEE President's Inaugural Speech
- 8 Industry News
- 16 Student News
- 20 Tertiary Education Facilities in South Africa
- 22 **Cable Theft in South Africa**
We take a look at the state of Cable theft in South Africa - everyone needs to get involved.
- 26 **The Impact of radial water blocking on MV XLPE Cable systems**
Necessary for cable longevity.
- 28 **Four Trends Impacting Enterprise Networks, And How to Support Them**
Businesses prioritise digital transformation to unlock opportunities.
- 36 Opinion
- 40 Legal Matters: Your Employees could be the reason you face millions in POPIA fines
- 44 SAIEE Membership
- 46 SAIEE Council
- 48 SAIEE Centres
- 49 SAIEE Events Calendar



Dear **wattnow** Reader,

South Africa utilises various types of cables for different purposes, including power supply, telecommunications, and data transmission. Submarine cables, such as the 2Africa cable, connect the country to the global network. For domestic use, low-voltage, medium-voltage, and high-voltage cables serve power distribution needs.

Our first feature article addresses the issue of cable theft in South Africa. This problem has a significant negative impact on the South African economy. The article presents insights from various industries on strategies to combat cable theft. You can read it on [page 22](#).

Aberdare Cables explores how cross-linked polyethylene (XLPE) is the most commonly used insulation material for medium voltage (MV) cables, operating between 6.6kV and 33kV, due to its excellent mechanical and electrical properties. This topic is further discussed in the article "The Impact of Radial Water Blocking on MV XLPE Cable Systems" on [page 26](#).

An impressive 97% of enterprise organisations are investing in data-driven initiatives. However, IT leaders face a complex challenge in effectively implementing these innovative technologies within their enterprise networks. Read the article "Four Trends Impacting Networks and How to Support Them" on [page 28](#) for more details.

The June issue will feature Motors & Drives, and the deadline for contributions is 16 May. Please send any submissions to minx@saiee.org.za.

Herewith the May issue - enjoy the read!

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 early 1900s was the golden era, when various associations were being formed in South Africa, primarily driven by the development of the mining sector and the railways. Voluntary associations have played a crucial role in developing engineers for South Africa's progress; however, recently, members have been exiting the associations, and the intake of new members has been declining.



[E: president@saiee.org.za](mailto:president@saiee.org.za)

Repositioning The South African Institute of Electrical Engineers Through Strategic Partnerships

Voluntary associations find it increasingly difficult to grow and retain membership today. The factors for the decline in membership vary from affordability to relevance.

One may have to look back into our history to strategise for the future. The success of our Voluntary Association (VA) will require us to critically analyse why we no longer have the exponential membership growth we once had. Could we have accidentally strayed away from the objectives of our founders? To answer this question and to find solutions to the current challenge of membership numbers, I chose to look back at the history of the formation of the South African Institute of Electrical Engineers (SAIEE). If the Institute's objectives are no longer being practised, then I would propose that we start to focus on establishing strategic partnerships to rekindle the relevance of our 116-year-old Institute.

SAIEE was formed in June 1909, with the first elected President being CWR Campbell. It was formed as a club where

engineers could belong and develop friends and colleagues. It was at a stage when mining and the railways were booming in South Africa, and various technologies were being explored in these industries. As the engineers from Britain and Germany settled in South Africa, the Institute became a home where they could compare notes and keep up to date with the developments in South Africa. One of the goals was for the Institute to achieve recognition of some status and we are proud that the Engineering Council of South Africa (ECSA) recognises SAIEE as an accredited VA.

The founding members wanted to be known as a "learned society" in which the strength was based on collective wisdom. The growth in membership numbers was essential for the achievement of this objective. The SAIEE coat of arms uses the words 'VIS NULLE SINE SCIENTIA', which translates to 'There is no strength without knowledge.' If we want to live up to the words in our coat of arms, it can only be achieved through growing our knowledge base,



which will mean expanding our reach in the country. Strategic partnerships, as well as our knowledge and strength, are essential to developing this reach.

The SAIEE founders also realised that essential work occurs at the national centres. This resulted in the formation of Cape Town on 11 June 1953, followed by Durban on 17 October 1957. I share this view. I believe that the Head Office exists as the administrative hub of the Institute, where matters of policy and compliance are managed. The real footwork takes place at the centres. Having been the past Chairman of the KZN centre, I often felt like the centre had to 'fight' with the head office for the means to its existence. Should it not be the other way around that Head Office could not exist without the centres. I want to leave this thought to the Centre Chairpersons and the Honorary Vice President to address in collaboration with the CEO. It should not be us and them but our collective strength. The first President of the Institute, Campbell, themed his inauguration address 'Relations of engineers of all branches to

one another.' This underscores why it is essential that the role of the centres gets reinforced again.

President Campbell emphasised the importance of a network of professionals supporting one another. He stated that our professional life is underscored by our 'mutual dependence on another for assistance and guidance.' We cannot achieve this if we do not establish these strategic partnerships to expand our circle of influence for the good of engineering wholistically. It is important to note that President Campbell did not see the various engineering streams competing. Instead, he acknowledged the other streams of engineering, namely Civil, Metallurgist, Chemist, Mechanical and Mining. In the early days of electrification in South Africa, the role of electrical engineers and the influence of the Institute was to improve communication and lighting. I find it interesting that in 1909, President Campbell stressed the increasing importance of electrical engineers as the rail transitions to be 'equipped with electric motive power.' Today, 116 years

later, we find ourselves at a different precipice. Electrical, electronic, and computer engineers, technologists, technicians, and artisans are essential in transitioning to alternate energy sources and moving from internal combustion engines to electric vehicles. We are still relevant but for a different challenge.

The initial objectives of the institution that went into the Constitution were to promote the advancement of electrical science, hold meetings for reading and discussing communications and electrical science, and form a technical library and laboratory for research in electrical science. Are we still upholding these objectives? Can it be done without strategic partnerships? We need to get back to networking at all levels of the Institute and even open some of these discussions with non-members to exchange knowledge and live up to the coat of arms. We need to build partnerships with sister institutes and not be in competition with each other. President Campbell referred to this as the need to reciprocate with 'ungrudging assistance' so that we jointly assist in

the development of South Africa. Wise words that we now need to live up to.

In the early days, the emphasis was on growing the student sections. This is where the membership came from and would come from. The formation of the Student Section was proposed by JS Ross on 11 August 1910 and started with 12 members. He suggested that the Section have its own President and associated structure. However, it was settled that JS Ross would be the Chairman of the Student Section. This laid the foundation for the formation that still exists today. However, I believe we are not doing enough with the student 'section'. We need to build our relations with the tertiary institutions at all centres and preferably get an academic to drive this student membership. I would probably not have joined SAIEE as a student member in 1990 had it not been for Professor Odendaal at the then University of Natal, who played an active role in the student membership of SAIEE. Let us use this opportunity to imprint in the young minds the role they can play in the development of South Africa by joining SAIEE. Let them start to appreciate the value of the Institute so that they are not reliant on an employer to pay their membership fees and are willing to pay the membership fees out of their salaries. They will do this if they see value in belonging, gaining knowledge, and having a network where they can start contributing to the profession. In 1914, President Elsdon-

Dew stated, "In this Institute's prosperity lies the success of Electrical Engineering in South Africa! It is only through new members that SAIEE will prosper. Our student members will remain with us if they see value in the Institute. Let us convince these members of the value of doing what Past President Price wanted the Institute to do by 'advising and assisting youthful engineers on matters pertaining to their advancement'.

I am not oblivious to the task ahead of me as the President of this illustrious institution. When I joined the SAIEE as a student member in 1990, I would never have thought that 35 years later, I would be bestowed the title of President of the SAIEE. It's a role that you cannot put your hand up for or apply for. It's a role that others in the SAIEE network would have to nominate and elect you for. I have the full realisation that I cannot let them down. My comfort is that I can always look back at past presidents' goals and try to emulate what they have done for the Institute. I also feel that the past presidents still active in SAIEE or the Council will guide me in repositioning the SAIEE for relevance today and into the future. **wn**



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



WEG Electric Panels

Locally produced and built to global standards, WEG electric panels ensure operator safety and protect your property. With easy assembly, installation, and maintenance, our standardized designs offer seamless expansion and interchangeability.

Trust WEG for superior performance.



SAIEE inaugurates new President



On Thursday, April 24, 2025, the South African Institute of Electrical Engineers (SAIEE) held its annual general meeting (AGM) at SAIEE House in Observatory, Johannesburg.

During the AGM, the SAIEE celebrated the inauguration of its 2025 President, Mr. Veer Ramnarain. With over thirty years of experience in the power generation, transmission, and distribution industry, Mr. Ramnarain has predominantly held Senior and Executive Management positions.

He holds a Bachelor of Science in Electrical Engineering, a Diploma in Engineering Business Management, a Master of Business Administration, and a Government Certificate of Competency. Additionally, he is a Registered Professional Engineer with the Engineering Council of South Africa (ECSA). His influence in the industry extends to tertiary institutions and various national and international professional organizations, including ECSA, SAIEE, CIGRE, IEC, NRS, NECOM, and AMEU.



Mr Veer Ramnarain, 2025 SAIEE President.

The newly elected SAIEE Office Bearers are:

- Veer Ramnarain, SAIEE President
- Prudence Madiba, SAIEE Deputy President
- Prof. Willie Cronjé, SAIEE Senior Vice President
- James Motladiile, SAIEE Junior Vice President
- Pascal Motsoasele, SAIEE Immediate Past President
- Prof. Pat Naidoo, SAIEE Honorary Treasurer
- Dr. Mohamed Khan, SAIEE Honorary Vice President.



Pascal Motsoasele, 2024 SAIEE President, reflecting on his term in office.



From left: TC Madikane, ECSA President and Veer Ramnarain, 2025 SAIEE President.

Watch the recording of the AGM [here](#). **wn**



2025 SAIEE Office Bearers

From left: James Motladiile, Junior Vice President; Pascal Motsoasele, Immediate Past President; Prof Willie Cronjé, Senior Vice President; Prudence Madiba, Deputy President, Veer Ramnarain, SAIEE President; Prof Pat Naidoo, Honorary Treasurer and Dr Mohamed Kahn, Honorary Vice President.



Leanetse Matutoane, SAIEE CEO



Prof Naidoo delivering 2024 Financial results.



From left: Nomsa Motsoasele and Sherona Ramnarain.



SAIEE partners with Festo to introduce a digital learning portal to its professional members



The South African Institute of Electrical Engineers (SAIEE) fosters technical knowledge, professional development, and innovation within South Africa's electrical engineering sector.

As technology evolves and industries move towards smarter, more automated solutions, continuous learning has become essential for engineers to remain at the forefront of industry advancements. Through this transformation and a comprehensive technical needs analysis, Festo and SAIEE forged a groundbreaking partnership to introduce SAIEE professionals to digital learning via the Festo Learning Experience platform.

Festo, a pioneer in industrial automation, launched this e-learning platform to equip professionals with in-demand technical skills, enhance workforce efficiency and support lifelong learning with flexible, high-quality courses that can be accessed anytime and anywhere.

This innovative portal offers didactically prepared learning content for many technical areas, such as electrical engineering, power grids, digital technology and electric drive technology. Through the intelligent combination of eLearning courses and practical exercises, professionals are able to elevate their knowledge and ensure their employability in the high-tech industries.

HOW DOES THIS PLATFORM WORK?

Professionals can select a course they are interested in, complete the registration, and the course will be assigned to them. Festo LX is a user-friendly web-based learning portal that allows users to access their courses at their leisure. All that is needed is a tablet, laptop, or smartphone with an internet connection. Upon completion, users

receive certificates for completing all the learning paths on Festo LX, which can boost the credibility of engineers in the job market. These certifications demonstrate technical proficiency and help professionals stand out in a competitive industry. Register today and experience the power of digital learning and enhance your expertise with the latest skills and knowledge in the technical field.

HOW TO REGISTER

Learning made easy in 5 easy steps:

Step 1: Visit [SAIEE Training Academy e-Learning](#)

Step 2: Select your course of choice

Step 3: Make payment for the course

Step 4: Register to log into your Festo LX profile

Step 5: Start learning once the course is assigned

The collaboration between SAIEE and Festo unites two industry giants, each committed to driving technical excellence and innovation.

Festo, a global pioneer in industrial automation, leverages decades of expertise in engineering education. As a leader in professional development, SAIEE empowers electrical engineers with the knowledge and skills needed to stay at the forefront of industry advancements. Together, they are transforming the future of engineering education by delivering world-class digital learning opportunities. This partnership will empower industry professionals and strengthen the



Festo Learning eXperience

A digital learning portal that empowers industries with interactive, flexible and industry-relevant training in automation and technical education.

→ Discover more about Festo LX

workforce, fostering a more skilled, competitive, and future-ready industry.

If you need further assistance or have any questions about this platform, our team at SAIEE is here to help. Contact us at training@saiee.org.za.

We are committed to providing the support you need to maximise your learning experience.

Click here: [Festo Learning Experience - Digital Learning as individual as you are](#) to explore the future of learning and the innovative experience that awaits you! **wn**

DO YOU NEED CPD CREDITS BUT DON'T HAVE TIME?



Register for our
E-learning courses and earn your
CPD credits in your own time!*



Invest in your greatest asset today. Invest in YOU.

** Each course does have a deadline date of ±30 days to complete.*

ONLINE & FACE-TO-FACE TRAINING COURSES | GROUP BOOKING DISCOUNTS | INHOUSE TRAINING

T | 011 487 3003 | training@saiee.org.za | www.saiee.org.za | view our course brochure [here](#)

Schneider Electric appoints Canninah Dladla as Cluster President for English-Speaking Africa



Schneider Electric, the global leader in energy management and automation, and recognized sustainability leader, has announced the appointment of Canninah Dladla as its new Cluster President for English-speaking (Anglophone) Africa, effective from 1 June 2025.

Dladla is Schneider Electric's first female Cluster President for English-speaking Africa, which comprises 24 countries and is headquartered in Johannesburg, South Africa. The region is important to Schneider Electric due to its rapidly growing economies and expanding populations.

The growing demand for energy and sustainable solutions makes Dladla's appointment strategic, which is in line with Schneider Electric's mission to promote sustainable growth through innovative energy management across the continent. She succeeds Devan Pillay, who will transition into his new international role as Segment President, Heavy Industries based in London, England.

Dladla has a well-established history with Schneider Electric from 2008 to 2013, spanning various strategic roles, including the position of Vice President for the company's Energy Business within its Power Systems division. She now rejoins Schneider Electric with an impressive 29-year career and a proven track record of impactful leadership.

Dladla most recently served as Managing Director and Country Sales Director, Africa of Rockwell Automation, where she played a key role in championing business transformation and promoting cultural alignment, ensuring that global strategy was seamlessly adapted to local markets.

As a brand and culture ambassador, Dladla was instrumental in driving

Rockwell Automation's expansion across both English-and French-speaking Africa, strengthening its regional presence while fostering a more inclusive and locally relevant approach.

Amongst other leadership roles, she also held an executive management role at GE Power, driving strategic accounts and key Business Transformation initiatives.

"We are thrilled to welcome Canninah Dladla into this pivotal leadership role. Her extensive industry expertise, proven leadership skills, and innovative vision will undoubtedly drive our operations and growth across English-speaking Africa.

Canninah will be leading this region on specific areas, starting with talent development and technology deployment towards our targeted segments through digitization and electrification, whilst ensuring that we continue to empower our customers, partners, and communities across the continent," states Walid Sheta, Zone President, Middle East & Africa at Schneider Electric.

Dladla adds, "I'm delighted to rejoin Schneider Electric at a time when Anglophone Africa shows great potential for transformation. The region holds many prospects for economic growth through improved infrastructure and expanded electricity access with its combination of vast natural resources, growing urbanization, and rising sustainable energy needs. Schneider

Electric's global and local expertise will enable me to drive innovative solutions and services which will empower businesses and communities whilst unlocking new possibilities that create enduring positive effects for millions of Africans,"

As Schneider Electric welcomes Dladla, the company would also like to acknowledge Pillay's outstanding tenure. During his leadership, his experience and expertise in energy and technology have helped the company to strengthen its presence in Anglophone Africa.

This was achieved through his segment-driven growth strategy, which increased the company's regional presence and reinforced its leadership in sustainability and innovation. His efforts in promoting renewable energy solutions and local empowerment have made Schneider Electric a key driver of sustainable progress across the continent.

With Dladla at the helm and the continued support of employees, partners, and customers, Schneider Electric looks forward to driving continued sustainable innovation and delivering even greater regional success. **wn**



ABB's electromagnetic stirrer improves efficiency and sustainability at Çolakoğlu Metalurji in Türkiye



ABB has secured an order from Çolakoğlu Metalurji A.Ş. for an ArcSave® electromagnetic stirrer (EMS) to be installed on one of the world's largest electric arc furnaces (EAF). This project in Türkiye represents a significant step forward in Çolakoğlu Metalurji's journey toward enhanced efficiency, sustainability, and operational safety in their steelmaking processes.



ABB's ArcSave EMS will be installed on a jumbo 370-tonne capacity EAF, the largest of its kind in the country. Primetals Technologies supplies the furnace at Çolakoğlu's steel plant, which will benefit from a revamp courtesy of ABB's advanced stirring technology. The revamp will enhance the production of various carbon steel products, including slabs, hot-rolled steel coils, billets, and reinforcing steel bars.

Founded in 1945, Çolakoğlu Metalurji has evolved from a small-scale production facility into one of the leading steel producers in Türkiye, establishing its first rolling mill in 1969 and its melt shop in 1985. The commissioning of its first EAF in 2007 marked a significant shift towards more sustainable steelmaking. Today, Çolakoğlu operates one of the largest and most advanced steel production facilities in Türkiye dedicated to technological advancement and sustainability, maintaining the highest standards of quality and efficiency.

Çolakoğlu Metalurji's investment in ArcSave highlights its legacy as a leader in sustainable steel production. The EMS will assist the company as it strives to achieve its sustainability targets through rapid chemical and thermal homogenisation in the furnace.

"This project presents many intricate technical hurdles to overcome," said Özgür Özsoy, Plant Director at Çolakoğlu Metalurji. "We were highly impressed with how ABB plans to navigate these challenges on the way to seamlessly integrating its ArcSave technology into our operations."

This collaboration will not only enhance the efficiency and sustainability of our steelmaking processes but leaves us confident that we have selected a partner that embodies our values of installing innovative solutions for a sustainable future."

"This project exemplifies ABB's versatility in working with customers," said Zaeim Mehraban, Global Head of Sales, ABB Metallurgy. "Integrating our ArcSave electromagnetic stirrer into the world's largest Primetals electric arc furnace underscores our commitment to enhancing the efficiency and sustainability of large-scale electric arc furnace operations and providing customers with industry-leading service and expertise."

Commissioning of ArcSave at Çolakoğlu's plant is scheduled for the fourth quarter of 2025. **wn**

Industrial Acoustic Imaging Tool

VISUALIZES SOUNDS OF SMALL LEAKS IN COMPRESSED AIR, GAS, AND VACUUM SYSTEMS



The Fluke ii Industrial Acoustic Imager series, equipped with an array of microphones for an expanded field of view, enables maintenance teams to locate leaks from compressor systems quickly and accurately, even in the noisiest environments. This product includes Fluke's innovative SoundSight™ technology, which overlays the sound map onto the image. If you can use a camera, you can use the Fluke Industrial Acoustic Imagers.

VALUE AND RETURN ON INVESTMENT

Even the smallest air leaks can compound over time, leading to massive energy waste and lost production time. According to the U.S. Department of Energy, compressed air systems can lose 20 to 30 percent of their output from leaks alone. For example, according to the DOE, a 1.5 mm-sized air leak at a flow rate of just 6.5 cfm will cost R 19.02* per year. That is just one leak.

Fluke, locally represented by COMTEST, is a global technology leader in manufacturing compact professional electronic test and measurement tools and software. It offers the Fluke ii Industrial Acoustic Imager series, a hand-held, easy-to-use tool that visualises sounds coming from small leaks in compressed air, gas, and vacuum systems.

One Fluke customer, a manufacturer, was spending between 30 and 45 minutes to find just one air leak. After testing the Acoustic Imager, the maintenance manager stated, "Rather than taking at least an hour to move everything out of the way, position the lift, spray the joint, and then put everything back, it now takes me only 30 seconds to a minute to locate an air leak with the ii camera. Some days, we can identify and repair 30 or 40 leaks in just a couple of hours." They added, "Moreover, we can use the ii cameras during production hours, when it's exceptionally loud in here, and we are still able to detect leaks at the rafter level, up to 6 to 9 metres away."

Another customer commented on the use of the LeakQ software, "Now I have something visual to show my customers. I can present them with images as an excellent aid, and it emphasises the importance of fixing those leaks to maximise system capacity."

*Values are indicative and subject to change.

The Fluke ii915 full package includes:

- Fluke ii915 Acoustic Imager
- USB-C Charger with country-specific connectors.
- Rugged lithium-ion smart battery pack
- USB-C cable
- Rugged, hard carrying case
- Adjustable hand strap and neck strap
- Sensor array protector

For more information, contact Comtest on www.comtest.co.za **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

SAIEE KZN Centre participates at the DUT Orientation Day



Dr. Mohamed Fayaz Khan, the Deputy Chairman of SAIEE KZN, was invited to speak at the First Year Orientation for Electrical Power Engineering students at the Durban University of Technology on March 13th.



From left: Prof Katleho Moloi, DUT and Dr Mohamed Fayaz Khan, SAIEE KZN Centre.

Dr. Mohamed Fayaz Khan, the Deputy Chairman of SAIEE KZN, was invited to speak at the First Year Orientation for Electrical Power Engineering students at the Durban University of Technology on March 13th.

He delivered a 20-minute presentation to a packed room of eager first-year students, helping them understand the career journey they have embarked upon and the many opportunities awaiting them upon graduation.

This event also provided a valuable opportunity to discuss the role of the

SAIEE in the electrical engineering landscape and the numerous benefits available to student members. Following his presentation, Dr. Khan answered questions from the students, leaving them with a message of encouragement. He motivated them to work hard to overcome the challenges ahead and to explore the potential of the new technologies emerging in the fourth industrial revolution.

Afterward, Dr. Khan met with senior staff in the department to discuss plans for re-establishing the SAIEE-DUT Student Chapter in 2025. Watch this space. **wn**



WE SELL CABLE

Since 2007, Continental Cables has sustained a continuous supply of quality cables at a competitive rate to customers across sub-Saharan Africa - growing to become one of Africa's largest power cable distributors.



Alberton	+27 011 617 1500
Durban	+27 031 304 1417
Pretoria	+27 012 111 9719 / 086 166 900
Nelspruit	+27 013 518 0237

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, Free State](#)

Bloemfontein Campus:

+27 (0)51 507 391

Welkom Campus:

+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



BECOME A CORPORATE PARTNER TODAY!

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 in many countries worldwide.



Corporate Partners

Corporate Partners are invited to monthly forum meetings to discuss and brainstorm critical issues in South Africa and find solutions.

Corporate Partners receive:

- Access to 6000 engineering practitioners
- Rub shoulders with your industry peers
- Preferential rates on all SAIEE advertising platforms
- Access to the peer-reviewed Africa Research Journal
- Website Listing linking to your website
- Product Launch Platform
- Training Facilities
- Networking Opportunities
- Recruitment Administration
- Skills Development Courses
- Preferential CPD training course rates for your employees
- Assisted Corporate Social Responsibility
- Mentorship
- Offering SAIEE Students Workbased Integrated Learning (WIL)



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.

[SAIEE Company Profile](#)

Contact Us

-  SAIEE House, 18A Gill Street, Observatory, JHB
-  minx@saiee.org.za
-  www.saiee.org.za

Cable Theft in South Africa



Cable theft in South Africa is not just a simple crime but a complex issue with far-reaching consequences. In particular, the theft of copper cables has become a significant problem that plagues the country, causing havoc and chaos.

*By: Minx Avrabos (PM, IAPW&E)
Managing Editor, wattnow*

This vandalism disrupts essential services and contributes to power outages, leaving communities in the dark and businesses at a standstill. The impact of cable theft is not limited to just inconvenience; it has severe economic and social implications that reverberate throughout the country.

One of the most troubling aspects of cable theft is its effect on essential services. Telecommunication networks, rail transportation, and power infrastructure rely on copper cables to function efficiently. When these cables are stolen, the services they support are disrupted, leading to widespread inconvenience for consumers and businesses alike. In some cases, entire communities are left without access to communication, transportation, or electricity, creating a ripple effect that can be felt for miles around.

The consequences of cable theft are not limited to just inconvenience; they also harm the economy. The South African economy loses billions of rand annually due to cable theft, as companies are forced to spend exorbitant amounts of money replacing stolen cables and repairing damaged infrastructure. This money could be better spent on investments that promote economic growth and development, creating jobs and opportunities for the people of South Africa.

Furthermore, cable theft perpetuates a cycle of crime and violence in South African communities. The thieves who

engage in this illicit activity often operate in dangerous conditions, risking their lives for a quick buck. This underground economy fuels criminal behaviour and perpetuates a culture of lawlessness and impunity. The social consequences of cable theft are far-reaching, affecting individuals and their communities.

We take a more detailed look at the impact Copper theft has in South Africa.

ECONOMIC IMPACT

The theft of copper cables is estimated to cost the South African economy billions of rands each year. This includes direct losses to state-owned enterprises like Eskom and Transnet and indirect costs related to security, repairs, and production losses.

In April 2023, large parts of Tshwane were plunged into darkness for several days due to the collapse of power lines. Upon inspection, three pylons were found to have been vandalised, leading to the failure of the power lines.

The widespread theft of copper cables and other forms of metal from public infrastructure threatens to cripple our nation and has serious real-world consequences. Metal theft impacts the power supply, often plunging suburbs into darkness, leaving trains unable to operate and causing massive damage to public facilities throughout the country.

DISRUPTION OF SERVICES

Cable theft leads to frequent power outages, disrupts transportation

(especially rail), and impacts telecommunications networks, affecting businesses and residents.

Cable theft significantly impacts crucial services like public transport, electricity, telephone, and the internet. Trains are delayed and cancelled when cables are stolen from the rail system because the infrastructure is badly damaged (Western Cape Government, 2019).

Furthermore, this affects free-flowing traffic, as road users are stuck in traffic, causing congestion and also affecting the economy.

Traffic congestion has been increasing in much of the world, developed or not, and everything indicates that it will continue to get worse, representing an undoubted menace to the quality of urban life. Its main expression is a progressive reduction in traffic speeds, increasing journey times, fuel consumption, other operating costs and environmental pollution compared to an uninterrupted traffic flow (Bull, 2003). Cable theft worsens traffic congestion in developing and developed countries as criminals destroy the telecommunication and transportation infrastructure, contributing negatively to the economy. Cable theft affects the community in various ways, including the inconvenience of power outages, the loss of appliances, the loss of revenue, the loss of perishable produce, traffic congestion, the loss of business/production, and the loss of communication and business.



INCREASED SECURITY COSTS

The need for increased security measures to prevent cable theft, such as private security companies, patrols, and surveillance, adds to the economic burden.

ORGANISED CRIME

Cable theft is often linked to organised crime syndicates, with stolen materials laundered through scrap metal markets. According to research by Genesis Analytics commissioned by the Department of Trade, Industry, and Competition, the economic damage inflicted by copper cable theft is estimated at more than R45 billion annually.

It is all part and parcel of organised crime networks that have become embedded in South Africa as a result of state failure and rampant corruption. According to World Bank estimates, crime robs South Africa of about 10% of its GDP annually.

Copper cables are coveted because of the metal's price and many applications. Much of the stolen material is laundered in the scrap metal market.

Advancing satellite technology and automation will consign at least one target for cable thieves to the dustbin of history.

GOVERNMENT AND PRIVATE SECTOR EFFORTS

Various initiatives are underway to combat cable theft, including partnerships between law enforcement, private security companies, and state-owned enterprises.

Through its efforts to curb cable theft and vandalism in the province, the Gauteng government has shut down

1,079 scrap yards for non-compliance and commissioned a 24-hour response team to tend to these crimes. This was announced in Gauteng Premier Panyaza Lesufi's State of the Province Address (Sopa) in February 2025.

The Premier said that in addition to shutting down scrap yards and launching a response team, Gauteng has also shut down 593 spare shops and 149 tyre shops found to be operating illegally.

According to the province, 716 owners and operators have been arrested and tried in Gauteng courts.

Copper is the second-best conductor behind silver, making it an attractive target for criminal syndicates wanting to sell the mineral on the black market.

As a result, the theft of copper cables has degraded and hindered the operation of numerous forms of infrastructure throughout South Africa.

ESKOM'S RESPONSE

Eskom, South Africa's electricity provider, is actively working to phase out copper cables in favour of alternative materials to reduce the attractiveness to thieves.

Cable theft significantly contributed to the intense load-shedding that South African residents experienced in 2021, 2022, and 2023.

"We are moving away from using copper because we have seen that it is quite in demand, so whenever we have any cable that has been stolen, we do not replace it with copper," Eskom's Gauteng spokesperson, Amanda Qithi, said in May 2024.

The theft of copper is also hurting South Africa's mobile networks, with thieves

targeting power cables at cellphone tower stations or base stations.

Vodacom loses roughly R100 million to mobile tower battery theft and infrastructure vandalism per year, and repairs to a single site's infrastructure can cost up to R100,000.

MTN said it had experienced close to 500 incidents of theft and vandalism, which ultimately cost R450 million to replace stolen batteries and damaged base stations in 2024.

Similar to how it affects Eskom's uptime in certain areas, vandalism at base stations can result in prolonged downtime.

PUBLIC REPORTING

Citizens are encouraged to report cable theft incidents to the authorities to help combat this problem.

The government is working to end metal theft through a smart mix of regulations and enforcement, but we need an all-society approach to tackle this most complex issue. All of us need to stop cable theft, and we need to do it now. These actions are an attack on our democratic order and our very way of life. They affect all of us, and therefore, we all need to stand up to end them.

PENALTIES

According to South African law, theft of cables, particularly copper cables, is a serious crime with potential penalties including imprisonment and fines.

The changes are in the Criminal Matters Amendment Bill 2015, which the Justice and Correctional Services Ministry tabled in 2024, creating a new offence.

"It criminalises the unlawful and

intentional tampering with or damaging or destroying of essential infrastructure and provides for the possibility of the imposition of a severe penalty, namely imprisonment, which may be up to 30 years," a ministry memo explaining the bill said.

"The creation of this offence provides an opportunity for the legislature to emphasise the seriousness of this offence by allowing for the imposition by courts of a harsh sentence, and to ensure that legislation is in place to regulate this aspect adequately, instead of having to rely on the common-law offence of malicious property damage, which is often regarded as a minor offence."

The bill says bail for such crimes may be granted only by courts. When those in positions of trust – police, security guards, employees or contractors of the entity targeted, or gangs are involved, it is regarded as a more serious offence and thus more difficult to get bail. Minimum sentences are harsh. First-time offenders face a minimum of three years in jail. A second offence brings five years, and a third time around, it's seven years.

Scrap-metal and secondhand dealers caught with any metal bits of "essential infrastructure" that cannot be legally explained face a minimum sentence of five to ten years.

The memo states that those whose interference with essential infrastructure is regarded as organised crime should expect minimum sentences of 15, 20, or 25 years, depending on the convicted person's previous convictions.

This part of the bill links the infrastructure crimes to the Prevention of Organised Crime Act.

The essential infrastructure is "any installation, structure, facility or system, whether publicly or privately owned, the loss or damage of, or the tampering with, which may interfere with the provision of a basic service to the public", the bill says.

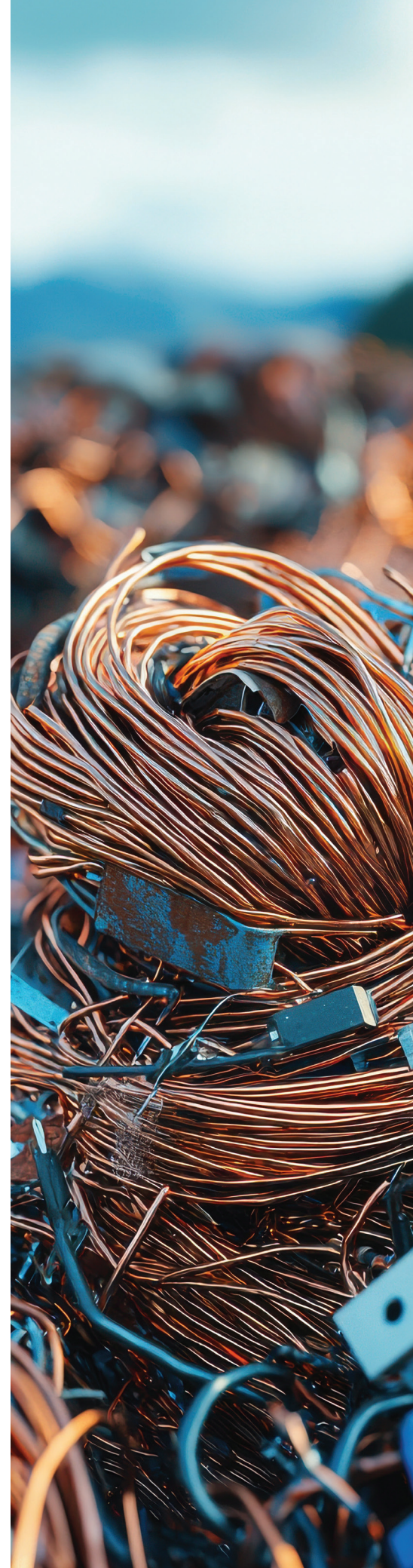
Basic services include energy, transport, water, sanitation and communication.

The bill explains that "essential infrastructure-related offences are becoming increasingly more organised and are often committed by armed and dangerous criminal groups." While the actions may sometimes seem relatively minor, they cause considerable damage to essential infrastructure.

Vandalism and theft of public infrastructure pose a significant risk to our nation and its people, and decisive action is needed to protect our vital infrastructure. Transnet, Eskom, and the South African Police Service have all indicated that copper and ferrous metal theft has reduced but remains at very high levels and continues to cause considerable damage to the infrastructure and the economy.

In conclusion, cable theft in South Africa is a significant issue that requires urgent attention and action. The disruption of essential services, the economic losses incurred, and the social implications of this crime can no longer be overlooked.

Authorities must adopt a proactive approach to combat cable theft, implementing measures that deter thieves and hold them accountable for their actions. Only through collective effort and cooperation can South Africa tackle this pressing problem and protect its infrastructure for the future. **WN**



The Impact of radial water blocking on MV XLPE Cable systems



The high-performance cross-linked polyethylene (XLPE) material is the most common insulation used in medium voltage (MV) cables between 6.6kV to 33kV mainly because of its impressive mechanical and electrical properties.

*By: Donemore Torerwa
Electrical Engineer; MEng, BSc (hon)
GM: Product Development and Applications
Aberdare Cables Pty Ltd*

XLPE's properties are impacted drastically if exposed to water and moisture, resulting in water trees; it becomes imperative in design to ensure that the cable structure offers water ingress protection to the XLPE insulation. The XLPE cable life is usually estimated to be above 30 years, but once XLPE material is exposed to water or moisture ingress, the life of the cable is affected, hence it then becomes essential that from the start of manufacturing, the cable production processes are well controlled to prevent any moisture or water ingress (The more reason why cable users must consider buying their cables from reputable cable manufacturers). It is also essential to prevent moisture ingress during cable operation by ensuring that the jointing and termination workmanship is up to standard and the cable will withstand the conditions under which the cable is installed.

SANS 1339 is a compulsory standard in South Africa covering cables with voltages rated from 6.6kV to 33kV (MV Cables). This standard specifies longitudinal and radial water blocking for MV Cables when required by the cable user. Longitudinal water blocking is the most commonly deployed water blocking method as applied by many cable manufacturers in the local market, mainly because it is relatively easy to implement. Longitudinal water blocking alone, however, may not be enough to offer the lasting water-blocking capabilities of a cable in some environments, especially in areas with

high groundwater levels. Offering radial water blocking becomes key to cables to ensure the enhanced water-blocking capability of MV XLPE cables at the design and manufacturing level. Radial water-blocked cables are not very common in South Africa for MV Cables; they are common for high voltage (HV) cables for 44kV-132kV rated cables (making use of CSA (Corrugated Seamless Aluminium)).

Longitudinal water blocking is intended to prevent water ingress and spread in the areas between cores, armouring, metallic screens, and insulation through moisture absorption barriers installed within the structure of the cable along its length. Water block yarns and tapes are commonly installed in the interstices of the multicore cables or around the bedding layers of single-core cables. If exposed to moisture, the yarns will absorb and swell, preventing further ingress of the water or moisture inside the cable, hence offering protection. As per SANS 1339 of 2020, the cable will be type tested for conformance, which becomes essential for the users to ask for these type test reports when purchasing all the cables claimed to have such features.

Radial water blocking features are not very common in South Africa's industry; this is also why the SANS 1339 standard does not specify the radial water blocking requirements in detail. Radial water-blocking technology relies on an impermeable concentric layer around the cable, preventing radial water



ingress. Radial water blocking in high-voltage cables is achieved through the CSA structure, which offers mechanical protection, earthing, screening, and radial water blocking for the cable. The common global radial water protection material for MV Cables includes lead sheathing, aluminium-laminate tape, and smooth welded aluminium tape. The cable, which offers both longitudinal and radial water ingress protection, has considerable use in areas with high water levels, mainly the coastal regions of South Africa as well as any wetland; for such applications, the paper cable with lead sheath has always been the best option which is the main reason why most coastal areas still prefer MV paper lead sheathed cables as opposed to XLPE MV Cables.

It is important to note that due to the thermal performances of XLPE MV Cables, paper MV cables have much lower current or load ratings than XLPE MV cables. Paper MV Cables may also introduce environmental issues related to the impregnated oil and lead. Hence, XLPE is the better way to go, especially if it has radial water-blocking features.

Understanding the challenges related to the continued use of paper cables and the need to improve the life of XLPE cables, mainly when used in high-water-level areas, Aberdare Cables, the leading manufacturer of cables in South Africa, has extended its range of products to include radially water-blocked cables for MV Cables using Aluminium Laminate technology. The product is available for sale in Africa and globally. **wn**

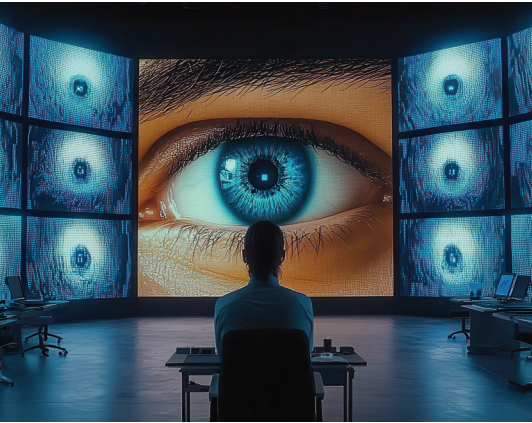


ABERDARE
A MEMBER OF HENG TONG GROUP
ENLIGHTENING THE FUTURE

**HIGH VOLTAGE
CABLES UP TO 132kV**
SANS/IEC 60840 & NRS 077

www.aberdare.co.za

Four Trends Impacting Enterprise Networks, And How to Support Them



In today's data-driven world, businesses prioritize digital transformation to unlock new opportunities and gain a competitive edge. A staggering 97% of enterprise organizations are investing in data-driven initiatives. However, IT leaders face a complex challenge: effectively implementing these innovative technologies into their enterprise networks.

*By David Knapp
Product Manager, Oberon Wireless Enclosures*

As an IT leader responsible for supporting these advancements, you understand the critical role a robust network plays. This white paper, by Chatsworth Products (CPI), dives deep into the top four trends shaping the enterprise network and explores advanced infrastructure solutions specifically designed to empower your digital transformation journey. By optimizing your enterprise network's performance and reliability, you'll lay the groundwork for a successful transformation that propels your business forward.

THE MIGRATION TO HYBRID CLOUD

Enterprise organizations originally embraced the public cloud to transform their IT spending model. The public cloud's subscription-based services and on-demand scaling capabilities facilitate a shift from upfront capital expenditures (Capex) to ongoing operational expenditures (Opex), eliminating the need for costly infrastructure upgrades. While the public cloud remains the go-

to solution for data storage, popular business applications like Microsoft 365 and Salesforce, and remote working tools like Zoom and Google Drive, a new trend is emerging. Many organizations are now migrating mission-critical and industry-specific applications to private clouds. These private clouds are hosted on premises or within dedicated leased spaces in multi-tenant data centers (MTDCs). Flexera's 2024 State of the Cloud report underscores this trend, revealing that 73% of enterprise organizations are adopting a hybrid cloud approach, leveraging both public and private cloud environments.

The high cost of the public cloud is a primary driver for enterprise organizations to adopt a hybrid cloud approach. While initial public cloud adoption aimed to reduce Opex, many businesses have found that their spending significantly exceeds expectations. A Flexera report highlights this challenge, ranking cloud cost management as the top concern,

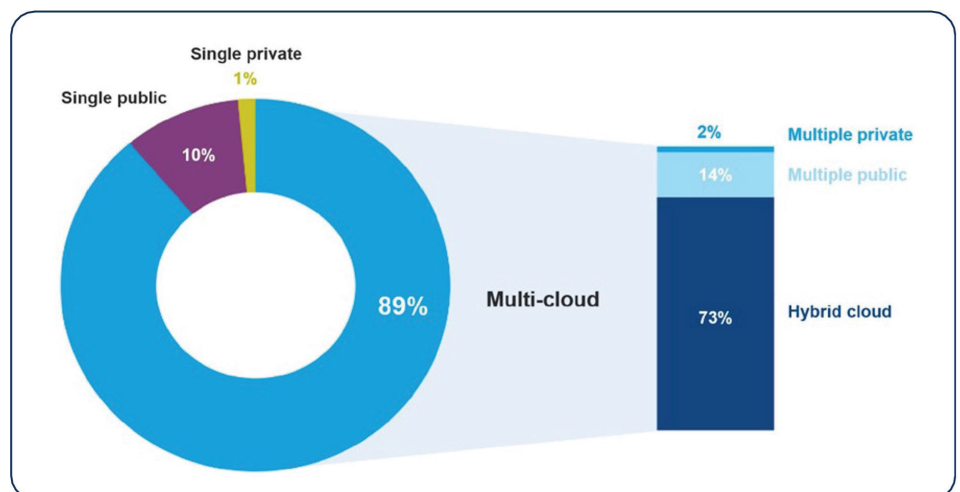


Figure 1: 89% of enterprise organizations are adopting a multi-cloud approach, with 73% opting for hybrid cloud.



with nearly half of respondents reporting cloud spending exceeded plans by some or a significant degree.

Economic uncertainty plays a role, but factors like storage and data egress fees (charges for transferring data out of cloud storage) can quickly spiral out of control if left unchecked. Lack of visibility, hidden fees, and unplanned growth all contribute to this “cost creep.” Public cloud providers have also raised hosting and storage fees in recent years to counter rising energy costs, inflation, and material shortages.

Security concerns are another primary reason for moving certain applications and data to private clouds. Public clouds offer cost-effective storage for non-sensitive data, but many enterprise organizations hesitate to store confidential information there, especially when shared resources with other organizations are involved. This includes human resource records, intellectual property, financial data, and customer information. A 2023 Flexera report found that 79% of respondents ranked security as their second-biggest public cloud challenge.ⁱⁱ Public cloud storage can also make compliance difficult for heavily regulated industries like finance and healthcare, which have strict privacy and security requirements for classified financial and medical records. While some public cloud providers may have secure infrastructure that meets compliance standards, they may not guarantee compliance at the rack level in their service level agreements (SLAs).

Ultimately, the responsibility falls on the enterprise organization to ensure compliance, which is significantly easier to manage in a private cloud environment.

While the public cloud offers cost benefits and scalability, it can limit control and customization for organizations with unique or complex application needs.

Additionally, shared resources and geographic distribution inherent to the public cloud can introduce latency issues for real-time applications like AI, virtual reality, and e-commerce

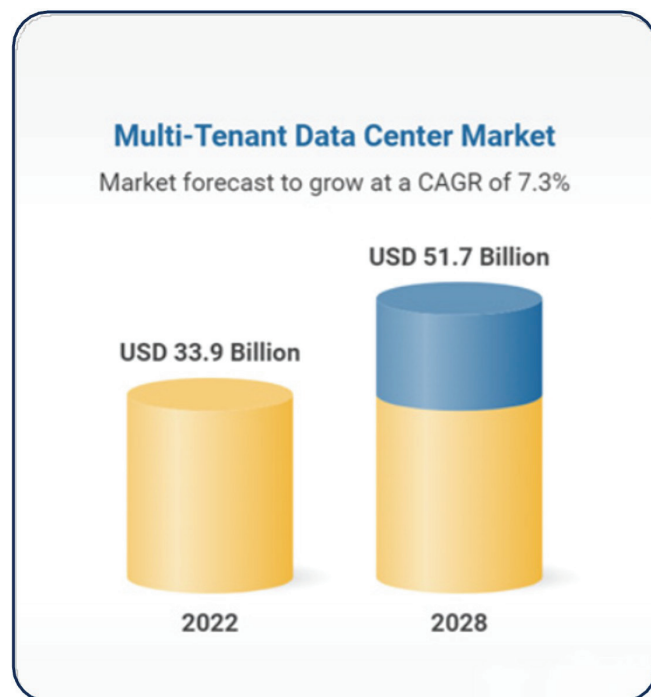


Figure 2: The multi-tenant data center market is rapidly growing.

that require closer proximity to users and devices. For enterprise organizations requiring ultra-low latency, strategically deploying cloud resources in regional MTDCs or on-prem edge data centers can significantly reduce data travel distances and minimize latency.

Enterprise organizations have long struggled to run cloud-scale applications within their on-prem data centers due to limited capacity and lack of access to high-performance computing (HPC) systems. Fortunately, the landscape is changing. Broader access to open-source solutions, cloud-scale virtualized servers, powerful GPUs, software-defined networking, efficient liquid cooling, and high-speed fiber connectivity (up to 400 Gigabits) now empower enterprise organizations to achieve high performance and scalability within their own data centers.

For organizations unable to implement private clouds on premises, regional MTDC facilities offer a compelling alternative. Retail and wholesale colocation data center deployments are booming, driven by the surge in demand

for cloud-based services and digital transformation initiatives. The global multi-tenant data center market, valued at U.S. \$33.9 billion in 2022, is projected to reach U.S. \$51.7 billion by 2028. As MTDC providers invest in new facilities across diverse locations and offer more flexible leasing options, enterprise organizations of all types and sizes can access the resources they need for private cloud deployments while also benefiting from closer proximity to users and devices for low-latency applications.

Migrating from a public cloud to a private cloud presents additional hurdles. Security, compliance, and maintaining efficiency remain concerns. Additionally, the return of Capex budgeting, a driver for the initial public cloud move, once again becomes a factor. Enterprise organizations may also face limitations due to a lack of skilled personnel, ever-changing market and customer

demands, and a resistant internal culture. To navigate these challenges, IT leaders need executive buy-in, optimized workflows, and access to training and design expertise. Partnering with trusted infrastructure providers who can guide them through complex designs, recommend suitable solutions, and ensure smooth installation can significantly bolster successful private cloud deployments.

THE RISE OF LOW-LATENCY EDGE COMPUTING

Enterprise organizations are increasingly embracing real-time technologies that necessitate low latency. This trend fuels the adoption of edge computing, which processes data near users and devices. Spending on enterprise edge infrastructure is outpacing traditional network equipment and overall IT expenditures, reflecting this shift.

Next generation 5G cellular that delivers

high-speed mobile wireless connectivity is a key edge computing technology. 5G may utilize higher frequencies with shorter ranges, requiring the deployment of denser small cells strategically placed closer to users often with local edge compute capabilities for real-time applications and high-bandwidth uplink and downlink networking for backhaul.

AI also thrives on low-latency networks. It's rapidly becoming a mainstay in enterprise organizations, tackling complex challenges and providing advanced analytics across various domains. AI offers many benefits, from improved business forecasting and threat detection to industrial automation, drug discovery, medical diagnosis, and customer service chatbots. The U.S. enterprise AI market is projected for significant growth, with a compound annual growth rate (CAGR) of 34.6% across cloud and on-premises deployments from 2022 to 2030.vi

Low-latency edge computing is crucial for various applications beyond AI and 5G. This includes the Internet of Things (IoT) and Industrial IoT (IIoT), e-commerce platforms, and predictive maintenance solutions. By processing data closer to its source, edge computing empowers these applications to deliver optimal performance.

Large public cloud data centers, often situated hundreds of miles away, are unsuitable for these real-time applications. Consequently, enterprise organizations are strategically deploying edge compute in smaller edge data centers, including remote micro data centers.

These edge data centers can vary in size and location. For instance, edge compute could reside in a single server rack in a

Growth in Enterprise Edge Infrastructure Spending

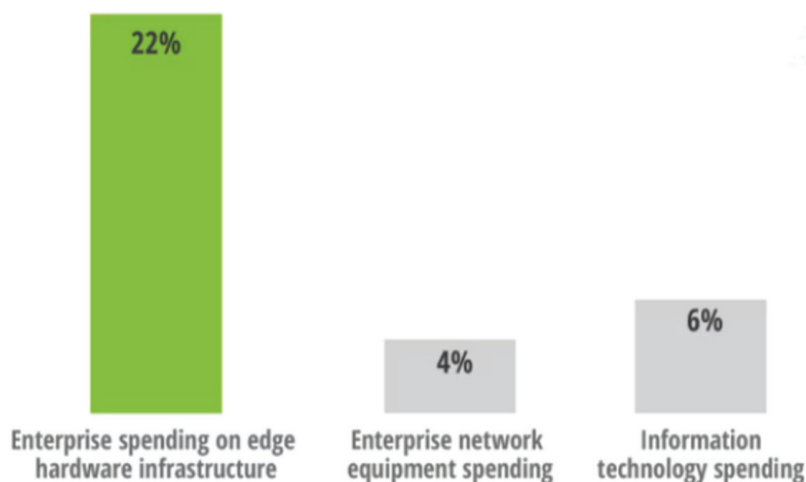


Figure 3: Growth in enterprise edge infrastructure spending is far outpacing growth in network equipment and overall IT spending.

U.S. Enterprise Artificial Intelligence Market

size, by deployment, 2020 - 2030 (USD Billion)

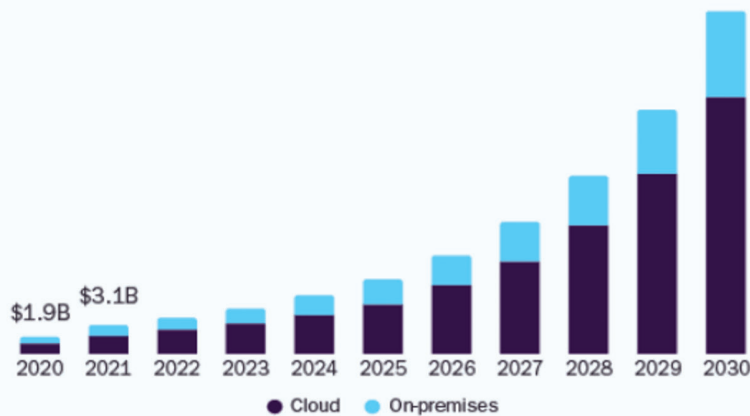


Figure 4: The U.S. enterprise AI market is expected to grow at a rate of 34.6% from 2022 to 2030.

WIRELESS CONNECTIVITY MARKET:

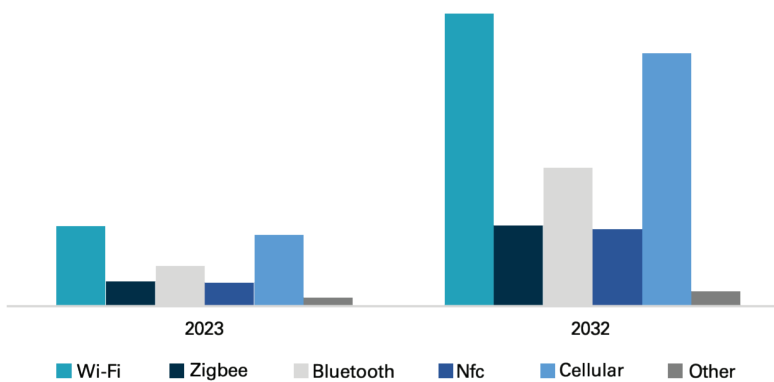


Figure 5: Wi-Fi and cellular technologies account for the majority of wirelessly connected devices.

Global WiFi 6, WiFi 6E, and WiFi 7 Chipset Market

Size, by Chipset type, 2023-2033 (USD Billion)

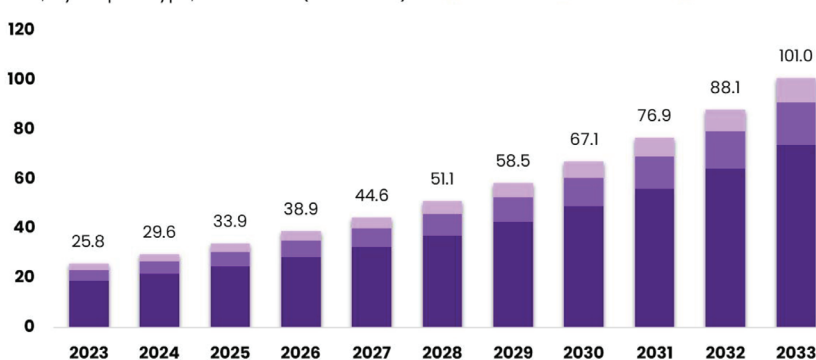


Figure 6: Wi-Fi will continue to increase, with Wi-Fi 6 predicted to maintain a larger share of the market over the next decade.

hospital telecom room to process real-time patient data. At the same time, a stand-alone ruggedized enclosure on a factory floor could support machine learning and automation tasks and remote, free-standing outdoor enclosures can provide edge compute capabilities for real-time 5G applications on industrial sites and college campuses.

ADVANCED HIGH-THROUGHPUT WIRELESS TECHNOLOGIES

The past two decades have witnessed the rise of advanced wireless technology as an essential tool. It seamlessly transmits voice, data, and video, connecting people and devices to the internet. The number of wireless devices continues to surge, with Wi-Fi and cellular networks leading the charge.

High-throughput Wi-Fi 6/6E and Wi-Fi 7 When it comes to indoor and short-range wireless connections, Wi-Fi reigns supreme. From corporate offices and hospitals to schools, factories, and even stadiums, nearly every enterprise building boasts Wi-Fi coverage. This technology is based on the IEEE 802.11 family of standards, which has seen significant advancements in speed, capacity, and coverage over the past two decades.

Wi-Fi 6 and 6E (approved in 2019 and 2020) boast impressive typical speeds of 5 Gigabits per second (Gb/s) – a fourfold increase compared to the previous Wi-Fi 5 generation. Building upon this foundation, Wi-Fi 7 (approved in 2024) further pushes the boundaries with typical speeds reaching a staggering 18 Gb/s, achieved through more spatial streams and wider channels.

While Wi-Fi 7 demonstrates immense potential, Wi-Fi 6 will dominate the market share for the next decade.

Wi-Fi 6 utilizes the traditional 2.4 GHz and 5 GHz bands, while Wi-Fi 6E and Wi-Fi 7 add the 6 GHz band to increase capacity significantly. These high-performance Wi-Fi technologies cater to a broader range of devices and applications. The 2.4 GHz band offers superior range and better penetration through walls, making it ideal for low-bandwidth IoT devices. The 5 GHz and 6 GHz bands, while having a shorter range, provide more bandwidth due to the wider spectrum and channel bonding capabilities. This makes them perfect for high-speed devices like laptops and smartphones used for streaming or large file transfers.

COMPARISON OF IEEE 802.11 AMENDMENTS - SEE TABLE 1

For today's enterprise organizations, Wi-Fi 6 and 6E are the go-to wireless solutions. However, maximizing their potential requires a robust network LAN infrastructure with the right cabling to support the increased throughput. While older cabling (Category 5e/6) sufficed for Wi-Fi 5, Wi-Fi 6 and above demand higher-performance options. Industry standards recommend a minimum of two Category 6A connections per Wi-Fi access point (AP) and a minimum backbone uplink capacity of 25 Gbps.

Many experts recommend that four Category 6A cables or fiber optic cabling should be deployed to each AP to future-proof the network. It's important to consider that while APs typically get refreshed every 3-5 years, the underlying cabling infrastructure should last 10-15 years.

The increased labor, space, and material requirements of deploying four Category 6A cables per AP often make fiber optic cabling more attractive. However, most APs utilize Power over Ethernet (PoE), so using fiber requires an alternative power source, such as local AC power or a hybrid fiber-copper cable that combines fiber strands for data and copper strands for power delivery.

ADDITIONAL WIRELESS TECHNOLOGIES

Wi-Fi 6/6E and Wi-Fi 7 excel in supporting daily business needs, Wi-Fi is not the only wireless game in town. The electromagnetic spectrum offers a vast range of licensed and unlicensed wireless technologies, from cellular networks and satellites to short and long-range low-power applications.

5G cellular promises up to 10 Gbps speeds and lower latency than 4G.

Operating within licensed high-frequency spectrums up to about 47 GHz, 5G uses lower-band frequencies for lower-speed blanket coverage across large areas and higher-band frequencies to deliver enhanced throughput and ultra-low latency. However, higher-band frequencies have poor propagation, which limits the range.

With a growing number of connections relying on high-speed, low-latency connectivity, 5G requires a network of more closely spaced small cell stations (like mini base stations) on poles and buildings. While small cells deployed on utility poles, streetlights, and the corners of buildings deliver broadband access and support emerging outdoor IoT/IIoT applications like connected cars, smart traffic systems, and other smart city applications, most enterprise cellular use happens indoors. Here, indoor small cell and distributed antenna systems (DAS) amplify and distribute a single base station's signal throughout a building, similar to Wi-Fi access points.

Many enterprise organizations must also support various low-speed wireless technologies for battery-powered IoT/IIoT devices. For example, long-

Wi-Fi Generation	Wi-Fi 5	Wi-Fi 6	Wi-Fi 6E	Wi-Fi 7
IEEE Standard	IEEE 802.11ac	IEEE 802.11ax	IEEE 802.11ax	IEEE 802.be
Frequency Band(s)	5 GHz	2.4, 5 GHz	2.4, 5, 6 GHz	2.4, 5, 6 GHz
Max Number of Spatial Streams	8	8	8	16
Max Data Rate per Stream	866 Mb/s	1.2 Gb/s	1.2 Gb/s	2.9 Gb/s
Max Aggregate Data Rate	6.93 Gb/s	9.61 Gb/s	9.61 Gb/s	46.1 Gb/s
Typical Throughput	1.3 Gb/s	5 Gb/s	5 Gb/s	18 Gb/s

range technologies like NB-IoT, Sigfox, LoRaWAN, and Wi-Fi HaLow operate at low frequencies for better building penetration and extended range (up to 40km). Short-range technologies like Bluetooth, Zigbee, Z-Wave, and RFID offer shorter range (up to 100 meters) for device-to-device communication and tracking within buildings (inventory, payments, access control, asset tracking). Some Wi-Fi APs integrate multiple wireless technologies to support both high-speed 802.11 Wi-Fi (laptops, tablets, smartphones) and low-speed IoT/IIoT sensors.

INCREASING ENTERPRISE DIGITALIZATION

Propelled by increasing digitalization, the connected enterprise market is estimated to grow from \$425.54 billion in 2023 to \$566.88 billion in 2024, reflecting a staggering CAGR of 33.2%. This growth is driven by the emergence of powerful technologies like the IoT/IIoT, advanced wireless solutions, and edge computing. These advancements also expand and extend enterprise Local Area Networks (LANs) to deliver services and connect a growing number of devices across diverse locations.

Today, many connected devices, from access control panels and surveillance cameras to wireless APs and LED lighting fixtures can be powered remotely over the network using Power over Ethernet (PoE) technology. This trend, combined with the sheer number of devices, is increasing the complexity of telecommunications rooms (TRs) and horizontal cabling infrastructure with more equipment, pathways, and cable runs. Additionally, the growing number of devices in more locations often means connecting devices like surveillance cameras, access control panels, and wireless access points

in remote locations like warehouses and parking garages. These spaces are frequently located beyond the traditional 100m reach limit of twisted-pair copper Ethernet cables as specified by ANSI/TIA-568 cabling standards for commercial buildings.

While fiber optic cables offer excellent reach to support devices located beyond 100m, the higher cost of fiber transmission often proves impractical for just a few outlying devices.

Additionally, fiber doesn't support PoE, necessitating separate power solutions. Even with existing local power, finding fiber-compatible LAN devices can be difficult. Media converters that require their own power source might then be needed to connect devices, adding cost and complexity. Deploying new TRs to reach remote devices is an option, but it's an expensive one. TRs require dedicated floor space, power, and cooling infrastructure.

SUPPORTING NEW TRENDS AND TECHNOLOGIES IN YOUR ENTERPRISE NETWORK

Moving compute resources to a private cloud, on premises or in an MTDC requires infrastructure capable of handling demanding cloud applications. New applications often necessitate significant processing power, leading to higher rack power densities and increased heat generation.

This can require more efficient cooling methods like aisle containment or liquid cooling. Enterprise data centers needing to support HPC environments must also be able to support high-density fiber cabling required for high-speed applications.

Maintaining efficiency and reliability

when migrating from public to private clouds is also necessary.

Integrated cabinet solutions, like the CPI ZetaFrame®, are ideal for meeting the next-generation computing demands of enterprise data centers. ZetaFrame seamlessly integrates with CPI's aisle containment systems, effectively managing power densities up to 25kW per rack. For even higher densities, ZetaFrame integrates with advanced direct-to-chip liquid cooling, enabling data centers to support high-compute, cloud-scale technologies like AI. ZetaFrame also incorporates CPI intelligent Switched Pro eConnect® PDUs, facilitating remote power monitoring and control. This allows enterprise data centers to remotely measure and cycle power for each piece of equipment connected to the PDU. With real-time monitoring of power parameters and usage, eConnect PDUs also empower enterprise data centers to optimize efficiency and make informed decisions regarding capacity planning and resource allocation.

CPI intelligent eConnect PDUs enable real-time monitoring of environmental conditions like cabinet-level temperature and humidity, sending alerts when critical thresholds are reached. This enables enterprise data centers to swiftly identify and address issues before they cause downtime. Furthermore, eConnect PDUs manage and power electronic access control, a feature crucial for preventing downtime caused by human error or malicious activity. Additionally, they log all access attempts (successful and failed), which is essential for healthcare and financial institutions complying with security regulations like HIPAA and PCI-DSS.

Enterprise organizations deploying

emerging edge computing technologies must also ensure adequate infrastructure and capacity (power, cooling, and connectivity), albeit on a smaller scale. CPI CUBE-iT® and ThinLine® II wall-mount cabinets are perfect for saving space and safeguarding edge equipment in various indoor environments.

Reliability is also paramount for edge data centers, especially those in harsh environments. Mission-critical equipment needs protection from extreme temperatures, dust, moisture, and vibrations. CPI's RMR® wall mounted, free-standing, or floor-mount environmental enclosures are ideal for safeguarding edge computing equipment in these demanding conditions. RMR® NEMA rated enclosures can be customized with thermal management, cable management, power, and electronic access control. Additionally, remote and unmanned edge data centers require robust remote monitoring and access control. CPI's intelligent eConnect PDUs provide these capabilities, ensuring enterprise data center managers can manage edge infrastructure effectively, even from afar.

High-throughput wireless technologies like Wi-Fi 6/6E/7 and 5G require careful planning to ensure optimal coverage.

A critical factor is choosing the right mounting solution for wireless Access Points (APs) for your environment. This ensures proper AP height and orientation while avoiding obstructions like soffits, ceiling tiles, and building systems. For instance, when suspended ceiling mounting isn't an option, CPI offers Oberon™ M-Frame™ Open-Ceiling mounts with various hanging options for open ceiling environments like

warehouses, factories, and gymnasiums. Oberon H-Plane™ Right-Angle Surface Mounts allow APs to be mounted on the wall in a horizontal orientation for optimum coverage.

Harsh environments like industrial spaces, labs, gyms, warehouses, and outdoor areas also require additional protection for APs. NEMA-rated enclosures, such as CPI Oberon Skybar™ environmental enclosures, safeguard APs from dust, water, and extreme temperatures. In outdoor spaces where wall or pole mounting isn't feasible, Oberon NetPoint™ free-standing weatherproof bollards provide an ideal solution for securing and protecting outdoor rated APs, antennas, and associated cabling.

Security is also crucial, especially in schools, hospitality, and healthcare settings. Wireless enclosures should prevent theft, vandalism, and unauthorized access. For healthcare facilities with suspended ceilings, infection control risk assessment (ICRA) procedure compliance is essential to avoid contaminant spread. CPI's Oberon Wi-Tile™ Ceiling Enclosure with a solid back box and cable entry plugs meets these requirements. In addition to protection, many enterprise spaces require a clean aesthetic. CPI Oberon wireless enclosures include recessed panels, matching flanges, and paintable covers, allowing them to blend seamlessly into ceilings or walls.

The increasing integration of digital technology across businesses demands more equipment and cabling within enterprise LANs. This can strain existing TRs designed initially for basic voice and data applications. These spaces must now prioritize organized connections,

equipment protection, and future growth to ensure high performance for expanding systems and devices. In addition, twisted-pair copper cabling and PoE have significantly improved over the past three decades to handle rising bandwidth and power demands. Category 6A cabling, supporting speeds up to 10 Gbps, is the recommended industry standard for enterprise LAN deployments. However, this cable boasts enhanced features that make it thicker with a larger diameter. Additionally, higher PoE levels transmitted through these cables can generate heat buildup within bundles, impacting performance.

Enterprise TRs and horizontal infrastructure need ample capacity within racks, robust cable management systems, and designated pathways. Maintaining proper cable bend radius and spacing between bundles is crucial. Solutions like CPI Universal Rack and Adjustable QuadraRack® offer the strength needed for heavier loads. Likewise, CPI Evolution® vertical and horizontal cable managers provide increased load ratings, support larger bend radii, and feature adjustable accessories. These features accommodate larger quantities of Category 6A cables while enabling seamless scalability for growing LANs. Zone cabling offers a strategic approach for managing many connected devices within enterprise LANs. This method utilizes intermediate connection points via patch panels housed in strategically placed CPI drop ceiling or wall-mount telecommunications and consolidation point enclosures. These enclosures, positioned closer to end devices, allow for shorter, more manageable cables. This setup facilitates faster moves, additions, and changes within the horizontal LAN infrastructure.

For businesses requiring reliable LAN connectivity beyond the traditional 100-meter Ethernet limit, housing telecommunications equipment in compact wall-mount or free-standing enclosures presents a cost-effective alternative to constructing an entirely new TR. CPI CUBE-iT and ThinLine II wall-mount cabinets serve as ideal mini-TRs for limited floor space while RMR NEMA-rated free-standing and wall-mount enclosures empower businesses to create mini-TRs that offer protection from dust and moisture in challenging environments like warehouses or parking garages.



SUMMARY OF ENTERPRISE NETWORK CHALLENGES

TREND	NETWORK IMPACT	OTHER CONSIDERATION	PRODUCT SOLUTION
Hybrid Cloud	Supporting HPC systems and higher rack power densities via advanced cooling. Managing high-density fiber optic cabling required for high-speed applications.	Optimizing reliability and efficiency with power monitoring and control, environmental monitoring, security, and compliance.	ZetaFrame Cabinet System with aisle containment or liquid cooling to manage higher rack power densities. Intelligent Switched Pro eConnect PDUs for advanced power monitoring and control with USB temperature and humidity sensors and RFID Electronic Lock Kit for reliability.
Edge Computing	Small, remote edge data centers located close to users and devices. Supporting high-density fiber optic cabling required for high-speed applications.	Ensuring reliability in harsh environments and remote monitoring and control. Limited access control.	Space-saving CUBE-it and ThinLine II wall-mount cabinets to house edge compute equipment. RMR free-standing and floor-mount environmental enclosures for harsh environments. eConnect PDUs with remote monitoring and electronic access control.
Advanced Wireless	Requires high-speed 10 Gigabit switches to support high- throughput Wi-Fi and 5G small cell or DAS. Recommend four Category 6A connections or fiber optic connections to wireless APs. Fiber-connected APs will need an alternative to PoE for power.	Maintaining proper AP height and orientation for optimal coverage. Protecting APs in harsh facilities and outdoor environments. Ensuring security, compliance, and aesthetics.	Oberon M-Frame Open-Ceiling mounts for open ceiling environments. Oberon H-Plane right-angle surface mounts to maintain horizontal orientation where ceiling mount isn't feasible. NEMA-rated Oberon Skybar environmental enclosures for harsh and outdoor environments. Oberon NetPoint free-standing bollards for outside deployments. Oberon Wi-Tile ceiling enclosures ensure ICRA compliance in healthcare settings and enhanced aesthetics.
Digitalization	Supporting more equipment and connections in TRs. Providing ample capacity in racks, cable managers, and pathways to support Category 6A and advanced PoE.	Zone cabling to ease moves, adds, and changes in horizontal spaces. Deploying mini-TRs to provide LAN connectivity to remote locations beyond 100m from TRs, including harsh environments like warehouses and parking garages.	CPI Universal Rack and Adjustable QuadraRack support heavier loads. Evolution cable managers accommodate large quantities of Category 6A cables with scalability. Telecommunications and consolidation point enclosures for zone cabling. Cube-IT, ThinLine, and RMR create mini-TRs in a variety of remote spaces.

The Deepfake dilemma

- HOW BUSINESS LEADERS CAN SAFEGUARD AGAINST AI-DRIVEN DECEPTION



Social media and online news platforms are filled with dynamic video and audio content designed to captivate audiences. But can we truly trust what we see and hear? Deepfake technology's quick development has made it harder to distinguish between fact and fiction, endangering companies, executives, and financial stability.

*By Kumar Vaibhav
Lead Senior Solution Architect
Cybersecurity at In2IT*

UNDERSTANDING DEEPPAKE TECHNOLOGY

Artificial Intelligence (AI) and deep learning algorithms, especially Generative Adversarial Networks (GANs) drive deepfake technology. These AI systems create hyper-realistic audio and video forgeries that convincingly mimic individuals' voices and facial expressions.

Originally designed to help in fields like entertainment and language localisation in movies, deepfakes are now a weapon used by scammers and cybercriminals.

The accessibility of deepfake software has expanded beyond skilled programmers. Digital content may now be altered by anyone with a computer and internet connection, making it more challenging to tell authentic content from fake. For companies and leaders that depend on digital communication to uphold credibility and trust, this increasing sophistication has significant ramifications.

The rising threat to business executives Deepfake-driven fraud primarily targets corporate executives. In one concerning instance, fraudsters pretended to be the CEO and used AI-generated audio to tell a financial officer to transfer millions of dollars into fictitious accounts. The employee obeyed without hesitation because the artificial voice seemed so realistic. The enormous financial hazards connected to deepfake technology are highlighted by this instance.

The use of deepfake films to propagate false information about corporate executives is another issue that is becoming increasingly concerning. Within hours, a modified video clip showing a contentious executive's remarks can undermine consumer trust, cause stock price volatility, and harm a company's brand. These hazards are increased by social media's viral nature, forcing businesses to take preventative action.

POLITICAL AND ECONOMIC IMPLICATIONS

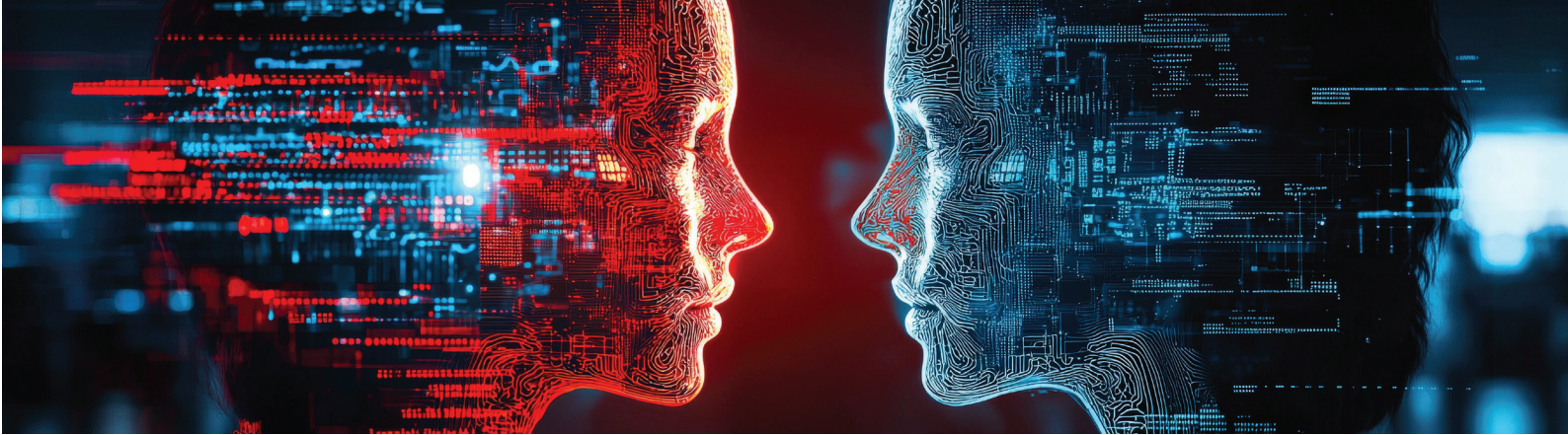
Beyond corporate threats, deepfake technology has far-reaching consequences for national security and political stability. Fabricated speeches by world leaders can incite geopolitical tensions, manipulate election outcomes, and fuel misinformation campaigns. The ability to create plausible but wholly untrue narratives poses a risky challenge for both governments and corporations in a time when market action is driven by public perception.

DEFENDING AGAINST THE DEEPPAKE THREAT

As deepfake technology develops, companies can reduce risks by implementing strategic countermeasures. Here's how:

1. Making authentication procedures stronger

Deepfake-driven impersonation attempts can be thwarted by implementing Multi-Factor Authentication (MFA) and biometric



verification. Executive orders and financial transactions should also need secondary verification, including real-time video authentication or encrypted digital signatures.

2. Investing in AI detection tools

AI-driven detection methods are developing at the same rate as deepfake technologies. Forensic tools that evaluate digital fingerprints and discrepancies in audio and video footage should be used by businesses. Additionally, blockchain-based authentication can confirm that important business communications are authentic.

3. Awareness and education of employees

In cybersecurity, people continue to be the weakest link. Employees should receive regular training on identifying deepfake risks, confirming odd requests, and adhering to stringent authentication procedures.

It is crucial to create a culture of mistrust regarding unexpected digital communications.

4. Collaborating with cybersecurity professionals

Because AI-generated threats are evolving quickly, companies should work with cybersecurity companies specialising in deepfake detection. Professional partners can execute security frameworks, offer real-time threat intelligence, and guarantee that businesses remain ahead of new threats.

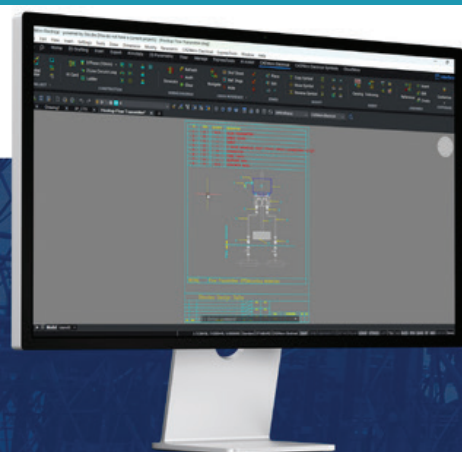
5. Putting in place stringent verification procedures

To stop illegal transactions, executives and financial teams need to implement strict internal controls. Before being carried out, any unique or valuable request should be independently confirmed through several channels, mainly if it is delivered by voice or video.

THE WAY FORWARD: ALERTNESS IN THE AGE OF DEEPPFAKE

Businesses need to continue being proactive rather than reactive as deepfake technology advances. To create regulations, invest in AI-powered security solutions, and promote digital literacy, governments, tech companies, and business executives must collaborate.

In the end, awareness, verification, and the ongoing development of defensive tactics are crucial for reducing deepfake dangers. Businesses can defend themselves against one of the most difficult cybersecurity issues of the digital era by adopting a multi-layered security approach and remaining informed. **wn**



HEXAGON

CHEMPUTE SOFTWARE

CADWorx® Electrical & Instrumentation Design Suite

Increases efficiency in your electrical design processes with full-featured 3D modeling
Cutting-edge tools for the oil and gas industry, driving projects in energy, pharmaceuticals, and manufacturing!

Tel: +27 11 803 6559 || sales@chempute.com || www.chempute.com

South Africa's Next Cybersecurity Frontier



AI-powered agents are rapidly transforming how South African businesses operate, from chatbots managing customer inquiries to automated systems processing financial transactions.

*By Boland Lithebe
Security lead for Accenture, Africa*

While these AI-driven assistants increase efficiency and reduce operational costs, they also present a new, and often underestimated, cybersecurity challenge: identity management. Without proper oversight, AI agents can be compromised, leading to data breaches, fraud, and reputational damage.

As AI adoption accelerates in South Africa, companies must ask themselves: Who is securing these AI agents? Can they be manipulated? Are our existing security frameworks robust enough to protect against AI-driven threats? These are no longer theoretical concerns; they are pressing issues that demand immediate action.

AI agents function autonomously, making decisions based on vast amounts of data. While they enhance productivity, they also introduce a new attack surface for cybercriminals. An unprotected AI agent is like an employee with unrestricted system access but no accountability. If compromised, an AI agent could be tricked into leaking sensitive data, approving fraudulent transactions, or even shutting down critical business operations.

This issue is particularly concerning for South Africa's financial and telecommunications sectors, where AI is increasingly being used for risk assessment, fraud detection, and automated decision-making. If an AI-driven fraud detection system is hacked, it could be manipulated to ignore illicit

transactions or flag legitimate ones, disrupting businesses and shaking consumer trust.

The traditional cybersecurity approach focuses on securing human users, with firewalls, passwords, and multi-factor authentication. But how do we verify the authenticity and security of AI agents? South African businesses must urgently rethink identity management strategies to include AI entities.

Just as human users need authentication, AI agents must have unique, trackable digital identities. Implementing AI-specific authentication protocols ensures that only authorised AI systems interact with critical business infrastructure.

Businesses should implement role-based access control (RBAC) for AI agents. Not all AI systems should have the same level of access. For instance, a customer service chatbot should not have the same data access as an AI fraud detection system.

And companies must continuously monitor AI activity using real-time tracking and anomaly detection tools. If an AI agent behaves unpredictably, automated security measures should flag and isolate it before any damage is done.

South Africa needs to develop policies that regulate AI security and identity management. AI agents should be subject to the same compliance requirements as human employees overseeing sensitive data. The government, in collaboration



with the private sector, should introduce guidelines to ensure AI security best practices are followed.

South African businesses cannot afford to be complacent. As AI adoption grows, so do the risks. Cybercriminals are already exploring ways to exploit AI vulnerabilities, and businesses that fail to secure AI agents will face costly consequences. Data breaches, financial losses, and regulatory penalties are just the beginning, the long-term reputational damage could be irreparable.

Moreover, failing to secure AI systems could deter foreign investment in South African businesses, as international partners may hesitate to engage with companies lacking robust cybersecurity protocols.

AI is revolutionising South African business, but security must keep pace with innovation. Business leaders

must take immediate steps to fortify AI security strategies.

Companies should conduct a comprehensive AI security audit to identify and mitigate vulnerabilities in their AI-driven systems.

CISOs and IT security teams must prioritise AI agent identity management and integrate AI-specific security measures into broader cybersecurity frameworks.

Policymakers should develop AI security regulations that provide clear guidelines on protecting AI-driven operations.

AI has the potential to drive economic growth and efficiency in South Africa, but only if it is secure. By taking a proactive approach, South African businesses can ensure that AI remains a force for good, rather than a ticking time bomb. **wn**



measure with confidence

COMTEST  ONLINE

Stay Ahead of Unplanned Downtime

Fluke ii500, ii905 and ii915 Acoustic Imagers

FLUKE®



[Learn More](#)

Your Employees could be the reason you face millions in POPIA fines - or worse!



If you think external hackers are your biggest data privacy threat, think again. The most dangerous risk may be sitting right across the office from you. From the boardroom to the breakroom, employee negligence is the number 1 cause of data breaches and compliance failures under POPIA (the Protection of Personal Information Act).

*By: Jodi Poswelleltski
Fairbridges Wertheim Becker*

And if you're a member of the South African Institute of Electrical Engineers (SAIEE), you're not off the hook - engineers handle massive amounts of personal information too, whether it's client's personal information, subcontractor details, or even sensitive site access credentials.

The Information Regulator is stepping up with enforcement. That means the next time one of your employees slips up - by sharing a password on a sticky note, forwarding unencrypted files, or storing confidential client personal information on a public server - you could be looking at millions in fines. In extreme cases, there's even potential jail time for those at the helm.

WHY SAIEE MEMBERS CAN'T AFFORD COMPLACENCY

"We're engineers, not data processors!" That excuse won't shield you when POPIA violations come to light. The engineering community relies heavily on digital tools and data-driven processes, making you especially vulnerable to breaches. A single oversight can lead to: **Data Breaches:** Exposing client or employee personal information, leading to massive liability.

Reputational Damage: Losing the trust of clients and partners who can't risk associating with a company under regulatory scrutiny.

Financial Fallout: Fines of up to ZAR 10 million can crush a small or mid-sized engineering consultancy.

Legal Headaches: Civil suits, criminal penalties, and a protracted investigation by the Information Regulator.

THE NEGLIGENCE HOTSPOTS

Password Problems—Passwords on Post-it notes, "123456" for critical systems, or employees sharing logins to "speed up" processes are prime examples of data security nightmares.

Improper Data Handling - Engineers often swap large files with client or proprietary details. Without encryption or secure channels, those files can be intercepted or mishandled.

Undertrained Staff - If your team isn't clear on what POPIA demands, it's only a matter of time before well-intentioned employees make a catastrophic mistake.

YOUR GAME PLAN FOR SURVIVAL

Staying safe isn't rocket science - it's about awareness, training, and strict protocols. Here's how to shore up your defences:

Regular, Targeted Training - If your employees aren't being reminded and re-trained on data protection, complacency can creep in. Make POPIA training an ongoing priority.

Robust Data Policies - Draft clear, enforceable policies covering data collection, processing, and sharing. Vague guidelines only lead to guesswork - and trouble.

Information Officer Appointment - POPIA mandates it, but many businesses treat it as a formality. Your Information Officer needs real authority to drive changes and crack down on non-compliance.

Continuous Audits - Regularly review your processes, perform risk assessments, obtain remediation reports and recommendations for mitigating risk, and document everything. These

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

Keitumetse Khutsoane

CANDIDATE ATTORNEY

Phone: +27 11 268-0250
Mobile: +27 76 268 0250
Email: keitumetse.k@fwblaw.co.za



steps prove you're serious about compliance if (and when) the Regulator comes knocking.

Zero Tolerance—Make it crystal clear that any breach or negligent data handling triggers serious repercussions. Once employees understand the stakes, they're far less likely to cut corners.

A single employee mistake can destroy your entire operation. POPIA fines, reputational ruin, and even criminal charges for leadership could become your new normal—unless you take action now.

As a partner at Fairbridges Wertheim Becker, Jodi Poswellewski has helped numerous engineering and technical firms navigate these choppy waters.

Her team provides comprehensive POPIA compliance, risk assessments and remediation reports, and targeted training to fortify your business against internal and external threats.

Tailored Workshops: Ongoing employee training that addresses the unique data handling challenges in engineering and technical fields.

Policy Development: Clear, actionable policies ensure every worker understands data privacy's do's and don'ts.

Risk & Compliance Roadmaps: Step-by-step frameworks to help you identify vulnerabilities and implement lasting solutions. **wn**



Leadership Conference

28 May 2025 // 08:30 AM – 2 PM

About the Conference

Effective business leadership goes beyond management. It involves creating a compelling vision that inspires teams to pursue strategic organisational goals. Successful leaders recognise individual talents and foster collaboration for overall success.

Join the SAIEE KwaZulu-Natal Centre for a one-day conference to enhance your leadership skills. Learn from industry experts, share insights and discover strategies to boost your leadership and organisational performance.



Venue:

Investec Auditorium
5 Richefond Circle
Ridgeside Office Park
Umhlanga



Entrance fee:

SAIEE Members: Free
Non-Members: R500

[RSVP by 23 May 2025](#)

THE AIM OF THE CONFERENCE

Skills Development

Keynotes focused on building leadership abilities, such as decision-making, communication, conflict resolution, and team management.

Inspiration

Motivating attendees through success stories, thought-provoking discussions, and presentations from accomplished leaders.

Collaboration

Encouraging the exchange of ideas and best practices among diverse groups to foster a culture of collaboration and innovation.

Networking

Creating opportunities for participants to connect with other like-minded professionals, mentors, and industry leaders.

Innovation & Strategy

Exploring new leadership trends, tools, and strategies for addressing contemporary challenges in the workplace or community.

The Goal

To equip attendees with the knowledge and inspiration to lead with greater confidence, impact, and effectiveness.

Scan the QR code and RSVP by 23 May 2025 or [click here](#) to register.
Limited seats available, book now to avoid disappointment.
For queries, please email kznc@saiee.org.za



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 <u>before</u> 31 March 2025		Annual Subscriptions paid <u>after</u> 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!

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 KAHN
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	pessection@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

MAY 2025

CALENDAR

08/05/2025	Understanding long-duration storage
09/05/2025	Road to Registration for Engineering Candidates
13/05/2025	Cable Jointing, Termination and Testing
15/05/2025	Writing Good Technical Specification
15/05/2025	Energy in Southern Africa
19/05/2025	New Engineering & Construction Contract
20/05/2025	Planning Feasibility Studies in IR 4.0: An Engineer's Perspective
20/05/2025	Incident Investigation and Management (Root Cause Analysis)
22/05/2025	LV/MV/HV Switch gear Operation, Safety, Maintenance and Management
27/05/2025	Lightning Protection of Structures, Low Voltage and Signal Systems
28/05/2025	KZN Centre Leadership Conference
29/05/2025	Analysis of Different Winding Configurations

JUNE 2025

03/06/2025	An introduction of Artificial Intelligence
10/06/2025	Photovoltaic Solar Systems
11/06/2025	Photovoltaic Solar Systems - EAST LONDON
12/06/2025	SANS 10142-1 Edition 3 2020
13/06/2025	Road to Registration for Engineering Candidates
18/06/2025	Fundamentals of Developing Renewable Energy Plants
19/06/2025	Finance Essentials for Engineers
25/06/2025	Project Management for Engineers



SAIEE Sections, Chapter & Centre Events

SAIEE Academy Online Training

SAIEE Academy Classroom Training

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

ABERDARE

— A MEMBER OF HENG TONG GROUP —
ENLIGHTENING THE FUTURE



HIGH VOLTAGE CABLES **(UP TO 132kV)**

SANS/IEC 60840 & NRS 077



1 Corobrik Street, Meadowdale Gauteng
PO Box 1679, Edenvale, Gauteng, 1610, South Africa
Tel +27 (0) 11 396 8000 | Fax +27 (0) 11 396 8013
info@aberdare.co.za | www.aberdare.co.za