

wattnow

THE OFFICIAL PUBLICATION OF THE SOUTH AFRICAN INSTITUTE OF ELECTRICAL ENGINEERS



CYBERSECURITY

4	SAIEE President's Message
6	SAIEE 2026 Membership fees
8	Industry News
28	Student News
32	Tertiary Education Facilities in South Africa
34	Securing the Unseen in 2025 <i>Global Trends And Personal Insights In Operational Technology Cyber Defense</i>
40	Biometrics in an AI-Driven Future <i>How Safe is "Something you are"?</i>
44	Implementing a Novel Cybersecurity Algorithm for Smart Grid SCADA System <i>Cybersecurity preparedness for organisations</i>
48	Strengthening Cybersecurity in Power Utilities <i>The Role of Directory Services in the IIoT Arena</i>
56	Trusted Execution Environments <i>A Step Towards The Zero-Trust Paradigm?</i>
58	Opinion
70	SAIEE Council
72	SAIEE Centres
73	SAIEE Events Calendar



Dear **wattnow** Reader,

In the first half of 2025, South Africa faced nearly 370,000 data breaches, reflecting a 23% decrease from the previous quarter. Common attack vectors include third-party compromises and phishing, while AI-driven attacks are on the rise. The average cost of a breach fell to R44.2 million, thanks to AI advancements. This highlights the urgent need for cybersecurity awareness.

The SAIEE Cybersecurity Chapter submitted five feature articles:

"Securing the unseen in 2025" by Chairman Matthew Taljaard ([Page 34](#)) - Discusses operational technology cyber defence trends.

"Biometrics in an AI-Driven Future" by Meenal Vala ([Page 40](#)) - Explores the importance of authentication in digital security.

"Implementing a Novel Cybersecurity Algorithm for Smart Grid SCADA System" by Kholofelo H. Halefose ([Page 44](#)) - Examines cybersecurity preparedness during the shift to remote work.

"Strengthening Cybersecurity in Power Utilities" by Kgomoetso Manyapetsa ([Page 48](#)) - Highlights the cybersecurity risks associated with IIoT in power utilities.

"Trusted Execution Environments – a step towards the Zero-trust Paradigm" by Dr Daniel Ramotsoela ([Page 56](#)) - Discusses advancements in technology and their impact on the fourth industrial revolution.

The November issue focuses on Transportation, with article submissions due by October 17. Please send your article to minx@saiee.org.za.

Herewith the October 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 EXECUTIVES

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

Preparing the 2026 SAIEE budget was a challenging balancing act between ensuring the financial sustainability of the SAIEE, providing our members with the benefits they signed up for, and maintaining membership fees at a reasonable level.



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

Strengthening Collaborations and Enhancing Member Value

Part of the research undertaken to determine a reasonable membership fee involved examining the practices of other Voluntary Associations. We also had to ensure that we limit access to funds from the Institute's investments.

However, after many hours of hard work, the Office Bearers and Finance Committee had compiled a budget that we were confident of proposing at the last council meeting.

The council was presented with three options: the low road, the middle road, and the high road. The budgeting process that has been undertaken now enables us to provide adequate notice to our members regarding the fees for 2026.

[Find the 2026 SAIEE Membership fees on page 6.](#)

In line with its commitment to staying relevant by fostering the personal growth of its members, the South African Institute of Electrical Engineers (SAIEE) has been making notable strides in collaborating with other like-minded institutions. In keeping with this spirit of collaboration,

SAIEE signed a Memorandum of Understanding (MoU) with the South African Institute of Architects (SAIA). The signing ceremony took place on August 13, 2025, at SAIEE House. SAIEE hosted the SAIA President, Claire McCusker, for the signing ceremony in the council chamber. In the discussion that followed, there was agreement that the respective CEOs would now take the following steps to discuss areas of mutual collaboration, which will include sharing training courses with members of both institutions.

During the month, we had also entered into an MOU with the Institute of Information Technology Professionals South Africa (IITPSA). Like other MOUs signed and those to be signed, these collaborations will enhance the offerings of the SAIEE Training Academy and provide a greater choice of courses for members of both institutions. It is my goal that voluntary associations build on the strengths of each institution rather than competing with one another.

It is essential that, as the leadership of the SAIEE, comprising the Office

Bearers, Governance Committee, Council, and various committees, we periodically review our strategic and guiding documents. Based on audit recommendations from the previous fiscal year, we undertook a review of the bylaws to ensure they remain relevant and practical. This is still a work in progress that will be concluded upon deliberation and approval by the council.

In terms of organisation design, it is said that structure must follow strategy. As we explore the relevance of the SAIEE and assess its risks, we are reviewing the current reporting relationships within the Institute's organisational chart. The intention is to enhance the efficiency of Head Office outputs under the leadership of the Chief Executive Officer while also mitigating any potential risks associated with the current structure. We are aware of the cost implications of the organogram changes, and these will be a consideration when proposing the structure to the council.

The highlight for September is the Bernard Price Memorial Lecture. In terms of the significance of the BP lecture, it

is essential to understand the history behind this annual event. Dr Bernard Price was born in England in 1887. He came to South Africa in 1909 to take up his appointment as Chief Engineer of the Victoria Falls and Transvaal Power Company Limited (VFP). Coincidentally, this was the year the SAIEE was formed. Dr Price was appointed as President of the SAIEE in 1915, 110 years ago. In 1940, Dr Bernard Price was awarded Honorary Life Membership of SAIEE. The Lecture is named in memory of Dr Bernard Price. This year, I decided to invite the Chairman of NERSA, Thembanani Bukula, to deliver a lecture on the envisaged journey towards a competitive electricity trading market. You can read the news piece on page (?) and watch the recording [here](#).

As we welcome the arrival of spring, I invite our student and younger members to share their feedback on how we can enhance the value of our offerings. Your input is crucial for ensuring that we stay relevant. Please send your suggestions to Head Office or your local Centre, and we will consider all proposals. Thank you! **wn**



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

MEMBERSHIP FEES EFFECTIVE 1 DECEMBER 2025

The Council meeting held on 5 September 2025 approved subscription & entrance fees as from 01 December 2025 as per schedule indicated below.

PLEASE NOTE: In terms of Bylaw 3.2 annual subscriptions are due on 1st December 2025

MEMBERSHIP FEES CAN BE PAID IN MONTHLY RECURRING PAYMENTS

Council agreed to a discount for fees paid before 31 March 2026. Members are therefore encouraged to pay promptly to minimize increase impact.

Grade of Membership	Annual Subscriptions paid <u>before</u> 31 March 2026		Annual Subscriptions paid <u>after</u> 31 March 2026		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	1 947	1 693	2 336	2 031	2 336	2 031
Associate	1 947	1 693	2 336	2 031	2 336	2 031
Member	2 152	1 871	2 582	2 245	2 582	2 245
after 6 years	2 514	2 186	3 017	2 623	3 017	2 623
after 10 years	2 631	2 288	3 157	2 746	3 157	2 746
Senior Member	2 631	2 288	3 157	2 746	3 157	2 746
after 6yrs/age 40	2 851	2 480	3 422	2 975	3 422	2 975
Fellow	2 851	2 480	3 422	2 975	3 422	2 975
Retired Member (By-law B3.7.1)	1 209	1 052	1 451	1 262	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 R3532.00 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 2026 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 2026.

2026 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 74th Bernard Price Memorial Lecture



Leanetse Matutoane, SAIEE CEO



From left: Pascal Motsoasele (SAIEE Immediate Past President), Thembani Bukula (74th BP Lecturer) and Prof Thokozani Majozi (Dean of the Faculty & Built Environment, Wits University).

SAIEE hosted its 74th Bernard Price Memorial Lecture at Wits University on the 18th of September. This year, our esteemed speaker, Mr Thembani Bukula, Chairperson of the National Energy Regulator of South Africa (NERSA), gave a talk on “The Envisaged Journey Towards a Competitive Electricity Trading Market - Policy Pathways, Challenges, and Prospects”.



Mr Bukula holds a BSc in Electrical Engineering from the University of Natal, a Post Graduate Diploma in Engineering Business Management from Warwick University, and an MSc in Mathematics, Science, and Technology Education from UNISA. He has been a registered Professional Engineer (Pr Eng) since 1997 and obtained his Government Certificate of Competency for Factories (GCC) in 1998. With over 30 years of experience, he is the CEO of PowerX, a licensed electricity trader in South Africa.

In his talk, Mr Bukula discussed the restructuring of South Africa's electricity sector through the unbundling of Eskom and the integration of Independent Power Producers (IPPs), which aims to create



a competitive electricity trading market. This transition offers opportunities for efficiency and investment but also poses challenges in governance and market stability.

A key policy priority is to establish a regulatory framework that promotes open access and transparent rules, while safeguarding vulnerable consumers and preventing the rise of dominant players.

Success will rely on striking a balance between sector development, innovation, and competition, supported by effective governance and regulatory consistency across various policy areas.

[Click here](#) to watch the recording. **wn**



From left: Andries Mthethwa (SAIEE Past President) and Thembani Bukula (74th BP Lecturer).



From left: Thembani Bukula (74th BP Lecturer) and Leanetse Matutoane (SAIEE CEO).



From left: Ian McKehnie, Andries Mthethwa and Dr Angus Hay - all SAIEE Past Presidents.



SAIEE Rotating Machines Section - Site visit to LHM Fan Division



On 28 August 2025, the Rotating Machines Section of the South African Institute of Electrical Engineers (SAIEE) successfully hosted a technical site visit to the LHM Fan Division.



The event drew an impressive turnout of 26 professionals, underscoring the strong interest and commitment within our industry towards advancing rotating machine technology in South Africa.

The LHM Fan Division welcomed our group with outstanding professionalism and hospitality. The visit began with a series of insightful presentations, where the LHM team shared their technical expertise, innovative approaches, and market perspectives. These presentations provided valuable context on the company's capabilities and their contribution to the broader engineering sector.

Following the presentations, participants were taken on a comprehensive tour of the facility. The manufacturing process, from design to assembly, was showcased with great attention to detail. The group was particularly impressed by the precision, quality standards, and innovation evident in LHM's operations. It was clear that their team takes great pride in ensuring excellence at every stage of the production process.

Beyond the technical aspects, the visit created an excellent platform for knowledge exchange and professional networking.

It also demonstrated the role of the SAIEE Rotating Machines Section in creating opportunities for members to engage directly with leading industry players, strengthening ties between engineers, manufacturers, and other stakeholders.

We extend our sincere appreciation to the LHM Fan Division for their generosity, professionalism, and effort in hosting our group. Their commitment to engaging with the engineering community is commendable and sets a strong example of industry collaboration.

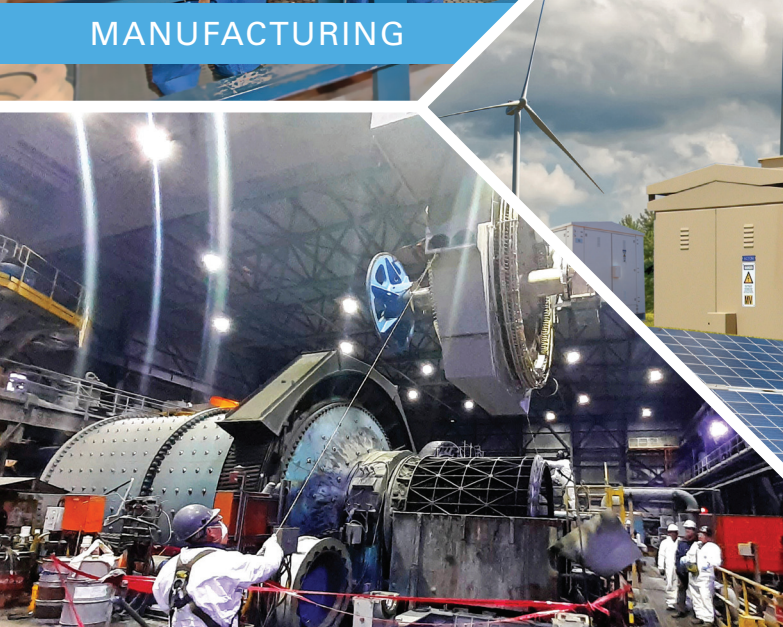
The success of this visit reinforces our mission to bring valuable experiences and learning opportunities to our members. We look forward to building on this momentum with future events that continue to support the growth and development of the rotating machines discipline in South Africa. **wn**



MANUFACTURING



PROJECTS



SERVICE AND REPAIRS



MAINTENANCE

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

Power Generation
Transmission
Distribution
Utilities

Healthcare
Industrial Processing
Mining
Oil & Gas

Paper & Pulp
Petro-chemical
Rail Transport
Signalling

Renewable Energy
Sugar
Textile
Water & Sanitation

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

Your one-stop global energy solutions partner

ACTOM

SINCE 1903

Africa's leading digital innovation agency warns

- FUTURE OF AI IN SA WILL DEFINE WHO HOLDS POWER



“Artificial intelligence has crossed a critical threshold. For the first time in history, our tools are learning to improve themselves. This moment marks the dawn of what experts call superintelligence, the machine learning capabilities that could one day surpass human performance in nearly every domain” comments Daniel Novitzkas, Chairman of Specno, Africa’s leading digital innovation agency. According to Novitzkas, the question is no longer if this future will arrive, but what form it will take, and who it will serve.

“If superintelligence is centralised in the hands of governments and global corporations, human agency will shrink. We risk becoming passive consumers in a system designed for profit and control. But if we build AI as personal superintelligence - or PSI - we can unlock a future that multiplies human potential rather than diminish it,” argues Novitzkas.

Centralised AI, he explains, risks entrenching monopolies of information, wealth, and power. The alternative - personal superintelligence - offers a decentralised system that belongs to individuals and is tailored to their unique goals, values, and strengths. Rather than dissolving individuality in the pursuit of efficiency, PSI would magnify diversity, giving people the tools to learn, create, and innovate on their own terms.

“The potential applications of PSI are vast. A student struggling with dyslexia could learn through an AI tutor designed precisely for their cognitive style. A farmer in Limpopo could receive real-time, personalised guidance on soil health and weather conditions.

A young musician could collaborate with an AI attuned to their creative rhythm, while a personalised health coach could continuously monitor biometrics, predicting and preventing illness years before symptoms appear” states Novitzkas.

“Personal superintelligence isn’t about replacing people - it’s about augmenting

them,” he explains. “The student still learns, the entrepreneur still builds, the farmer still farms, but each with supercharged capacity.”

For Africa, the implications are profound. Just as mobile phones allowed the continent to leapfrog landline infrastructure, PSI could democratise access to world-class expertise, placing tutors, doctors, and business advisors directly into the hands of millions.

Communities once excluded from global opportunities could find themselves at the cutting edge of human capability. Yet the danger is equally clear: if personal superintelligence is ignored, the future will default to centralisation, calcifying inequality and entrenching dominance in the hands of a few.

“This debate can’t stay confined to Silicon Valley,” Novitzkas warns. “The decisions we make now, about whether intelligence is centralised or personal, will shape the next century of human life. Africa has the chance not just to catch up, but to leap ahead.”

Specno is urging policymakers, innovators, and industry leaders to recognise PSI as humanity’s next great leap forward.

Without intentional design and distributed frameworks, superintelligence risks becoming humanity’s greatest divide instead of its greatest breakthrough. **Wn**

MIDTRONICS' GROUND-BREAKING MVT BATTERY TESTER POWERED BY MDX-AI

Midtronics, a global leader in battery management technology, represented locally by COMTEST, offers the proven MVT handheld battery tester. This revolutionary tool, powered by MDX-AI, is set to redefine the standards of battery diagnostics and testing in the automotive industry.

The MVT battery tester is designed to deliver unparalleled accuracy and efficiency in battery diagnostics, making it an essential tool for automotive technicians and quick-service centres. This innovative product introduces a new era in handheld battery testing, showcasing capabilities previously thought to be unattainable.

KEY FEATURES OF THE MVT BATTERY TESTER:

- Accurate Diagnosis of Discharged Batteries in-vehicle, eliminating the need for charging.

- Instant Test Results with no user input required in most quick lane testing scenarios.
- Accurate Battery Diagnosis when the Cold Cranking Amps (CCA) rating is not visible.
- Reliable Battery Diagnosis in the presence of vehicle system noise interruptions.

Powered by MDX-AI, the MVT delivers lightning-fast battery testing while maintaining professional accuracy, ensuring that automotive professionals can efficiently diagnose and address battery issues with confidence and precision.

In addition to its ground-breaking diagnostic capabilities, the MVT features a range of user-friendly attributes, including:

- An Intuitive User Interface for straightforward operation.
- Over-the-air data transmission

and Updateability for continuous improvement.

- Email Test Results for seamless communication and record-keeping.
- An Optional Integrated Printer for convenient hard copy results.

Will Sampson, President of Midtronics, said, "The MVT enables automotive industry technicians and service centres to accurately diagnose batteries faster than ever before, improving customer satisfaction and streamlining operations. The MVT powered by MDX-AI is truly unique!"

For more information on MIDTRONICS MVT Battery Tester powered by MDX-AI, a ground-breaking tool, and to explore its features in detail, contact COMTEST on sales@comtest.co.za or www.comtest.co.za **wn**



Like nothing else.

MVT

Powered by MDX-AI

MIDTRONICS

SAIEE Balance

- 8 KM LAUNCH HIKE MARKS THE START OF CENTRE'S WELLNESS PROGRAMME



June 2025 saw the SAIEE Central Gauteng Centre (CGC) formally launched its wellness initiative, SAIEE Balance, with an 8-km hike at the Klipriviersberg Nature Reserve. The session brought together more than 60 participants, including CGC members and invited professionals, with structured warm-up and recovery guidance provided by Virgin Active fitness coaches. The launch marks the beginning of a broader and more structured commitment by the Centre to prioritise health and well-being as part of a sustainable professional culture in engineering.

SAIEE Balance was established as part of CGC's 2025/26 strategic programme under the theme "Disrupt. Evolve. Sustain." The initiative is built on the understanding that high-performance engineering is not only a function of technical expertise and leadership, but also of physical resilience, mental clarity, and long-term well-being.

The programme will operate year-round and is designed to provide SAIEE members with access to structured wellness opportunities, including physical activities, mobility training, and education around recovery, mental health, and performance sustainability.

In partnership with Virgin Active, SAIEE Balance will roll out a series of member-focused offerings, including:

- Quarterly hikes hosted at established nature reserves across Gauteng
- Fitness and recovery workshops facilitated by certified coaches
- Exclusive gym membership packages available to SAIEE members and their families

- Targeted wellness events addressing stress management, fatigue, nutrition, and related focus areas

The programme has been developed to complement CGC's leadership development, student outreach, and professional advancement initiatives, reinforcing the Centre's commitment to building a well-rounded, future-ready engineering community.

Klipriviersberg Nature Reserve was selected for the launch due to its accessibility, diverse terrain, and ability to accommodate groups of varying fitness levels. The 8 km route included moderate inclines, water features, and shaded paths, providing a fitting environment for the Centre's first formal group hike.

The morning programme began with a structured warm-up session facilitated by Virgin Active trainers. It concluded with guided stretching and mobility techniques, ensuring participants had proper recovery.



The event marked the first in a planned series of physical wellness activities designed to be inclusive, professionally managed, and well-integrated into the Centre's calendar.

Planning is already underway for the second hike in the Recharge Circuit series, scheduled for the third quarter of 2025. Additional wellness-focused events are being scoped in partnership with Virgin Active and other collaborators.

These will include in-gym sessions, workshops, and direct-to-member wellness resources to support long-term behaviour change and healthier professional habits.

The Centre is also working to finalise discounted gym membership offers, which will be made available to active SAIEE members and extendable to partners or immediate family.

Further details on these benefits will be communicated via email and official SAIEE channels in due course.



HOW TO GET INVOLVED

Members interested in participating in future SAIEE Balance activities or accessing wellness benefits are encouraged to express interest via email: cgc@saiee.org.za

wn

COMTEST Wows Channel Partners



*Barend Niemand
COMTEST CEO Welcoming Channel Partners.*



*Legacy Partner Award
- TYCOM.*



*Best Overall Performing Channel Partner
- Bolt and Engineering.*

Spotlights, rock anthems, and a packed house at the Barnyard Theatre – that’s how COMTEST, together with FLUKE, set the stage for an unforgettable afternoon as they welcomed over 80 Channel Partners to their annual celebration of excellence at The Emperor’s Palace, Gauteng.

This wasn’t your typical corporate meeting. The Annual Gathering had one goal: to celebrate COMTEST’s incredible stakeholders, share the latest product knowledge, and recognise excellence—delivered with plenty of energy, excitement, and entertainment!

Barend Niemand, CEO of COMTEST Group, shared how the company is embracing change and reinventing itself to become a South African market leader. “Our mission is clear,” he said. “We’re all about service excellence—from customer support to warehousing, the accounts team, and ultimately, our amazing sales crew.”

Barend emphasised that teamwork and high ethical standards are the secret ingredients to achieving these goals. “When we work together and stay true to our values, everyone wins—customers, suppliers, employees, and shareholders alike.”

And the results speak for themselves! Since 2022, COMTEST has been smashing records, with projections

for 2025 set to outpace SA GDP once again. Barend gave a special shoutout to Brolin Moonsamy (Fluke South Africa) and Kristo Engelbrecht (Fluke Africa) for their ongoing support.

Looking even further ahead to 2026, COMTEST plans to focus on business partners who share their vision—partners who see COMTEST as a trusted ally and want to make a real impact in their own markets while growing together. These are the partners who go the extra mile for end-users and embrace COMTEST’s “Go-to-Market” model.

Guests also got a peek at Fluke’s latest technologies, including the 2052/2062 Cable Finders, the Fluke iSee Mobile Thermal Camera, the SB140 Sound Beacon for the Motor & Aviation Industries, and the 729 PRO Pressure Calibrator—just a few highlights from a line-up packed with innovation.

AWARDS MADE TO CHANNEL PARTNERS:
Legacy Partner Award - Tycom
Best New Channel Partner - Top Dog Tool Shop



*Extra Mile Award
- North West - APPLECON*



*Extra Mile Award Limpopo
- Giant Marketing.*



*Extra Mile Award Vaal Triangle
- Corel Instrumentation & Controls.*

Best Electrical Wholesaler - Adendorff Machinery Mart
Best Overall Performing Channel Partner - Bolt And Engineering

BEST PERFORMING CHANNEL REGIONAL PARTNER

North West - Voltex Rustenburg
Mpumalanga - Bolt And Engineering
Gauteng - Communica
Vaal Triangle - Corel Instrumentation & Controls
Kwazulu-Natal - Magnet Electrical Supplies
Limpopo - Jpc Wholesaler
Western Cape - L&D Electrical

THE EXTRA MILE AWARD

Vaal Triangle - Corel Instrumentation & Controls
North West - Applecon
Limpopo - Giant Marketing
Mpumalanga - Hmf Technologies
Kwazulu-Natal - Magnet Electrical Supplies
Gauteng - Lamba Automation
Western Cape - Technosales



*Barnyard's "More than a Feeling"
Rock Legends live music show.*



COMTEST Channel Partners Goodie Bag.

Finally, Barend saluted "The A-Team"—Comtest's rockstar Sales Team—who've visited over 2000 end-users, running demos, training sessions, commissioning advanced diagnostic tools, and hosting Technology Days.

And with the serious business wrapped up, the lights dimmed, the amps turned up, and guests tucked into lunch while rocking out to Barnyard's More than a Feeling show—a perfect finale to a day of recognition, camaraderie, and celebration. **wn**



COMTEST Channel Partners.

African companies lead in climate risk assessment, adaptation and value creation



From the outside, it may seem like corporate climate action is stalling. Only 7% of global and 6% of African companies fully report greenhouse gas emissions across Scopes 1, 2, and 3. Globally, reporting is down from 9% in 2024 and 10% in 2023.

Similarly, the number of global companies setting targets to reduce emissions across all scopes decreased by three percentage points year-over-year to 13%, following a high of 19% in 2023. Meanwhile, only 10% of African companies set targets for all scopes – three percentage points below the global average.

These are among the findings from the fifth annual climate survey report [How Companies Are Tackling the Climate Challenge—and Creating Value](#) by Boston Consulting Group (BCG) and CO₂ AI, being released today. The report draws on responses from 1,924 executives, responsible for their company's emissions measurement, reporting, and reduction initiatives. These companies originate from 16 major industries and 26 countries, collectively responsible for approximately 40% of global greenhouse gas emissions.

African companies are broadly aligned with global peers in terms of emissions transparency, but fewer have set explicit targets to reduce those emissions. This suggests that while disclosure may be driven by external requirements from other jurisdictions or customers, there is less emphasis on decarbonisation relative to the rest of the world.

Measurement of climate-related risk is also limited, with only 12% of global firms assessing all types of physical and transition risks. African companies, at 14%, are above the survey average in terms of identifying and measuring both physical and transition climate risks,

ranking second regionally, after the Asia-Pacific (16%).

African countries are among the most likely to assess climate risks, especially physical climate risks, as the continent is expected to be disproportionately impacted by climate change. This impact is already evident in the increased frequency of flooding and drought.

In fact, the survey found that the Asia-Pacific, the Middle East, and Africa experienced the highest increase in climate loss, normalised as a percentage of revenue, with the average climate-related loss in Africa increasing from 1.9% in 2023 to 2.1% in 2024.

There is a strong local awareness that climate change poses significant risks to business operations, and many companies are already experiencing its effects. As a result, businesses in the region are taking a more proactive approach to comprehensively identifying and measuring these risks, placing them ahead of other regions.

Over the next five years, companies globally plan to increase their investments in mitigation, adaptation, and resilience by dedicating an additional 16% of their capital expenditure budget to sustainability, which amounts to an increase of \$69 million per company.

This helps mitigate climate risk for these companies, for example, by weather-proofing assets, while also enabling avenues for green growth, such as sustainable product lines.

Africa leads in adaptation and resilience investment, with companies planning to increase their investments by an additional 18% of their capital expenditure budget over the next five years. Companies in the region are experiencing climate risks firsthand and, as a result, are placing greater emphasis on preparation measures such as addressing water scarcity and weather-proofing buildings.

"Around seventy per cent of companies are maintaining, if not increasing, their overall investments in sustainability. This is encouraging as it shows that climate action hasn't stalled, and momentum continues steadily around the world," said Hubertus Meinecke, the global leader for Climate & Sustainability at BCG and co-author of the report.

Commenting on the findings, co-author Hamid Maher, Managing Director and Senior Partner, BCG Casablanca, said, "African businesses are leading by example, with 14% comprehensively measuring climate risks, which is well above the global average. This is a testament to the continent's commitment to resilience and forward-thinking leadership, both of which are vital as Africa faces disproportionate climate impacts, yet also shows remarkable resourcefulness."

CLIMATE RETURNS ARE MATERIALISING AND DRIVING ACTION

According to the report, 82% of the global companies surveyed claim to have captured economic benefits from decarbonisation, with 6% reporting

a value that exceeds 10% of annual revenue; that is, a net value (after accounting for costs) of \$221 million per company. These benefits are primarily driven by revenue growth from sustainable products and operational savings from efficiency gains and resource optimisation.

Africa leads in capturing significant benefits from decarbonisation (11% of companies, compared to the survey average of 6%) and adaptation (7% of companies, compared to the survey average of 4%). Their investments in climate action are yielding tangible benefits, strengthening their position as reliable suppliers and generating greater value for their businesses.

Among global firms that assess both physical risks, such as storms and rising seas, and transition risks, including policy and market shifts, the average projected financial exposure by 2030 is \$790 million. Nearly half of the companies report that their climate risk adaptation efforts generate a return on investment of more than 10%—demonstrating that proactive preparation delivers real and measurable value.

"What matters most is that investment and action are accelerating, and our survey shows that companies are investing in climate action where there is a business case around strategic risk management and compelling financial returns," said Diana Dimitrova, a Managing Director and Partner at BCG X and co-author of the report.

ADVANCED TOOLS FOR TURNING CLIMATE GOALS INTO ACTION

As companies scale up their climate investments and goals, they are also strengthening how they finance and operationalise climate action and increasing their use of advanced governance mechanisms. The survey found that one-third of companies have implemented internal carbon prices, and the adoption of climate transition plans has risen by five percentage points year-over-year, with 61% of plans now approved at the board level. These tools represent a significant shift as companies are transitioning from broad aspirations to more operationalised climate strategies.

Hamid Maher concludes, "It is encouraging to see African companies increasing their sustainability investments and leading globally in realising financial value from decarbonisation and adaptation. With 11% of firms reporting significant returns from climate action, the continent is proving that business growth and climate leadership can go hand in hand. By embracing digital tools and prioritising adaptation, African businesses are developing a blueprint for climate resilience and sustainable value creation." **wn**

Download the publication [here](#).



John Thompson celebrates 90 years of engineering excellence in South Africa



In 2025, John Thompson, a leading South African boiler manufacturer, service provider, and division within the ACTOM group, a major electromechanical engineering business in Africa, will be celebrating its 90th year in business – a milestone for the division. Since 1935, the division has supplied and maintained industrial and utility boilers nationwide, establishing a reputation for technical expertise, reliability, and long-term customer support.

In 2025, John Thompson, a leading South African boiler manufacturer, service provider, and division within the ACTOM group, a major electromechanical engineering business in Africa, will be celebrating its 90th year in business – a milestone for the division.

Since 1935, the division has supplied and maintained industrial and utility boilers nationwide, establishing a reputation for technical expertise, reliability, and long-term customer support.

A PROUDLY SOUTH AFRICAN LEGACY

John Thompson's story in South Africa began in 1935 with the importation of boilers from the UK. It evolved to complete local manufacturing by 1954 at its Bellville factory in Cape Town, which remains the heart of the business's industrial operations today.

Over the past 70 years, John Thompson has produced approximately 5,000 package boilers and larger water-tube boilers that serve vital industries ranging from food and beverage to sugar processing.

"Our journey of starting as a boiler-building pioneer to becoming a comprehensive energy solution provider reflects a proud South African legacy that combines local expertise with global reach," says Jaco Grobbelaar, Chief Executive Officer at John Thompson Industrial Division.

"We are the only boiler manufacturer in Africa that is also an Original Equipment Manufacturer (OEM), supplying

products known for their durability and quality. Recently, we decommissioned a John Thompson boiler, one of the first built in our Bellville factory 70 years ago, that was still fully operational. This is proof of the lasting craftsmanship we deliver."

INSTRUMENTAL IN ENERGY SECURITY

This rich history of craftsmanship and innovation underscores the business's ongoing commitment to energy security and local economic development. John Thompson's Utilities division has maintained a close partnership with Eskom since 2002, providing full-time maintenance across six of South Africa's power stations.

The division also completed a key project at the Koeberg nuclear power station. Each site is staffed by hundreds of local workers, with the number increasing to over 800 during planned maintenance outages, thereby supporting local job creation and skills development.

"We have built and maintained a significant portion of the country's power infrastructure," notes Gladstone Mbili, Chief Executive Officer at John Thompson Utilities Division. "Our in-depth involvement with Eskom and regional power stations illustrates our commitment to 'keeping the lights on.' We actively seek ways to improve energy availability and reliability to avoid load shedding."

INNOVATORS WITH A GLOBAL REACH

Looking ahead, John Thompson is leading innovation in green and



From left: Jaco Grobbelaar, Chief Executive Officer at John Thompson Industrial Division; Gladstone Mbili, Chief Executive Officer at John Thompson Utilities Division; and Mervyn George, Management Consultant – Strategy & Governance.

alternative energy solutions. The business helps customers optimise existing plants for lower emissions and can even assist in converting them to cleaner fuels, such as wood chips.

John Thompson's research and development programme is advancing renewable energy technology, including a new range of package boilers designed to burn green and/or low-quality fuels efficiently.

"We are more than just manufacturers; we are committed to building a sustainable energy future," adds Grobbelaar. "Our expertise extends globally as we export our technologies and services around the world.

Through partnerships and financing models, we work to make clean energy accessible, managing and maintaining equipment so customers can focus on their core businesses."

INVESTING IN SOUTH AFRICA'S ENGINEERING FUTURE

John Thompson is committed to both its products and the people behind them. Through an annual intake of apprentices and engineers-in-training, the business actively cultivates local talent and builds a skilled workforce prepared to meet the challenges ahead.

"Skills development is a key part of our broader commitment to sustainability and innovation," says Mbili. "We currently have approximately 83 trainees in welding, fitting and boiler making programmes, supported by an apprentice school that nurtures the next generation of engineers. By growing our own talent, we help strengthen South Africa's industrial capacity and resilience."

As John Thompson celebrates 90 years of service, it reaffirms its dedication to advancing South Africa's energy

transformation. With a legacy built on quality and a future focused on clean, reliable solutions, the business is ready to meet the evolving needs of the energy and industrial sectors.

"Our history inspires us, but it is our mission that drives us forward. We will continue to deliver innovative solutions that create lasting value for our customers, communities, and the environment," Grobbelaar concludes. **wn**



SEW-EURODRIVE Leads with Next-Gen Planetary Gearboxes



Nick McKey
Business Development Representative
SEW-EURODRIVE.

Leading the way in planetary gear unit innovation, SEW-EURODRIVE is extending its reach across a growing range of industries, delivering the advantages of this powerful technology through locally engineered solutions that ensure faster lead times.

Nick McKey, Business Development Representative at SEW-EURODRIVE, explains that planetary gear units are ideally suited for applications that demand low speeds and high torque. SEW-EURODRIVE has tailored its solutions to meet the needs of heavy-duty sectors, such as sugar and mining, as well as diverse industries, including automotive and food processing.

"Our SEW P2.e planetary units, for example, are the first in their class to feature a planetary head directly coupled to an electric motor," McKey says. "This design maximises one of their key advantages - a compact footprint and reduced weight - making them easy to integrate into a wide range of applications."

Their smaller size and lighter weight allow these planetary gear units to be installed in tight spaces and overhung applications, while also simplifying installation and lowering associated costs.

"On top of these benefits, SEW-EURODRIVE enhances energy efficiency by equipping all our units with premium efficiency motors," McKey adds. "Planetary gears already achieve an impressive 96 to 98% efficiency, and by pairing them with our IE3 motors, we help customers further reduce power consumption and operating costs."

SEW-EURODRIVE has also enhanced the efficiency and longevity of its geared motors and industrial gearboxes by utilising its specialised gear oil,

which has been well received by local customers.

"We now use this oil across all our gearboxes, and it is enabling them to run at cooler temperatures - delivering improved efficiency and extending service life for our customers," McKey says.

McKey notes that SEW-EURODRIVE's planetary gear units are designed for easy installation, offering multiple interface options, such as torque arms or flange mounting, for use in various orientations, including vertical, horizontal, and at multiple pivoting angles.

"With our technological advancements making these units significantly more compact, they now integrate seamlessly into a wide range of end-user applications," he explains. "It is a major evolution from the older-generation planetary drives, which were typically large, bulky and heavy."

McKey highlights the increasing demand for shorter lead times in supplying planetary gearboxes—an area where SEW-EURODRIVE stands out, thanks to its substantial stockholding at its expansive Aeroton facility in Johannesburg. The company is currently advancing a second phase of development at the site to further strengthen its local engineering, training and manufacturing capabilities.

"With the wide variety of components we keep in stock locally, we can offer a broad selection of planetary heads in

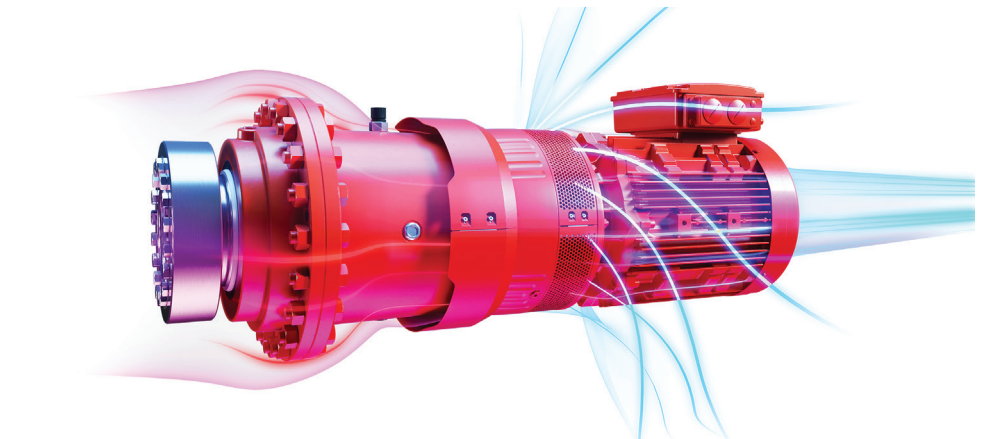
different sizes," he says. "This allows us to meet specific gear ratio and power requirements and assemble complete solutions right here in South Africa."

McKey underscores SEW-EURODRIVE's strong focus on project planning and engineering to ensure each planetary gearbox is precisely matched to the customer's application in terms of size and torque. Unlike many off-the-shelf offerings on the market, every unit assembled at the Aeroton facility is custom-built to meet exact specifications.

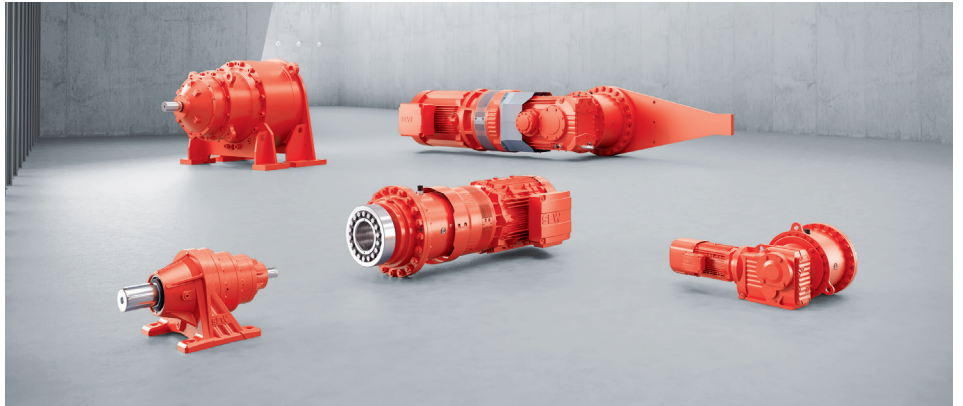
"We maintain tight control over our local parts inventory, allowing us to deliver solutions quickly without compromising on quality," he says. "Our engineering department plays a central role in the design of our industrial gearboxes, including our planetary units, ensuring optimal performance and reliability."

As part of the design process, customers receive CAD drawings, detailed data books, and comprehensive project plans, providing them with full visibility into the solution being developed. SEW-EURODRIVE's engineering team can also conduct performance simulations to demonstrate precisely how the gearbox will operate under site-specific conditions.

"This level of technical support gives our customers real peace of mind," says McKey. "They know they are not only getting a fast turnaround but also a solution engineered to deliver maximum value and reliability for their operations."



The SEW-EURODRIVE P2.e planetary gear unit offers a high thermal rating, thanks to its optional integrated motor fan that enhances cooling and supports continuous operation under demanding conditions.



SEW-EURODRIVE's complete planetary gear unit range is built for high torque and compact performance.



SEW-EURODRIVE's GearOil lubrication technology is engineered specifically for SEW gear units, providing superior wear protection, thermal stability, and extended service intervals to maximise gearbox reliability and lifespan.

Breaking barriers in South African solar

- FROM TARIFF HIKES TO SOLAR SAVINGS



While there have been fewer dark days in 2025, South Africans have progressed from finding creative ways to cope with power outages to a new cycle of rising bills and changes in tariffs, as the national power utility still struggles to meet our power needs reliably.

This year alone, Eskom direct customers faced a 12.74% tariff increase, while municipal customers experienced a slightly lower increase of 11.32%. In addition, as NERSA (National Energy Regulator of South Africa) confirmed that tariffs will increase by 8.76% in 2026/27 (instead of the previously approved 5.36%), and by 8.83% in 2027/28 (as opposed to the previously approved 6.19%), many are left wondering what else can be done to secure stable energy while managing affordability issues.

The revision over the next two years, which forms part of the NERSA Revenue Recovery Plan, is a settlement between Eskom and NERSA to correct a R54 billion revenue shortfall that NERSA admits it miscalculated. The original price hikes approved for 2026 and 2027 were based on a data input error that affected Eskom's allowable revenue. To avoid a prolonged legal battle, NERSA agreed to allow Eskom to recover the R54 billion from consumers through additional, phased-in tariff increases over the next few years.

"The new fixed charges and rising tariffs are not just an inconvenience; they are a fundamental challenge to the financial stability of households and businesses and a key issue that we as an industry are trying to tackle, looking at how best to support South Africans who are desperate for a reprieve," said Andrew Middleton, CEO of GoSolr.

"While it is true that our electricity is going to cost more in the coming years, there are positive elements in the mix as well,

as we continue to shape our residential solar offering while witnessing continued growth and innovation across the sector from competitors and partners who are rolling out much-needed renewable energy alternatives," says Middleton.

Policy shifts are paving the way for private generation, and some municipalities are pioneering the use of smart grid technology and feed-in tariffs (systems that allow homeowners to sell their excess solar-generated electricity back to the grid for credit on their utility bills).

REINFORCING THE CASE FOR SOLAR

South Africa is one of the sunniest countries in the world, with over 2,500 hours of sunlight annually. This abundance of sunshine and long peak sun hours means solar panels can operate at maximum capacity for much of the day, generating significant electricity.

BEYOND RESIDENTIAL, THERE ARE BUSINESS IMPLICATIONS TO POWER SHORTFALLS

The shift to clean energy is not just a trend; it's a necessity as we enter the warmer months, coinciding with ongoing challenges in pricing and performance. The impact on the economy, small businesses, households, and the country as a whole due to production and supply shortfalls of the national power utility cannot be ignored. Disruptions to businesses, a reduction in productivity, and the ability to discourage investment will all lead to economic losses. "While our focus is on the residential market,



we cannot overlook how the mining, manufacturing, and retail sectors suffer the most, with GDP growth slowing and unemployment rising,” says Middleton. “Wherever you look, solar is a huge necessity”.

SO WHY THEN ARE WE STILL EXPERIENCING SOME BARRIERS TO ADOPTION?

“Many homeowners still have the wrong understanding of the options now available on the market, dismissing the idea of renewable solar due to the perceived cost”, says Middleton.

Installing a system can cost anywhere from R80,000 to R300,000, and these costs are also added to the homeowner’s ongoing maintenance expenses. There has also been concern about Eskom’s insistence that installations must be signed off by a professional engineer—a step that could cost homeowners up to R20,000.

He goes on to mention that Eskom recently revealed that the South African Bureau of Standards (SABS) is finalising regulations that would enable electricians to sign off on installations

for registration purposes. “This would mean that homeowners would be able to apply for a Certificate of Compliance (CoC), which would bring this cost down significantly”.

That said, the installation cost for a residential rooftop PV installation remains out of reach for most South Africans.

Middleton believes there is a viable alternative: “Subscription solar and rental models are strategically designed to break down this barrier, increasingly finding ways to empower people to take back control of their energy future with simple, flexible options that require no upfront payments and include maintenance and insurance,” explains Middleton.

“We see a future where South Africa is powered by distributed, reliable, and sustainable sources, and we’re working towards this by not only providing solutions but also acting as a trusted advocate and a leader in the space. We are committed to a future where South Africans can thrive, free from the constraints of an unstable grid”, Middleton concludes. **wn**



Operational Readiness Is Key To PDS Implementation On Mines



Anton Lourens, CEO of Booyco Electronics.

Level 9 vehicle intervention for collision avoidance has been mandatory on South African mines since 2022; however, the effective roll-out of proximity detection systems (PDS) remains slower than expected, not due to technical limitations insofar as integration, but rather to operational readiness on site, says Booyco Electronics CEO Anton Lourens.

The Level 9 requirements mandate the implementation of engineering controls on trackless mining machines (TMMs) to automatically slow down or stop vehicles, thereby preventing both machine-to-pedestrian and machine-to-machine collisions. While PDS technology has advanced considerably to meet these requirements, Lourens stresses that a real challenge lies in how mines prepare to integrate it.

"Many operations are still not ready to operationalise PDS within their daily activities, safety systems or workflows," he explains. "Successful adoption demands coordinated involvement from all stakeholders, including the mine's own management, operators and departments, regulators, technology suppliers and TMM OEMs."

Detailed risk assessments remain a key requirement for mines to identify and mitigate significant hazards, specifically around TMMs. Lourens notes that PDS is a valuable tool in this mitigation process, providing helpful information; however, its implementation must be systematic and aligned with the broader risk framework.

The choice of PDS technology will depend on the specific environment and be based on identified risks, whether underground or surface, and whether it involves hard rock or coal. However, it must be introduced without creating further unintended risks to other operational systems, particularly production.

A critical starting point, he says, includes the mine's traffic management plan. Reducing vehicle-pedestrian interaction lowers risk and minimises production disruption. Continuous analysis of incident hotspots can inform traffic flow adjustments, and sometimes operational plans may need to be revised accordingly. Once traffic patterns are optimised, PDS deployments can be aligned to complement these flows. Misalignment risks frustrating operators, creating "PDS fatigue" from excessive warnings, which can lead to alerts being ignored.

Operational readiness, therefore, requires full leadership commitment and cross-functional collaboration. While PDS suppliers often deal with engineering teams, Lourens points out that production, finance and human resources must also be engaged. Finance teams need to weigh capital and maintenance costs against safety and efficiency benefits; HR must oversee operator training, and production must understand the operational implications.

Change management, he warns, is neither quick nor easy. It requires active communication across the mining ecosystem, ensuring that everyone understands the system's function and value. "A behaviour change must accompany any new system, or nothing will improve," he says. "Unlike when introducing mechanical equipment, some PDS operate invisibly through radio frequencies (RFID), so early engagement, clear communication, and thorough training are essential."



Level 9 vehicle intervention technology is designed to automatically slow or stop machines, reducing the risk of collisions in mining environments.

From induction and operator instruction to ongoing best practice reinforcement, Lourens concludes that mines must adopt a structured, inclusive approach to PDS if they are to achieve the full safety benefits envisioned by the Level 9 regulations. **wn**



Change management and operator training are critical to achieving the full safety benefits intended by the Level 9 collision avoidance regulations.



Proximity Detection Systems (PDS) provide a powerful tool to protect both pedestrians and operators in high-risk trackless mining machine areas.

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

Top Students Awarded Prestigious Scholarships



The University of KwaZulu-Natal (UKZN) recently honoured 86 outstanding student achievers with the University's most prestigious scholarships, awarded to only the very best of thousands of applicants.

Of the awards presented at the University's 2025 Scholarship Awards ceremony, 78 went to students who excelled academically, demonstrated strong community engagement, and distinguished themselves as leaders. Eight awards were given to students who had excelled on the sporting field, earning provincial and national honours.

The scholarships, awarded on a fiercely competitive basis, are named after South African luminaries and benefactors and are primarily funded by the University as well as donors.

In his welcome address, Deputy Vice-Chancellor: Teaching and Learning and Chair of the Scholarships Committee, Professor Thabo Msibi, stated that the

event was a celebration of excellence and the remarkable achievements of the students, who are the institution's pride and joy.

Msibi described the awards as a reaffirmation of the University's purpose in imparting knowledge, nurturing young leadership, inspiring innovation and shaping the changemakers of tomorrow.

Notable scholarships include the 'Prestige Undergraduate Scholarships', awarded to the three top-performing undergraduate students in the entire University; that is, the three top students in a cohort of over 30,000 students.

These are the 'UKZN 100th Anniversary Scholarship' - awarded to Bachelor of Science in Computer Science and Information Technology student, Mahomed Ally (3rd place), the 'Brenda M Gourley Scholarship' - awarded to Bachelor of Science in Engineering student, Talha Dada (2nd place) and the 'Lawrence and Constance Robinson Scholarship' - awarded to Bachelor of Business Science in Investment Science student, Yadiel Chatterpersad (1st place). Another prestigious award is the 'Zac Yacoob Scholarship', which is awarded to the single best Honours student in the University, specifically to Bachelor of Science Honours student Jaedon Naidu. The award for the top-ranked Master's student in the University is known as the 'Vincent Maphai Scholarship'. The 2025 recipient of this award is Saarisha Govender, a master's student in Science.

Recognising women scholars in particular, the 'Maryam Babangida Scholarship' is awarded to the best

female student in the entire University, proceeding from undergraduate to honours study. The Babangida scholar is Nokwanda Biyase, a Bachelor of Science Honours student. Another top scholarship awarded to women achievers is the 'Emma Smith Overseas Scholarship', which uniquely offers recipients the opportunity to study abroad—awarded to the top-performing female postgraduate students: Bachelor of Theology Honours student - Abongile Mpu, Bachelor of Medical Sciences Honours student - Karina Maharaj, and NDP Human Sciences student - Tatum Lee Thomas.

Sporting excellence is encouraged and nurtured at UKZN, with eight students receiving the 'UKZN Prestige Sports Scholarships' - awarded for outstanding achievement in sports at international, national and provincial levels. The award recipients this year are Dhruv Heeralal (Karate), Grace Daley (Netball), Lwanele Gaba (Rugby), Callista Ramowtar (Badminton), Amber Thomson (Netball), Jean-Luc Maurel (Body Building), Senamile Manqele (Karate) and Bontle Finger (Volleyball).

Applauding the trailblazers, Msibi said, "Remember that the scholarships you have attained carry the names of iconic individuals who have shaped the history of our country. May their legacies continue to inspire you, may you reach even higher grounds, may you push even further, and reach a level where you leave a unique mark in the world."

He added, "This recognition is not the end, only the beginning, and the world awaits your brilliance." **WN**

IEEE SPEC 2025

APPLICATION FOR SCHOLARS OPEN

DECEMBER 1-4 | Wits University, JHB



UNIVERSITY OF THE
WITWATERSRAND,
JOHANNESBURG



FOR STUDENTS

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

The conference organising committee is delighted to announce scholarships for students attending the 2025 IEEE Southern Power Electronics Conference (IEEE SPEC 2025).

Scholarships are administered by the Conference Committee and cover the student registration fee for about 10 winning recipients.

IMPORTANT DATE

23

OCTOBER 2025

Scholarship Application

Closing date for Applications: 23 Oct 2025.

Eligibility criteria for Scholarships:

- Be an IEEE PELS student or Young Professional Member.
- A paper (or papers) with you as a co-author is accepted for presentation at the IEEE SPEC 2025 conference.
- Complete the [Scholarship Application Form](#).

Please submit the completed [Scholarship Application Form](#) and send it to:

s.b.tennakoon@staffs.ac.uk

before 23 October 2025.



IEEE SPEC 2025

[CLICK HERE](#) FOR MORE INFORMATION

Universities in South Africa



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

Cape Peninsula University of Technology

Call Centre: +27 21 959 6767

Central University of Technology

Bloemfontein: +27 (0)51 507 391

Welkom: +27 (0)57 910 3500

Durban University of Technology

Switchboard: 031 373 2000

Mangosuthu University of Technology

Call Centre : 031 907 7111

Nelson Mandela University

Call Centre : 041-504 1111

North-West University

Call Centre : 0860 169698

Rhodes University

Call Centre : +27 46 603 8111

Sefako Makgatho Health Sciences University

Call Centre : (012) 521-4111

Sol Plaatje University

Call Centre : 053 491 0000

Stellenbosch University

Call Centre : +27 21 808 911

Tshwane University of Technology

Call Centre : +27 21 808 911

University of Cape Town

UCT switchboard: +27 (0)21 650 9111

University of Fort Hare

East London: 043 704 7000

Bhisho Campus : 040 608 3407

Alice Campus: 040 602 2011

University of Johannesburg

Call Centre : +27 11 559 4555

University of KwaZulu-Natal

DBN: +27 31 260 1111

PMB: +27 33 260 5111

University of Limpopo

Switchboard: (015) 268 9111

(015) 268 3332 / (015) 268 3276

University of Mpumalanga

Switchboard: (013) 002 0001

info@ump.ac.za

University of Pretoria

Switchboard: +27 (0)12 420 3111

info@up.ac.za

University of South Africa

Switchboard: 012 441 5888

study-info@unisa.ac.za

University of the Free State

Bloemfontein Campus: +27 51 401 9111

Qwaqwa Campus: +27 58 718 5000

South Campus: +27 51 401 9111

University of the Western Cape

Call Centre : +27 21 959 2911

University of the Witwatersrand

General enquiries : +27 (0)11 717 1000

Admission enquiries: +27 (0)11 717 1888

Vaal University of Technology

Call Centre : +27 (0)861 861 888

Admission enquiries: +27 (0)16 950 9356

University of Zululand

Switchboard : +27 (0)35 902 6000

Walter Sisulu University

Mthatha Campus : 047 502 2844

University of Venda

Call Centre: 015 962 8000

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

Securing the Unseen in 2025

- GLOBAL TRENDS AND PERSONAL INSIGHTS IN OPERATIONAL TECHNOLOGY CYBER DEFENCE



As I conclude my tenure as Chairperson of the South African Institute of Electrical Engineers Cybersecurity Chapter (SAIEE CSC), I would like to extend my deepest gratitude to every member of the committee. Your commitment, collaboration, and tireless efforts have been instrumental to our collective success. It has been both an honour and a privilege to serve alongside such dedicated professionals.

*By: Matthew Taljaard
CISSP | Pr. Eng. | NSE 7 OT
Chairman: SAIEE Cybersecurity Chapter*

The incoming Chairperson will continue to advance the vision and objectives of the CSC, building on the foundation we have established and guiding the chapter to even greater achievements.

The CSC was founded to serve as a platform for collaboration among Operational Technology (OT) security professionals in our industry. Within this publication, readers will find contributions from CSC members who share their perspectives, expertise, and experiences. As an OT cybersecurity professional myself, I recognise the unique challenges of finding peers who truly understand the complexities of this domain. Throughout my tenure, I have endeavoured to foster an environment where professionals can engage, collaborate, and support one another in addressing these challenges.

Those interested in joining the CSC are encouraged to contact us by email at csc@saiee.org.za for further information.

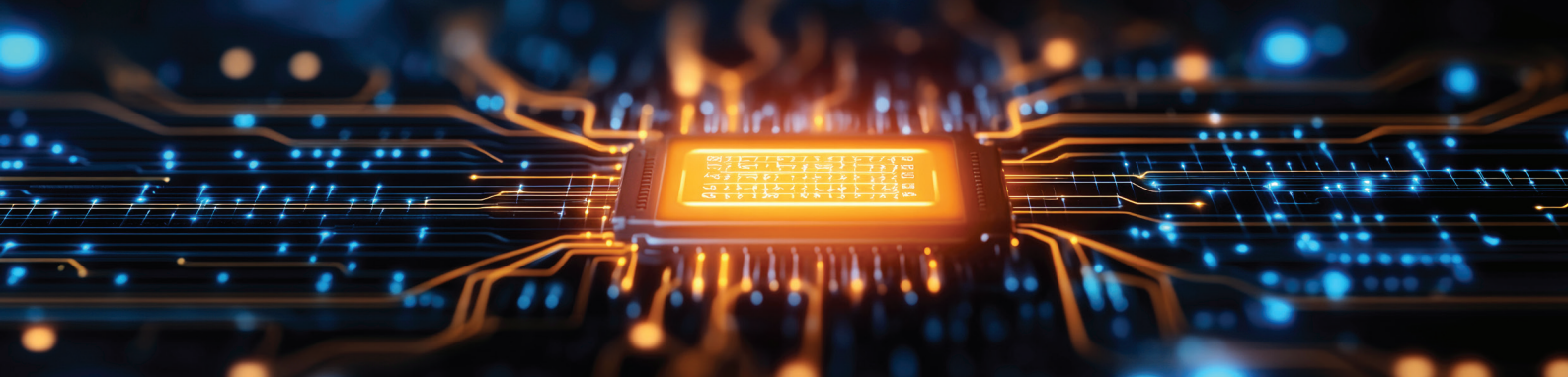
DEFINING OPERATIONAL TECHNOLOGY IN 2025: FROM NIST TO GARTNER

The National Institute of Standards and Technology (NIST) provides one of the most widely accepted definitions of Operational Technology (OT). According to NIST, OT encompasses "programmable systems or devices that interact with the physical environment (or manage devices that do), by detecting or causing direct change through the monitoring and/or control of devices, processes, and events." This definition has become a cornerstone for how industry and regulators understand OT, as it frames these systems as the

technologies that directly manage and influence the physical world.

Industries that fall within this definition include electric power, oil and gas, mining, water treatment, transportation, and manufacturing, among others. In these sectors, OT systems such as Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controllers (PLCs), and Distributed Control Systems (DCS) platforms monitor and control critical processes. The importance of this definition is evident: a cyberattack on these environments does not remain confined to data theft or IT disruption. Instead, it can lead to direct physical consequences, from halting production lines to damaging equipment, disrupting essential services, or even endangering human lives. This linkage between cyber intrusion and physical impact is what sets OT security apart from traditional IT security.

In recent years, Gartner has reframed this concept under the term Cyber-Physical Security (CPS). Gartner argues that OT cannot be viewed in isolation as just industrial control technology. Instead, it is part of a broader cyber-physical system ecosystem, where computing, networking, and physical processes are deeply integrated. This perspective expands the lens from factories and utilities to encompass areas such as smart cities, autonomous vehicles, healthcare systems, and intelligent transportation networks. The shift in terminology underscores Gartner's focus: preventing digital attacks that could cause cascading failures in the physical world.



COMPARING NIST OT AND GARTNER CPS

Scope: NIST provides a narrower, system-centric definition, focusing on the programmable devices and systems that control industrial processes. Gartner adopts a broader, ecosystem-wide perspective, positioning OT within a cyber-physical landscape that includes IT, OT, IoT, and digital infrastructure.

Focus: NIST’s definition is descriptive and technical, laying the groundwork for standards, classification, and compliance. Gartner’s CPS framing is strategic and risk-oriented, designed to highlight resilience, safety, and cross-domain security.

Implications: For practitioners, Gartner’s view underscores the need

for comprehensive security strategies that encompass IT, OT, IoT, and physical safety domains.

- For regulators, NIST remains the technical reference point that informs policy and compliance frameworks.
- For industry leaders, Gartner’s CPS model positions OT security as a boardroom-level concern, integral to enterprise risk management and national resilience.

In essence, NIST defines what OT is, while Gartner reframes why OT matters, positioning it squarely at the heart of modern cyber-physical resilience.

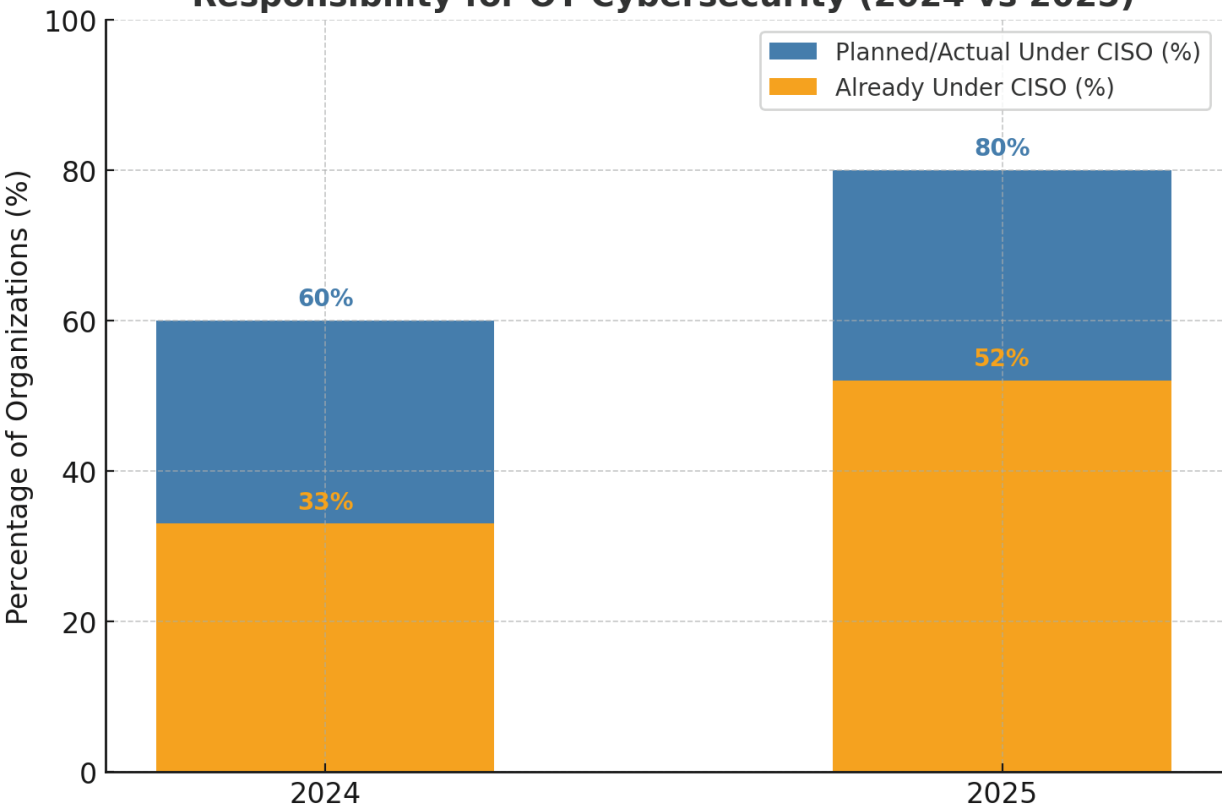
STATE OF OPERATIONAL TECHNOLOGY 2025

It is beneficial to examine both historical and current information to identify trends in our domain. Fortinet’s State of Operational Technology (OT) 2025 can offer valuable insights into these trends. Some key results of interest are:

RESPONSIBILITY FOR OT

Between 2024 and 2025, responsibility for OT cybersecurity made a decisive shift toward executive leadership. In 2024, 60% of organisations reported that OT security was either already under the CISO or planned to be within the following year. By 2025, this figure had risen to 80%, with over half (52%) confirming the CISO/CSO now holds

Responsibility for OT Cybersecurity (2024 vs 2025)



direct responsibility. This year-over-year change underscores how quickly OT security is being elevated from operational oversight to a strategic, board-level priority, ensuring that industrial risk is integrated into broader enterprise cybersecurity frameworks.

IT/OT IMPACT

The convergence of IT and OT continues to reshape the risk landscape. In 2024, 49% of intrusions impacted both IT and OT systems, but this rose significantly to 60% in 2025. This shows how integrated IT/OT networks mean that attacks often ripple across both environments, challenging the notion of OT's historical isolation or "air-gap".

VISIBILITY

Asset visibility shows a paradoxical trend. In 2024, 67% of organisations claimed 75% visibility of OT systems, while in 2025 this figure fell to 62%. This decline is not necessarily negative; it suggests that as organisations mature, they are becoming more aware of blind spots and limitations, rather than assuming complete oversight.

INTRUSIONS EXPERIENCED

Intrusion trends improved in 2025 compared to 2024. In 2024, only 24% of organisations reported zero intrusions; in 2025, that number jumped to 52%. Companies at maturity Level 4 reported the lowest intrusion rates (65% experienced no intrusions), while less mature organisations (Levels 0–2) were more vulnerable to phishing, ransomware, and malware. Business email compromise also declined significantly between 2024 and 2025, signalling the effectiveness of basic cyber hygiene practices. Phishing and ransomware/wiper malware are now the most reported intrusions experienced in 2025.

OPERATIONAL TECHNOLOGY THREAT LANDSCAPE WITH ARTIFICIAL INTELLIGENCE

With the potential for exponential growth of Artificial Intelligence (AI), many anticipated vast and sophisticated cyberattacks. However, AI has lowered the barrier of entry for carrying out cyberattacks, meaning less-skilled individuals can now execute attacks that once required deep technical expertise. This has been especially visible over the past two years as AI has become more accessible through open tools, underground forums, and as-a-service offerings.

HOW AI ENABLES LESS-SKILLED ATTACKERS

Automating Social Engineering:

Generative AI tools can produce compelling phishing emails, smishing texts, or even deepfake voice messages. Where attackers previously relied on broken grammar or poor translation, AI now creates polished, personalised lures that trick more victims.

Code Generation and Malware Development:

Attackers without programming skills can now prompt AI models to produce scripts, exploit code, or even obfuscated malware. While models have guardrails, determined attackers often find workarounds, enabling them to assemble functional attack code with minimal expertise.

Reconnaissance at Scale: AI can sift through massive datasets — public records, social media, open-source intelligence — to map targets efficiently. Tasks such as identifying vulnerable systems or finding employee details for spear phishing are significantly faster with AI-driven analysis.

Evasion of Defences: AI helps attackers modify malware or phishing kits in ways that evade traditional signature-based

detection. By automating variation, attackers can generate an endless number of polymorphic malware versions, making it more challenging for defenders to keep pace.

As-a-Service Ecosystem: AI has reinforced the "Cybercrime-as-a-Service" economy. Pre-built ransomware kits, phishing platforms, and AI-driven attack bots are now sold or rented online. Less-skilled individuals don't need to know how the tools work — they subscribe or pay for access.

AI as an Enabler of Emerging Threat Actors:

With the rapid and exponential growth of Artificial Intelligence (AI), much of the early concern centred on the possibility of highly sophisticated, nation-state-level cyberattacks. Yet, one of the most immediate impacts has been quite different: AI has significantly lowered the barrier of entry to cybercrime. Activities that once required advanced technical skills are now within reach of less-experienced individuals. Over the past two years, this trend has accelerated as AI capabilities have become widely accessible through open-source platforms, underground forums, and "as-a-service" offerings.

HOW AI EXPANDS ATTACKER CAPABILITIES

AUTOMATED SOCIAL ENGINEERING

Generative AI enables the creation of compelling phishing campaigns, smishing messages, and even deepfake voice or video content. In contrast to the poorly written lures of the past, attackers can now craft polished, contextually relevant, and personalised messages that substantially increase the likelihood of success.

CODE GENERATION AND MALWARE DEVELOPMENT

Individuals with limited or no programming knowledge can exploit

AI to generate scripts, exploit code, or even obfuscate malware. Although safeguards are in place within most AI tools, adversaries continue to identify methods to circumvent them, allowing functional malicious code to be produced with relative ease.

ACCELERATED RECONNAISSANCE

AI-driven analysis can process vast quantities of publicly available data, including open-source intelligence, corporate information, and social media content, to rapidly identify potential targets. This automation greatly enhances attackers' ability to prepare spear-phishing campaigns or pinpoint system vulnerabilities.

EVASION OF DEFENSIVE MECHANISMS

AI techniques are increasingly applied to adapt and modify malware or phishing kits to avoid detection. By generating polymorphic variations, adversaries can continually bypass traditional signature-based defences, creating a moving target for security teams.

EXPANSION OF CYBERCRIME-AS-A-SERVICE

AI has also reinforced the broader cybercrime economy. Ransomware kits, phishing frameworks, and AI-powered attack bots are now offered on a subscription basis. This "as-a-service" model means that individuals with little technical knowledge can launch impactful attacks simply by purchasing ready-made tools.

The FortiGuard Threat Landscape Report 2025 highlights how adversaries are moving faster and with greater precision, leveraging automation and AI-driven tools to enhance their capabilities.

Reconnaissance activity surged, with billions of scans each month mapping exposed services, including critical OT

and IoT protocols. Of particular concern, Modbus TCP accounted for 1.6% of global scans, indicating that industrial control systems remain a high-value target for attackers.

The report also reveals that the average time to exploit newly disclosed vulnerabilities held steady at just over five days, giving defenders little margin to react before systems are at risk. Among exploitation attempts, Windows SMB (CVE-2017-0147) accounted for 26.7% of activity, highlighting how attackers continue to rely on older, well-known flaws that organisations have failed to patch. The most heavily targeted sectors were manufacturing (17%), business services (11%), construction (9%), and retail (9%), reflecting attackers' focus on industries where downtime has immediate operational and financial consequences.

Together, these findings highlight that OT environments are being systematically probed and exploited, making proactive defence, continuous monitoring, and rapid patch management essential priorities.

CONCLUSION

Building Resilience in Operational Technology Cybersecurity

OT environments are increasingly intertwined with broader enterprise systems, and this convergence has created both opportunities and risks. To meet the challenges of today's cyber-physical threat landscape, organisations must pursue a proactive, layered approach to defence that strengthens resilience at every level.

Segmentation

A foundational step is the implementation of robust segmentation and zoning within networks. By separating

operational systems from corporate IT and establishing tightly controlled pathways between them, organisations reduce the potential impact of an intrusion and prevent attackers from moving freely across environments.

Deeper Visibility

Another critical practice is achieving deeper visibility of assets and communications within OT. Without apparent oversight of devices, traffic, and protocol use, adversaries can exploit blind spots undetected. Enhanced monitoring of industrial protocols and network behaviour allows for earlier detection of anomalies and more effective containment of malicious activity.

Vulnerability Management

Vulnerability management must also be approached with a sense of urgency. In an era where attackers can weaponise new exposures in days, reliance on slow patch cycles leaves environments exposed. Organisations should pair rapid patch deployment for internet-facing systems with compensating controls, such as virtual patching, to protect legacy or unpatchable devices.

Centralised Security Operations

Equally important is the integration of OT security into centralised security operations and incident response. Treating OT as an isolated domain creates unnecessary risk when most attacks now span both IT and OT environments. By aligning incident response processes and ensuring security teams understand the operational implications of a cyber event, organisations can respond in a coordinated and timely manner.

Unified Security Architecture

The path forward also requires simplifying and unifying security architectures.

Fragmented tools and siloed solutions slow down defenders while adversaries operate at machine speed. Consolidated platforms, supported by automation, enable a coordinated defence posture that quickly adapts to evolving threats.

PROACTIVE PREPAREDNESS

Organisations should commit to proactive preparedness through intelligence and adversary emulation. By simulating real-world attack behaviours and continuously testing defences against the techniques adversaries are known to use, defenders can move beyond a reactive posture and strengthen their readiness for the next wave of threats.

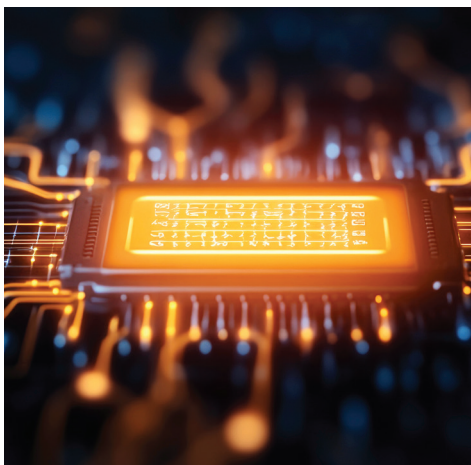
FINAL THOUGHTS

OT environments now stand at the forefront of the cyber-physical battleground. The convergence of IT and OT, combined with the acceleration of automated exploitation and the widespread availability of AI-driven attack tools, has made it clear that traditional, reactive defences are no longer sufficient. While Africa's OT security maturity may lag behind that of more developed regions, there is a unique opportunity to adopt proven global practices and chart a deliberate path forward.

By prioritising segmentation, enhancing visibility, accelerating vulnerability management, integrating OT into enterprise security operations, and adopting proactive testing of defences, leaders can build organisations that are not only resilient but also prepared to anticipate and counter emerging threats. With AI lowering the barrier of entry for adversaries, the urgency for decisive action has never been greater. **Wn**

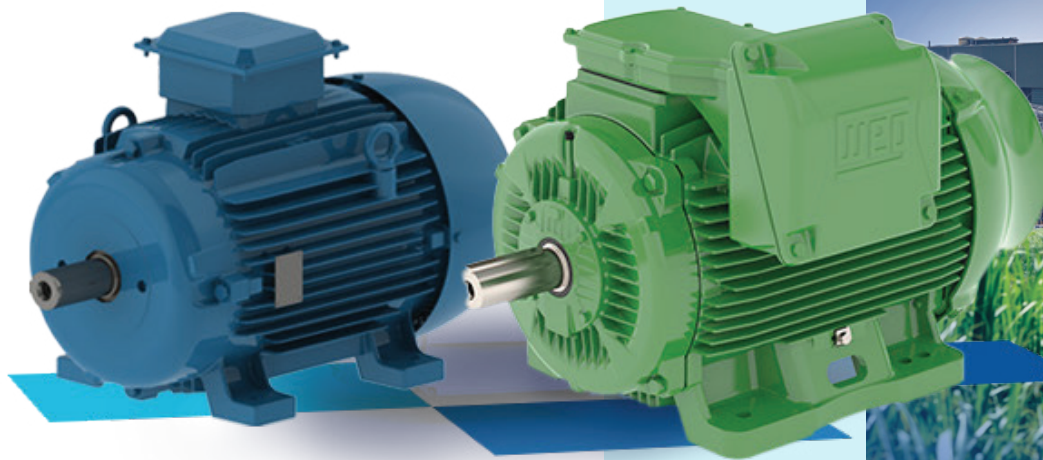
SOURCES

- National Institute of Standards and Technology (NIST), Guide to Operational Technology (OT) Security, NIST Special Publication 800-82, Rev. 3, U.S. Department of Commerce, Sept. 2023. [Online]. Available [here](#).
- National Institute of Standards and Technology (NIST), Operational Technology Security Program. [Online]. Available [here](#).
- National Institute of Standards and Technology (NIST), Glossary: Operational Technology, Computer Security Resource Centre (CSRC). [Online]. Available [here](#).
- Gartner, Market Guide for CPS Protection Platforms. [Online]. Available [here](#).
- Microsoft Tech Community, "Understanding Cyber-Physical System and IoT/OT Risk (featuring Gartner®)," Microsoft Security Blog, Jan. 10, 2022. [Online]. Available [here](#).
- Fortinet, 2025 State of Operational Technology and Cybersecurity Report, Fortinet, Jul. 9, 2025. [Online]. Available [here](#).
- FortiGuard Labs, 2025 Global Threat Landscape Report, Fortinet, May 1, 2025. [Online]. Available [here](#).



MEPS Compliant Electric Motors

WEG has your back.
For all Heavy & Light Industry applications.



Biometrics in an AI-Driven Future

- HOW SAFE IS "SOMETHING YOU ARE"?



Authentication is the cornerstone of digital security, ensuring that only authorised individuals gain access to systems and information. While traditional approaches have relied on passwords or tokens, biometrics like fingerprints, facial recognition, and voice identification have rapidly become the preferred method due to their speed and convenience.

By: Meenal Vala (Pr.Eng. CISSP)

However, in an era where artificial intelligence is evolving at a breakneck speed, how secure are these authentication factors? Advances in deepfake technology now enable the replication of faces and voices with alarming accuracy, while high-resolution imaging can capture fingerprints from everyday objects. Unlike passwords, biometric data cannot be changed once compromised, raising serious questions about its long-term reliability.

This article aims to raise awareness and provoke thought about the future of authentication and security. It does not attempt to unpack every challenge or provide definitive answers, but rather to highlight emerging risks and encourage reflection on where current trends may lead.

But enough of the disclaimers, Ts and Cs, and setting the scene, let's get into it. Authentication is the process of proving that you are who you claim to be before gaining access to a system, service, or device. Traditionally, authentication has relied on one of three categories:

1. **Something you know** – a password, PIN, or passphrase.
1. **Something you have** – a security token, smart card, or one-time password (OTP) sent to your phone.
1. **Something you are** – biometric traits such as fingerprints, facial recognition, iris scans, or voice patterns.

Multifactor Authentication (MFA) builds on this principle by requiring a

combination of two or more factors from different categories. The logic is simple: while a password alone can be guessed or stolen, combining it with a fingerprint or OTP makes unauthorised access significantly harder.

For years, the cybersecurity community has advocated for the adoption of MFA across personal and business environments. Passwords remain the weakest link, with users often recycling them or choosing weak ones. By adding a second or third factor, the attack surface shrinks.

Common MFA examples include:

- Password + OTP via SMS or authenticator app.
- Smart card + PIN.
- Password + fingerprint.

MFA is now widely used in banking apps, workplace systems, and personal devices, often blending convenience with improved security.

Among the MFA options, biometrics stand out as a distinct choice. Unlike tokens that can be lost or passwords that can be forgotten, biometrics are always with you. The appeal is undeniable:

- **Convenience** with no more struggling to remember complex passphrases.
- **Speed** of unlocking your phone or accessing an app takes milliseconds.
- **Accessibility** with biometrics reduces barriers for users who struggle with traditional credentials.

It is no surprise that fingerprints, facial recognition, and even voice-based logins are now standard in commercial technology. Airports use them to speed up border control. Banks use them for customer authentication. Many workplaces, residential community sites and apartment complexes are deploying them for physical access control. There is also an extensive adoption for its use in the personal and consumer technology space. The most significant adoption is on end-user devices and home security. Biometrics have become synonymous with modern, user-friendly security.

But are biometrics still safe in a world shaped by artificial intelligence (AI)?

The very technology that makes our lives easier is also arming cybercriminals with powerful tools:

- **Deepfakes** for faces and voices: With just a few seconds of video or audio, AI can generate convincing fakes capable of bypassing facial recognition or voice unlock systems.
- **High-resolution photography:** Advanced cameras can capture fingerprints from surfaces you've touched, which can then be recreated with surprising accuracy.
- **Synthetic biometrics:** Generative AI can now produce lifelike biometric data, ranging from fingerprints to iris patterns, thereby increasing the risk of spoofing.
- **Template theft:** Unlike passwords, biometric templates stored in databases cannot be changed once



stolen, making breaches especially dangerous.

In short, the same innovations driving AI are blurring the line between legitimate and fraudulent identities. The fundamental issue is permanence.

- Forgot your password? Reset it.
- Lose your smart card? Replace it.
- Compromise your fingerprint? You only have ten, and they cannot be changed.
- Have your likeness uploaded and repurposed? Are you truly who you claim to be in the digital world?

Once biometric data is stolen or replicated, it is compromised forever. With the proliferation of biometric databases, ranging from government systems to consumer errors and actions, the risk of large-scale exploitation increases. In this age of social media, the risks extend beyond deliberate cyberattacks. Many popular apps encourage users to upload selfies to generate avatars, predict how they will look in the future, or transform their image with filters. While entertaining, these platforms often collect biometric data without clear regulation or transparency. Users usually lack knowledge of where their images are stored, how long they are retained, or who ultimately owns the data. In some cases, these images could be used to train AI systems or even resold, creating risks that extend far beyond the original intent. In effect, we are voluntarily giving away our most permanent identifiers —our faces and voices — without fully understanding how they may be exploited in the future.

Unlocking your phone or opening a door may feel futuristic, but what happens when an attacker can generate a near-perfect synthetic version of that same

face? And how safe will you feel if that same attacker can use the technology to gain access to your home?

This raises an important question: Are we placing too much faith in 'something you are' as the ultimate form of security, and do end users truly understand the future repercussions of today's trends and fads, as well as the risks they pose to others?

However, we are at a turning point where biometrics should not be abandoned, but rather re-evaluated in light of AI's rapid progress. Some possible paths forward include:

- **True Multifactor Authentication:** Biometrics should always be combined with at least one other factor; therefore, the statement may be that 2FA (two-factor authentication) is dead and will always require MFA (multifactor authentication). For example, facial recognition paired with a hardware token, along with the original password.
- **Liveness Detection:** Advanced biometric systems aim to determine whether a fingerprint, face, or voice is from a genuine, live human rather than a replayed or synthetic sample. While effective today, attackers are already adapting to bypass these checks.
- **Continuous Authentication:** Instead of a single login, systems can monitor user behaviour (typing rhythm, movement, interaction patterns) to verify identity continuously.
- **Privacy-Preserving Biometrics:** Emerging technologies, such as homomorphic encryption and secure enclaves, may reduce the risk of biometric databases being misused.

Ultimately, biometrics should be viewed as one tool in a layered defence strategy, not a silver bullet.

Biometrics have transformed authentication by offering speed, convenience, and accessibility. Yet, in an AI-driven future, they are not immune to compromise. Unlike passwords or tokens, biometric traits cannot be reset once stolen, making their misuse potentially lifelong. As engineers and technologists, we must ask: in a future where AI can mimic our faces, voices, and even fingerprints, how much longer will biometrics remain reliable as a primary authentication factor?

The answer is not to abandon biometrics, but to adapt to them. Not every security requirement should default to biometric use, even though it may seem attractive, easy to use, or marketable as a modern solution. For instance, some commercial apartment buildings are turning to facial recognition for access control, but is that really the best application of the technology? Security choices must be deliberate, selective, and forward-thinking. The goal is not to appear futuristic, but to develop measures that remain effective and resilient against future threats.

The safest path forward lies in layered security: using biometrics in conjunction with other factors, investing in AI-driven anti-spoofing defences, and never assuming that "something you are" is unbreakable.

As October's Cybersecurity Awareness Month reminds us, security is a moving target. Our role as engineers is not only to embrace innovation but also to question its limits, consider purpose-fit implementation and prepare for the next frontier of challenges it brings. **WN**

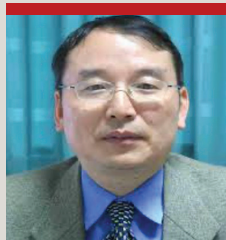
IEEE SPEC 2025

SAVE THE DATE

DECEMBER 1-4 | Wits University, JHB

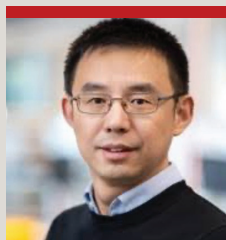
Introducing our Keynote Speakers

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



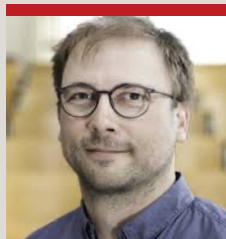
Mark Dehong Xu

Dr Xu has authored ten books and over 200 papers, holds more than 40 patents, and his research focuses on power electronics, renewable energy, and energy efficiency.



Xionfei Wang

Prof Wang is a professor at the KTH Royal Institute of Technology in Stockholm and a part-time professor at Aalborg University.



Andreas Liske

Dr Liske's research focuses on modelling, control and condition monitoring of electrical drives and power electronics.



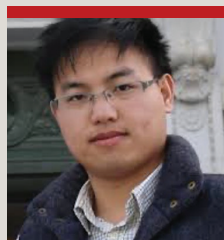
Günter Keller

Dr Keller has instructed over 70 industrial and university workshops and seminars worldwide, as well as more than 10 conference workshops and tutorials globally.



Frede Blaabjerg

Dr Blaabjerg's research focuses on power electronics applications, reliability, harmonics, and adjustable-speed drives.



Changfu Zou

Dr Zou is currently an Associate Professor. His research interests include advanced modelling and automatic control of energy storage systems, and particularly batteries.



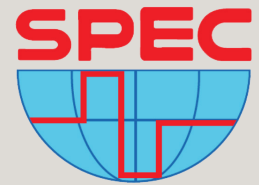
Minjie Chen

Dr Chen has received several accolades and holds three issued patents and has several patents pending.



Petar Grbović

Dr Grbović's research focuses on advanced energy storage devices, power converter topologies, and control of power converters.



UNIVERSITY OF THE
WITWATERSRAND,
JOHANNESBURG

IEEE SPEC 2025



Implementing a Novel Cybersecurity Algorithm for Smart Grid SCADA System



My fascination with Technology and its role in fostering innovation and adaptability has driven my Academic and professional interests. During the COVID-19 pandemic, this curiosity led me to question the Cybersecurity preparedness of organisations during the transition to remote work.

*By: Kholofelo H. Halefose,
Topside E. Mathonsi,
Tonderai Muchenje and
Deon Du Plessis*

With my vested interest in the protection of Electric Power Utilities (EPUs), I began to focus on the vulnerabilities and risks faced by the critical infrastructure, specifically the Smart Grid.

Recognising the immense scope of the Smart Grid, my Supervisors advised me to narrow the focus of my research study. I subsequently decided to concentrate my efforts on Supervisory Control and Data Acquisition (SCADA) systems, a key component of modern power grids. Thank you to my Supervisors; this focused approach ultimately led to the publication of my research article titled "Implementing a Novel Cybersecurity Algorithm for Smart Grid SCADA System".

Figure 1 illustrates a Smart Grid communication network. It demonstrates the connection between various

networks, including Consumer Premises Networks (CPN), Home Network Area (HAN), Industry Area Network (IAN), and Business Area Network (BAN), utilising technologies such as Zigbee, PLC, Z-Wave, and IEEE 802.11. These connect to Neighbourhood Area Network (NAN) and Access Network via Smart Meters (M) and concentrators (C).

The Access Network utilises BPL/WiMAX, connecting to the Core Network (S) and Data Centre (D) through wireless and wireline network providers. Keywords: Smart Grid, Communication.

YOU MAY ASK: 'WHY CYBERSECURITY ALGORITHMS?'

Cryptographic algorithms are essential for ensuring the secure transmission of data across a network. They provide the fundamental protection needed for communication in any

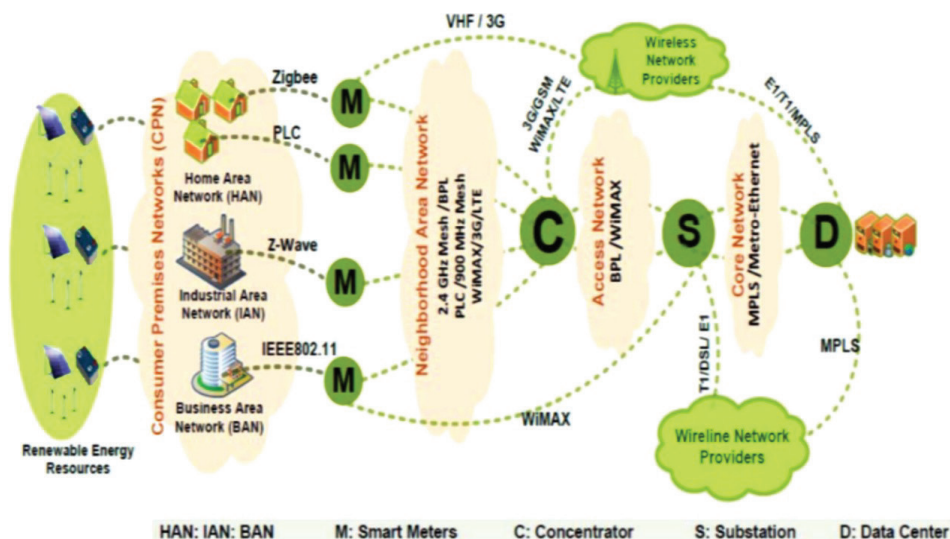


Fig. 1. Smart Grid basic network architecture (Saidallah, 2017).



digital system. Without them, any information transmitted across a network is vulnerable to interception, manipulation and theft. The integrity and confidentiality of data, whether it is financial transactions, personal information, or critical infrastructure commands, would be nonexistent.

Furthermore, these algorithms are crucial for achieving the three core cybersecurity goals of the CIA triad model: Confidentiality, Integrity, and Availability. Unlike Information Technology (IT) cybersecurity, where Confidentiality is the top priority, Operational Technology (OT) within the power grid, such as SCADA, prioritises Availability. To ensure that this research comprehensively addresses this critical objective of Availability, the research study focused specifically on Denial-of-Service (DoS) attacks, as they directly threaten the operational continuity of the SCADA system.

Widely used Public Key Cryptography (PKCs), including Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) algorithms, are commonly employed to secure communication within various systems. This research study presented a comparative analysis of these well-known algorithms, alongside others such as N-th Degree Truncated Polynomial Ring (NTRU). The selection of two specific algorithms for integration, as detailed below, was based on

an extensive literature review and a thorough comparative analysis of their performance and suitability.

THE PROPOSED CYBERSECURITY ALGORITHM

The primary goal of this research study was to develop a more effective cybersecurity algorithm that would strengthen and enhance cybersecurity for smart grid SCADA systems. To achieve this, the proposed Enhanced Cybersecurity Algorithm was designed by integrating the NTRU algorithm and Toom-Cook algorithm.

NTRU was chosen because it is among the fastest and most robust public cryptosystems, resistant to both classical and quantum attacks (Premnath, 2018). The Toom-Cook algorithm was chosen because it is among the most efficient methods for multiplying large integers, which in turn increases the efficiency of the encryption and decryption process by reducing the complexity involved in key encoding and decoding, as well as the transmission rate.

NTRU ALGORITHM

The paper suggests integrating a quicker and more lightweight NTRU asymmetric cryptosystem into SCADA systems. The goal of the NTRU algorithm was to reduce memory and processing overheads drastically. The two algorithms that comprise the NTRU cryptosystem are NTRUSign, used for digital signatures, and NTRUEncrypt, used for encryption. Compared to RSA

encryption, which performs modulo exponentiation under specific rules, and ECC encryption, which involves scalar multiplication for points on an elliptic curve, NTRU encryption utilises polynomial operations for encryption and decryption, allowing for faster speeds. Consequently, the NTRU is a quicker and lighter method compared to others, as it offers simple key generation, fast encryption and decryption, and requires very few computational resources.

Nonetheless, the suggested approach integrated the NTRU and Toom-Cook algorithms, considering data encryption and decryption, as well as user authentication. This integration ensures the efficient and secure encryption and decryption of data for the Smart Grid. The fact that NTRU is immune to quantum assaults and is classified as a post-quantum cryptosystem is another factor in the decision to use it. On the other hand, NTRUSign is useful for SCADA applications that have real-time limitations.

TOOM-COOK ALGORITHM

Since the Toom-Cook algorithm is faster than both the Karatsuba and Toom-Cook-4-way approaches, it was selected for merging with the NTRU. Additionally, a study by Mera et al. showed that the Toom-Cook algorithm is a 9/5 improvement over the Karatsuba approaches, which reduce the number of multiplications from 9 to 5. Large integer multiplication improves efficiency in just a small

number of methods. The well-known techniques Karatsuba, Toom-Cook-3, and Toom-Cook-4 aid in increasing the effectiveness of cryptosystems. These methods are applied in cryptographic algorithms, such as the Diffie-Hellman key exchange protocol, ElGamal, RSA, and elliptic curve cryptosystems, to reduce the complexity of key encoding and decoding.

McEliece Cryptosystems also employs this technique to get around issues with transmission rate and encrypted key size. The research examined various cybersecurity algorithms and well-established methods for enhancing the efficiency of cryptosystems. Thus, by combining the NTRU and Toom-Cook algorithms, the study proposed an integrated cybersecurity method for the Smart Grid SCADA system. An increase in processing speed was made possible by this integration. As a result, encryption and decryption methods became more effective, ensuring a safe network connection.

The results obtained demonstrate that NTRU outperforms ECC, RSA and AES in cryptographic operations, achieving speeds approximately 2 to 10 times faster for comparable security levels. Under DoS attacks, ECS experienced only 0.5% packet loss, proving its suitability for SCADA systems. Additionally, it is resistant to both classical and quantum attacks. The algorithm enhances authentication, availability, data integrity, and confidentiality while minimising computational overhead.

This research study concludes with a clear direction for future research and recommendations. Our analysis has demonstrated that NTRU is a robust algorithm with significant resistance to quantum computing threats. However,

in a rapidly evolving technological landscape, new risks emerge daily, and what was sufficient two years ago may no longer be a viable defence.

This is precisely why continuous research is vital—to ensure our cybersecurity algorithms are constantly improving. While we face an array of new challenges, including those from Artificial Intelligence (AI)-driven attacks, the looming threat of quantum computing is one we cannot afford to ignore, especially when safeguarding critical infrastructure like EPU. My current research is a focused effort to integrate a Post-Quantum Cryptography (PQC) algorithm, addressing this vital and undeniable risk faced by the Smart Grid.

A recent study conducted by Unsal (2025) states that “Quantum computers have made tremendous progress in recent years, and their potential capabilities could revolutionise many fields of science and technology. However, one of the most significant challenges posed by the advent of quantum computing is its impact on cryptography, which underpins the security of modern communication systems”.

It is therefore imperative that we guard against the threat of quantum computing. My contributions aim to develop robust cybersecurity controls that contribute to effective, sustained, and resilient systems, thereby ensuring a secure and reliable electricity supply for the nation. **Wn**

REFERENCES

- Saidallah, M., Fergougui, A.E.L., Elalaoui, A.E.: A survey and comparative study of open-source wireless sensor network simulators. *Int. J. Adv. Res. Comput. Sci.* 7(3), 1–7 (2017).
- Premnath, A.P.: Application of NTRU Cryptographic Algorithm for securing SCADA communication. UNLV Theses, Dissertations, Professional Papers, and Capstones, pp. 1–54 (2018).
- Mera, J.M.B., Karmakar, A., Verbaughede, I.: Time-memory trade-off in Toom-Cook multiplication: an application to module-lattice based cryptography, pp. 1–23. The International Association for Cryptologic Research (IACR) (2020).
- Unsal, S.: (2025) A Comparative Performance Evaluation of Kyber, sntrup761, and FrodoKEM for Post-Quantum Cryptography. Department of Computer Engineering (2025).
- All references can also be found in the article. A special thanks to my Co-Authors: Topside E. Mathonsi, Tonderai Muchenje and Deon Du Plessis. This research study has also been cited in the online proceedings of Pan-African Artificial Intelligence and Smart Systems ([PAAISS2024](#)).



BREAST CANCER AWARENESS



Breast cancer is one of the most common cancers among women. Breast Cancer Awareness Month is an invaluable reminder that you are never too young – or too old – to start protecting yourself both physically and financially against the possibility of developing such a debilitating illness,” says Dr Kerissa Naidoo, Old Mutual Chief Medical Officer.

Depending on the severity, recovering from an illness like breast cancer can be quite costly.

At 39, Bernadette found herself at an oncologist’s office with no severe illness cover. Watch the video [here](#).

THE COSTS INVOLVED INCLUDE:

The direct costs associated with diagnosis, hospital admission and medication are normally covered by medical aid or gap cover.

The indirect costs are often overlooked, this includes taking time off work to recover, hiring a full-time caregiver, buying a special diet, and more.

WE’VE GOT YOU COVERED

Old Mutual’s Illness insurance pays out a single tax-free amount of up to R6 million to help with your recovery or day-to-day expenses while you take time off. The payout percentage depends on how severe the illness is.

You can decide what you use the payout for.

WHY CONSIDER ILLNESS INSURANCE FROM OLD MUTUAL?

In 2024 we paid out R888 million in claims, 50% of which was for cancers.

You’re covered for up to 30 days before your first premium is due.

With the help of a financial adviser, you can choose and pay only for the cover you need.

Use our interactive tool to see what people in your age group claimed for (www.omclaimstool.co.za).

For more information and Ts & Cs, visit oldmutual.co.za/illness

SPEAK TO ME TODAY

to get illness insurance to protect yourself financially from an illness like breast cancer.



Misheck Mdala
Executive Financial Adviser
mmdala@oldmutual.com
082 546 1674



OLDMUTUAL

Strengthening Cybersecurity in Power Utilities

- THE ROLE OF DIRECTORY SERVICES IN THE IIoT ARENA



The proliferation of Industrial Internet of Things (IIoT) and the convergence of Operational Technology (OT) and Information Technology (IT) within power utilities have introduced both significant advancements and increased cybersecurity risks.

By: Kgomoiso Manyapetsa

As Industrial Control Systems (ICS) become more interconnected, the need for robust identity and access management (IAM) frameworks has grown. Directory services such as Lightweight Directory Access Protocol (LDAP), OpenLDAP, and Active Directory (AD) provide centralised IAM solutions that enhance security, scalability, and compliance within OT environments.

This article examines the crucial role of directory services in safeguarding power utilities by mitigating risks associated with unauthorised access, credential misuse, and regulatory non-compliance. Furthermore, the paper discusses implementation challenges, including integration with legacy systems, performance considerations, and high availability requirements.

It highlights key industry standards and Request for Comments (RFCs) that underpin directory services, such as RFC 4511 for LDAP and RFC 4120 for Kerberos-based authentication. Future directions in OT security emphasise the adoption of Zero-Trust architectures, AI-driven anomaly detection and network access control based identity verification.

As power utilities continue to embrace digital transformation, the deployment of scalable and resilient directory services will be instrumental in strengthening cybersecurity defences against evolving threats.

INTRODUCTION

Identity and Access Management (IAM) has become a cornerstone of security in Operational Technology (OT) and Industrial Control Systems (ICS) environments, which ensures controlled access to critical systems. With increasing integration of Distributed Energy Resources (DERs), Independent Power Producers (IPPs), Industrial Internet of Things (IIoT), and Prosumers, the need for centralised IAM has become paramount. Typical OT/ICS architectures include Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA) systems, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), and IIoT devices connected via field buses such as the new Ethernet-APL (Advanced Physical Layer) and other protocols.

The diversity of devices and systems necessitates robust IAM frameworks that support seamless integration. Directory services play a pivotal role in this ecosystem by centralising user, application, and device management while providing authentication, authorisation, and auditing capabilities. This article examines how directory services enhance security, operational efficiency, and compliance in OT/ICS environments.

BACKGROUND

OT/ICS systems underpin critical infrastructure, including power



generation and delivery. These environments face unique challenges due to real-time operational requirements, legacy systems, safety aspects, and the need to maintain high availability. The Purdue Enterprise Reference Architecture (PERA) model referenced in the figure encompasses levels 0 to 3.5 in the industrial hierarchy, as well as levels 4 to 5, which represent the enterprise information technology hierarchy.

This highlights the layered approach in OT/ICS, covering field devices, control systems, and operational management. Modern implementations integrate IIoT technologies, adding complexity to IAM due to the proliferation of devices and data flow across these layers. Furthermore, field buses such as the new Ethernet-APL standard will result in increased Ethernet-based connectivity, which will require centralised IAM solutions to ensure security and operational consistency.

PROBLEM STATEMENT

Many OT/ICS environments lack centralised identity and access management systems, which leads to fragmented credential management and inconsistent security policies across devices. The growing number of IIoT devices and embedded systems further complicates authentication and authorisation, increasing the risk of unauthorised access and cyber threats. Traditional security mechanisms, such

as network segmentation and endpoint protection, often fail to address the modern threat landscape adequately. Cybersecurity risks, including ransomware attacks, unauthorised access, and insider threats, have escalated and are targeting critical

infrastructure and disrupting operations. In addition to user identity management, securing device credentials has become essential.

Many OT devices rely on hardcoded or default passwords, which make



Figure 1: Purdue Enterprise Reference Architecture Model

them vulnerable to exploitation. A lack of centralised device password management leads to operational inefficiencies and increased security risks.

Directory services must extend beyond user authentication to incorporate device identity management, to ensure that IIoT devices, controllers, and field devices adhere to the same authentication and authorisation standards. Integrating IAM solutions with automated credential rotation, certificate-based authentication, and multi-factor authentication for both users and devices can significantly improve security and compliance. These challenges are compounded by the integration of legacy systems with modern IAM frameworks, which create gaps in security and operational efficiency. Addressing these issues requires a structured approach to directory services that support OT/ICS-specific requirements, including comprehensive user and device identity management, centralised credential storage, and seamless interoperability between heterogeneous systems.

OVERVIEW OF DIRECTORY SERVICES

Directory services provide a structured repository for managing identities, permissions, and access controls. Core components include schemas, replication mechanisms, and access control lists (ACLs), collectively enabling centralised management. Protocols such as LDAP and Kerberos facilitate secure authentication and authorisation, ensuring efficient communication between users and directory services. The integration of directory services with OT/ICS systems supports regulatory compliance by generating auditable logs and enforcing centralised policies.

OPERATING SYSTEMS AND ASSOCIATED DIRECTORY SERVICES

In OT/ICS environments, the choice of operating systems plays a significant role in implementing directory services. Embedded Linux-based operating systems, such as Yocto and OpenWrt, dominate IIoT devices due to their flexibility and lightweight design.

These systems integrate with directory services such as OpenLDAP and FreeIPA, providing a scalable IAM solution. On the other hand, Windows-based systems commonly utilise Active Directory, leveraging features such as Group Policy for centralised management. Interoperability between Linux and Windows platforms is facilitated by protocols such as Kerberos and Samba, which enable seamless synchronisation and unified IAM frameworks. However, differences in architecture between these systems pose challenges to integration, requiring tailored solutions to achieve compatibility.

TYPICAL DEVICES IN POWER PLANTS AND SUBSTATIONS

Power plants and substations house a range of critical devices responsible for automation, protection, and control. With reference to figure 2, these include:

- SCADA Systems – Provide centralised monitoring and control of industrial processes.
- PLCs – Used for automation control of electromechanical processes.
- RTUs – Interface between field devices and SCADA systems.
- IEDs – Enable advanced protection and monitoring functions.
- Human-Machine Interfaces (HMIs) – Facilitate user interaction with control systems.
- Protection Relays – Ensure power system stability and fault mitigation.
- Industrial Switches and Routers – Manage network traffic within the OT environment.
- Ethernet-APL Devices – Provide connectivity for process automation applications.

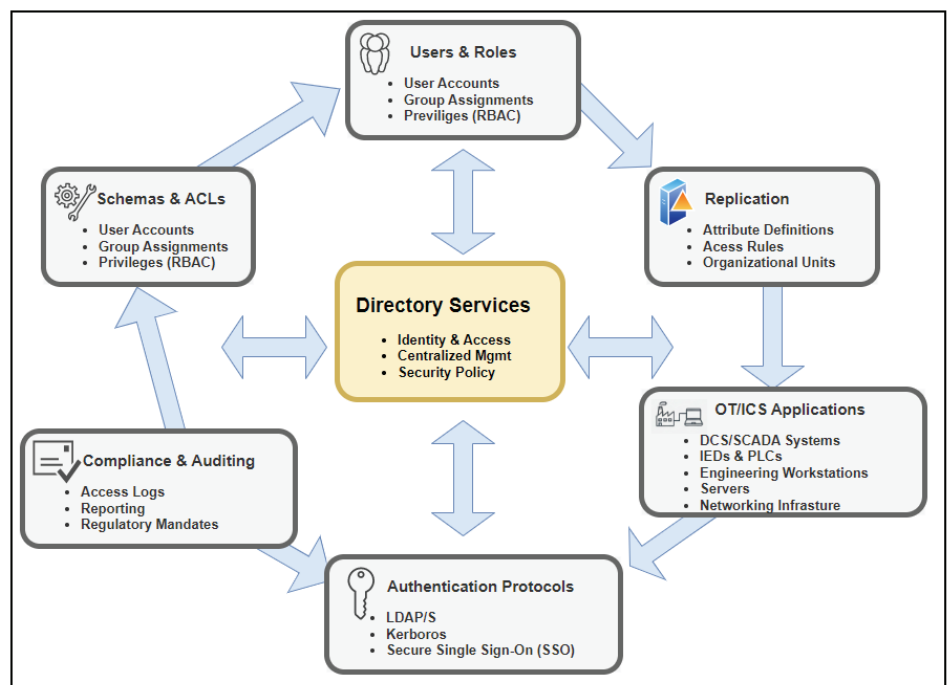


Figure 2: Directory Services Overview

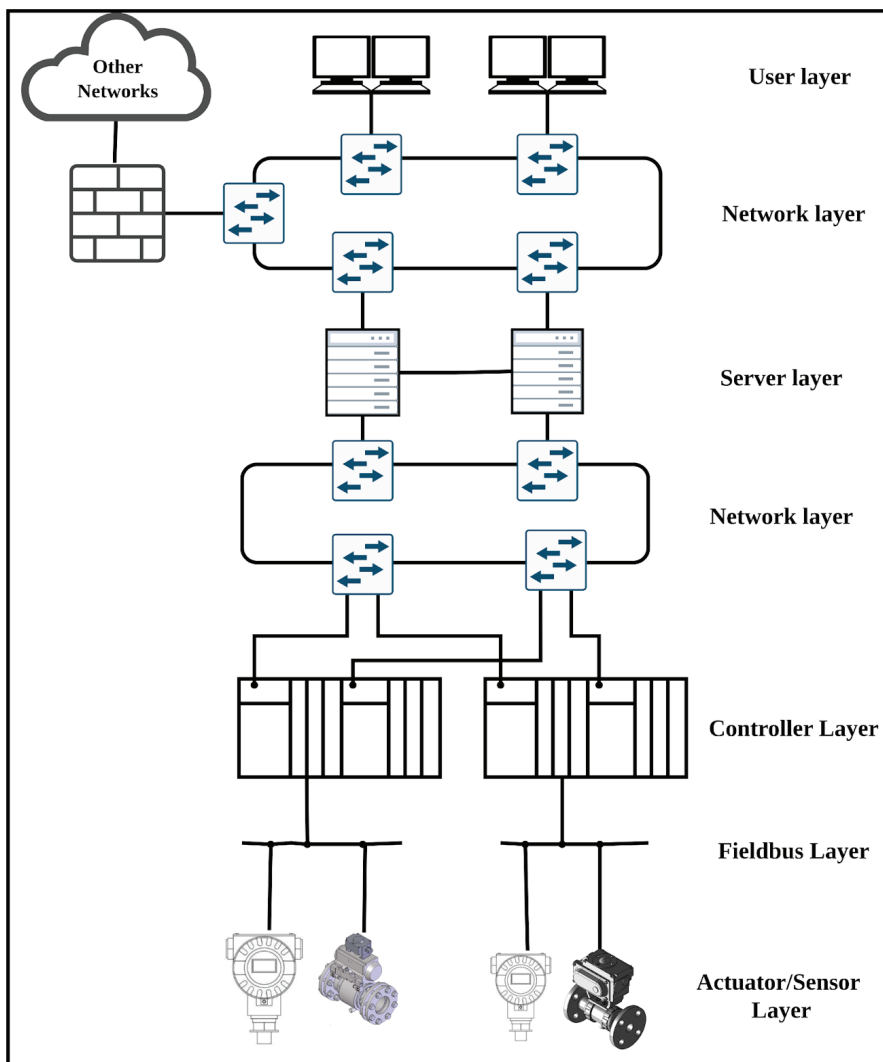


Figure 3: Typical Power/Process Plant Reference Architecture

These devices increasingly support IEEE 802.1X authentication, making them suitable for integration with directory services such as LDAP. IEEE 802.1X operates at the network level to ensure that only authenticated and authorised devices can connect. The protocol interacts with directory services by using RADIUS or TACACS+ to validate credentials, making it a critical component of modern OT/ICS security.

SECURITY CHALLENGES IN DIRECTORY SERVICES IMPLEMENTATION

Despite the benefits of directory services, their implementation in OT/

ICS environments presents security challenges. One major issue is the integration of legacy systems that lack modern authentication support, increasing the risk of vulnerabilities.

Additionally, misconfigured directory services can expose systems to attacks such as LDAP injection, credential theft, and privilege escalation.

A robust security approach must include continuous monitoring, encryption, role-based access control (RBAC), and multi-factor authentication (MFA) to mitigate these risks.

A recurring theme in OT/ICS cybersecurity is the perceived shortage of skilled personnel. However, this often becomes a convenient excuse that obscures deeper organisational issues. The reality is that there are numerous certification pathways and training institutions, ranging from vendor-neutral programs such as CompTIA, SANS, IEC, and GIAC, to vendor-specific certifications from Check Point, Fortinet, Microsoft, Red Hat, Siemens, Huawei, and Cisco, that provide practical, hands-on, and job-ready training.

These platforms make it entirely feasible to teach directory services, identity management, and network access control at scale. Therefore, it is inaccurate to claim that skill availability is a barrier to progress. Instead, organisations must prioritise investment in human capital. This includes funding certifications, establishing internal labs, and developing rotational training programs to build internal expertise. Security gaps due to underinvestment in people are a management failure, not a market problem.

BENEFITS OF DIRECTORY SERVICES IN OT/ICS

Directory services enhance security by enforcing centralised authentication policies and access controls, thereby reducing unauthorised access risks. Directory services enhance compliance by aligning with industry standards such as IEC 62443 and NIST 800-82, to ensure regulatory adherence. Furthermore, centralised identity and access management simplifies administrative workflows, thereby reducing the burden on OT/ICS operators. The scalability of directory services also enables seamless integration of new devices and users, supporting the rapid expansion of IIoT in industrial environments.

IEEE 802.1X AND ITS ROLE IN OT/ICS SECURITY

IEEE 802.1X is a network access control protocol that enforces authentication before granting devices access to industrial networks, thereby enhancing the security of OT and ICS. It operates at the Open System Interconnect (OSI) Layer 2, ensuring that only authenticated devices can communicate within the network infrastructure.

The authentication process relies on the Extensible Authentication Protocol (EAP), where the supplicant (client device) interacts with an authenticator (such as a network switch or access point), which in turn forwards authentication requests to a RADIUS server. Depending on the authentication backend, the RADIUS server may integrate with OpenLDAP or a Kerberos Key Distribution Centre (KDC) to validate credentials. In LDAP-based authentication, the RADIUS

server verifies user or device credentials against an OpenLDAP directory using an LDAP bind request, ensuring that only authorised personnel and trusted devices gain access.

Alternatively, in a Kerberos-based approach, the RADIUS server interacts with the KDC to request a Ticket Granting Ticket (TGT) and subsequently a service ticket for network access.

Upon successful authentication, the RADIUS server sends an Access-Accept message to the authenticator, which grants network access to the supplicant.

This integration with directory services strengthens cybersecurity resilience in OT environments by enforcing centralised, policy-driven authentication while preventing unauthorised access to critical control networks.

IEEE 802.1X & OPENLDAP

The sequence diagram illustrates the authentication process in an IEEE 802.1X network access control framework, leveraging the Extensible Authentication Protocol (EAP) and a RADIUS server with OpenLDAP for identity verification.

The process begins when a user (1) requests network access, prompting the supplicant (the client device) (2) to initiate an EAP authentication exchange with the authenticator, typically a network switch. The authenticator (3), acting as a pass-through device, forwards the EAP request to the RADIUS server (4), which in turn queries the OpenLDAP server to validate the user's credentials via an LDAP bind request. Upon receiving a response from the OpenLDAP server (5) indicating authentication success or failure, the RADIUS server (6) conveys an Access-Accept or Access-Reject message to the authenticator. Based on

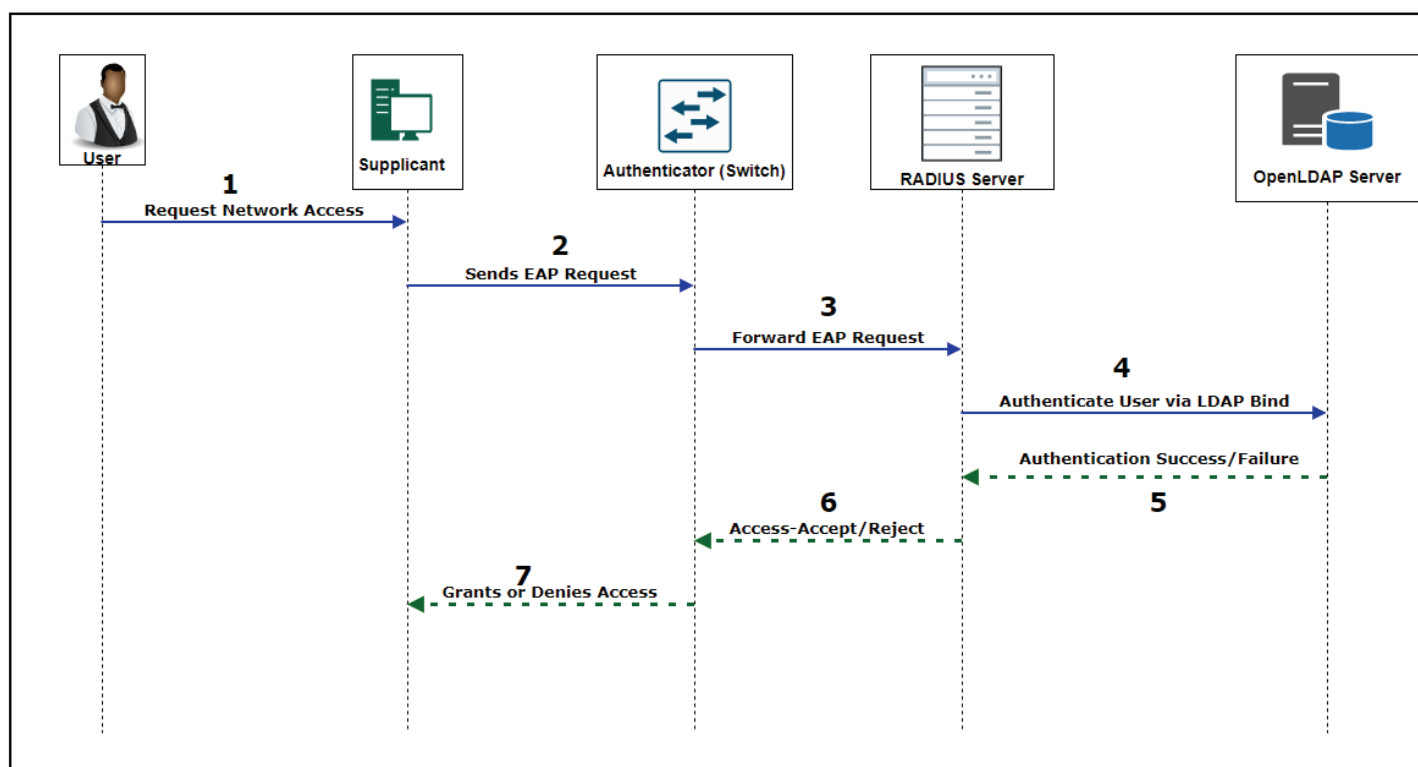


Figure 4: OpenLDAP

this decision, the authenticator (7) either grants or denies network access to the supplicant.

This authentication mechanism enhances network security by enforcing centralised access control, preventing unauthorised access, and ensuring that only authorised users can connect to the network. The integration of RADIUS and OpenLDAP in this process aligns with best practices in enterprise/industrial network security by leveraging directory services for identity management, supporting scalable and policy-driven authentication mechanisms.

IEEE 802.1X & KERBEROS

The diagram represents an IEEE 802.1X authentication process that integrates the Kerberos authentication protocol through a RADIUS server to enforce secure network access control.

The process begins when a user (1) attempts to connect to the network, prompting the supplicant (client device) (2) to send an EAP (Extensible Authentication Protocol) request to the authenticator, which is typically a network switch. The authenticator (3) acts as an intermediary, forwarding the EAP request to the RADIUS server, which is responsible for handling authentication.

Instead of using LDAP for credential verification, the RADIUS server interacts with a Kerberos Key Distribution Centre (KDC) to authenticate the user. The RADIUS server (4) first requests a Ticket Granting Ticket (TGT) from the KDC (5), which verifies the user's credentials and issues the TGT. Using this TGT, the RADIUS server (6) then requests a service ticket specifically for network access. Upon receiving the service ticket from the KDC (7), the RADIUS server (8)

sends an Access-Accept message to the authenticator, including the service ticket. Based on this response, the authenticator (9) either grants or denies network access to the supplicant.

This method enhances security by leveraging Kerberos' strong authentication model, which minimises password transmission and provides mutual authentication between entities, ensuring that only legitimate users gain network access.

NETWORK ACCESS CONTROL (NAC) AND DIRECTORY SERVICES INTEGRATION

In OT environments, particularly power plants, substations, and power delivery networks, the adoption of Network Access Control (NAC) remains limited today. However, looking ahead, NAC has the potential to serve as a critical gatekeeper. By enforcing authentication and posture assessment at the point

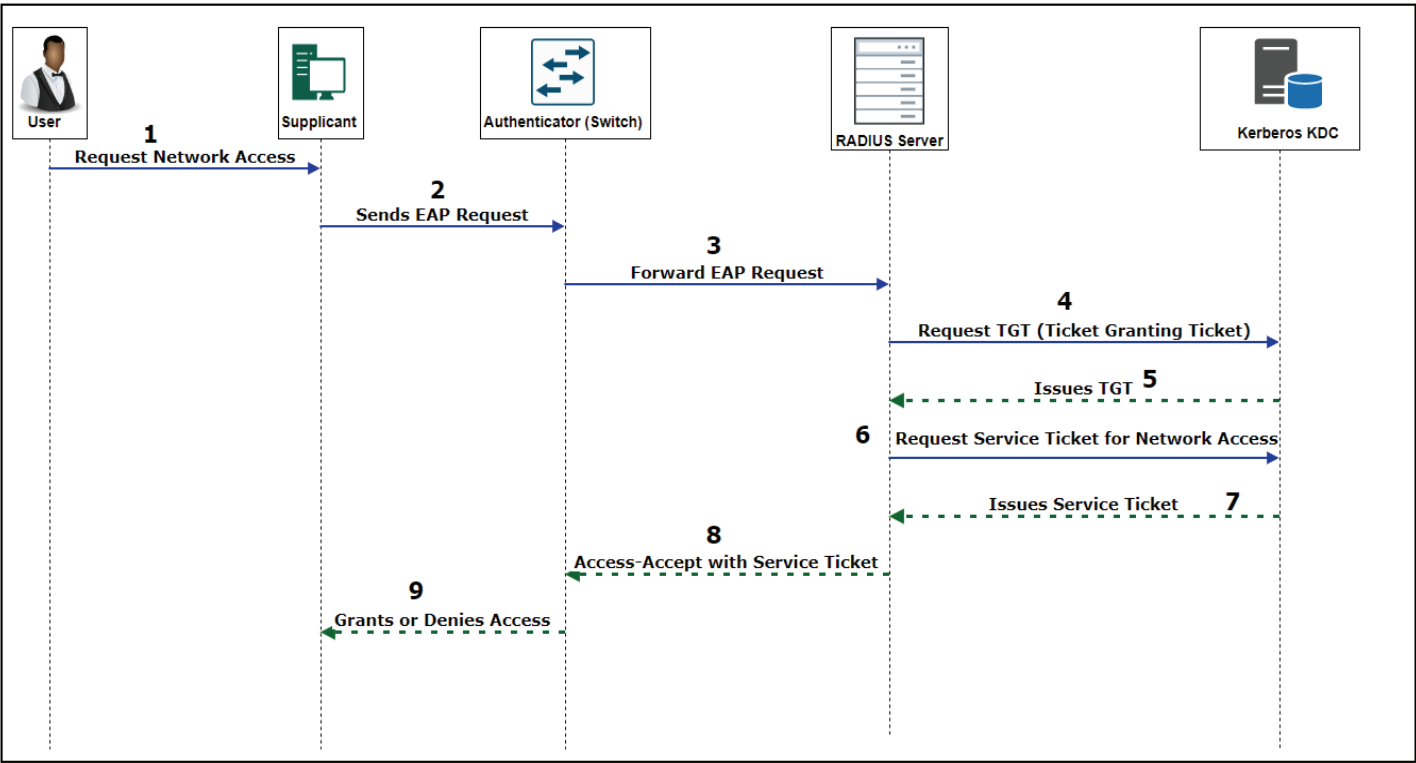


Figure 5: Kerberos

of entry, NAC could ensure that only trusted users and devices connect to sensitive control networks. The technical foundation already exists in open standards, including IEEE 802.1X for port-based access control and the IETF's RADIUS and EAP frameworks for Authentication, Authorisation, and Accounting (AAA).

Where NAC could be transformative in OT is through its integration with directory services. Identity and access management for engineers, operators, contractors, and support staff is typically centralised through Microsoft Active Directory or other LDAP-compliant directories. If applied to OT, NAC integrated with directories could deliver:

- **Unified Identity Enforcement:** NAC policies could leverage existing group memberships, OU structures, and role definitions in the directory. This would avoid duplicating access rules and ensure that admission to substation LANs or plant control networks aligns with corporate identity policies.
- **Granular Role-Based Access:** For example, in the future, a protection engineer in the "Substation Operators" group might be dynamically assigned to a VLAN with restricted access to IEDs, while contractors could be placed in a guest VLAN with restricted access to shared project resources.
- **Dynamic Policy Decisions:** NAC can query the directory in real-time to make access decisions. If a technician's account is disabled or flagged for risk, their connection to a critical SCADA or historian system could be automatically blocked or quarantined.
- **Audit and Compliance:** Because authentication events tie back to unique user identities in the directory,

NAC can help significantly eliminate or reduce the long-standing issue of shared or anonymous device access — a key compliance requirement for the energy sector and other critical infrastructures.

- **Support for Legacy Devices:** Many OT devices, such as IEDs or controllers, do not support 802.1X. In these cases, MAC Authentication Bypass (MAB) can be used as a fallback, allowing device access based on registered MAC addresses. This approach acknowledges legacy constraints while still providing an auditable entry point.
- **Time-Bound Access:** Certain operational requirements necessitate that controllers, vendor laptops, or diagnostic tools connect for a limited period. NAC could be configured to grant time-based access, automatically expiring permissions once tasks are completed, thereby balancing security with operational continuity.

In practice, such a deployment might look like:

1. A device connects to the OT network at a substation or plant.
2. The NAC (via 802.1X supplicant and switch/wireless authenticator) challenges the user or applies MAB for legacy devices.
3. Credentials are passed through RADIUS/EAP (or MAC identity) to the central directory service.
4. Based on group membership, attributes, or device identity, the NAC assigns the connection to the appropriate VLAN (e.g., SCADA network, corporate DMZ, or guest access) or enforces posture remediation.

This forward-looking approach highlights how identity could become

the new perimeter in OT: not just verifying that an authenticated device is connected, but also ensuring its posture is compliant, thereby safeguarding future power generation and delivery assets, as well as other critical infrastructure systems.

RECOMMENDATIONS AND FUTURE DIRECTIONS

To ensure the successful implementation of directory services in OT/ICS environments, organisations must adopt a comprehensive security strategy that addresses both technical and human factors. A critical component of this strategy is security training for administrators, engineers, and end-users. Training programs should encompass:

- multi-factor authentication (MFA),
- role-based access control (RBAC),
- least privilege principles,
- advanced identity federation models.

Additionally, awareness campaigns should focus on mitigating threats such as credential theft, phishing attacks, and unauthorised privilege escalation, which remain significant risks in industrial environments.

Beyond training, organisations must conduct a thorough assessment of their existing IT/OT infrastructure to identify legacy systems and proprietary protocols that may lack native support for modern directory services. Where full replacements are not feasible, middleware solutions or protocol adapters can be deployed to bridge the gap between ageing OT systems and contemporary authentication frameworks.

Furthermore, automated auditing and compliance enforcement tools should

be integrated to continuously monitor access logs, detect anomalies, and ensure adherence to industry standards such as IEC 62443 and NIST 800-82.

Looking ahead, future advancements in directory services for OT/ICS security should prioritise the adoption of Zero-Trust architectures, where authentication is continuous and context-aware, eliminating implicit trust for any device or user.

AI-driven anomaly detection can enhance security by proactively identifying unusual access patterns, privilege misuse, and lateral movement within the network. Moreover, NAC-based identity verification holds potential for decentralised and tamper-resistant authentication, which can ensure that device and user credentials remain secure against forgery or compromise. These innovations, combined with greater industry collaboration and regulatory alignment, will play a pivotal role in protecting OT/ICS networks against evolving cyber threats while ensuring seamless and secure access management across industrial environments.

CONCLUSION

Directory services play a critical role in securing OT/ICS environments by enabling centralised authentication, access control, and identity management. Directory services ensure that only authorised users and devices gain access to critical industrial networks. Their integration with IEEE 802.1X, RADIUS, and TACACS+ enhances security by enforcing stringent authentication policies, reducing the risk of unauthorised access, and mitigating threats such as credential theft, privilege misuse, and insider attacks.

By providing a unified framework for managing identities across distributed OT infrastructures, directory services streamline access governance while supporting compliance with industry standards such as IEC 62443 & 62351, NIST 800-82, and NERC CIP. As the convergence of IT and OT accelerates, traditional perimeter-based security approaches are proving inadequate for safeguarding modern industrial systems against sophisticated cyber threats.

The adoption of scalable, fault-tolerant, and resilient directory services will be essential in protecting critical infrastructure from threats such as ransomware, supply chain attacks, and nation-state cyber warfare. Organisations must adopt Zero-Trust security principles, implement role-based and attribute-based access controls (RBAC/ABAC), and integrate real-time security monitoring to enforce access policies in evolving OT environments dynamically. To ensure long-term security and operational resilience, organisations must prioritise investments in Identity and Access Management (IAM) frameworks, conduct regular security training for OT personnel, and enforce regulatory compliance to align with best practices.

Additionally, leveraging AI-driven anomaly detection, behavioural analytics, and NAC-based identity verification further enhances the security of OT/ICS networks. Ultimately, a proactive and adaptive approach to directory service implementation will be crucial in protecting industrial systems, preventing cyber intrusions, and ensuring the reliability and security of critical infrastructure in an era of increasing digitalisation and cyber threats. **wn**

Note: Throughout this article, the discussion on directory services in OT/ICS environments refers specifically to independent and private directory services, which are architecturally separate from enterprise IT directory systems. This separation is intentional and strategically aligned with the principle of defence in depth. Mixing OT directory services with enterprise identity systems introduces risk and undermines the security segmentation essential to protecting critical infrastructure.



Trusted Execution Environments

- A STEP TOWARDS THE ZERO-TRUST PARADIGM?



Advancements in the fields of telecommunications and computing have catapulted the world into the fourth industrial revolution. This has led to the development of networked industrial control systems, capable of intelligent monitoring and control, known as cyber-physical systems [1].

*By: Dr. Daniel Ramotsoela
Department Of Electrical Engineering
Senior Lecturer
University of Cape Town*

These are engineered systems that seamlessly integrate computational algorithms and physical processes using network infrastructure similar to conventional IT systems. Advancements in the field of cloud computing have also led to the conceptualisation of the cyber-physical cloud (CPC) [2], which enables the outsourcing of computational resources for increased flexibility and cost reduction.

These technological advancements improve efficiency, but this comes at the cost of increasing the system's attack surface. This is particularly concerning because these cyber-physical systems are typically deployed in critical infrastructure applications such as water and electricity. The consequences of successful cyber-security breaches (which have been well documented) thus have devastating economic, social and environmental consequences [3]. Preventative cybersecurity mechanisms alone are therefore not adequate, and a move towards Zero-Trust environments is required to limit the impact of successful breaches.

Zero-Trust is a cybersecurity paradigm based on the principle that neither external nor internal networks should be trusted: "never trust, always verify" [4]. This means that data on the internal network should also be protected and verified. This would practically mean that even if an attacker can bypass the external preventative security mechanisms, they would still be considered an untrusted entity within the internal network, thus limiting the impact of the breach.

An interesting technology related to the Zero-Trust paradigm is the Trusted Execution Environment (TEE) [5]. TEEs reduced the trust boundary of the system to a small hardware enclave within the processor and assume the rest of the system is untrusted. This means that data is encrypted outside the enclave and must be verified before it is used in any processing. In the CPC, for example, this would allow outsourcing of sensitive system processing to the cloud, without the need to trust the cloud provider with your data. Examples of TEEs in practice include Intel SGX (Software Guard Extensions), ARM TrustZone, and AMD SEV (Secure Encrypted Virtualisation).

TEEs, however, do not meet the strict definition of the Zero-Trust paradigm because a portion of the system (however small) still needs to be trusted. For example, in the CPC, cloud providers they use would have to be trusted. The reduction of the trust boundary thus does not eliminate the risks associated with trusting external providers, but it significantly reduces the attack surface. My argument is that this technological innovation represents a significant step in that direction, and it is definitely one to watch as the technology evolves. **Wn**

REFERENCE

- [1] I. Subeh, "Cyberphysicality: Toward a Conceptual Framework for Studying the Fourth Industrial Revolution and its Implications on Business, Communication and Learning," in *The Implementation of Smart Technologies for Business Success*

and Sustainability: During COVID-19 Crises in Developing Countries, Springer, 2022, pp. 721–736.

- [2] V. K. Sehgal, A. Patrick, and L. Rajpoot, "A comparative study of cyber physical cloud, cloud of sensors and internet of things: Their ideology, similarities and differences," in 2014 IEEE International Advanced Computing Conference (IACC), IEEE, 2014, pp. 708–716.
- [3] D. T. Ramotsoela, G. P. Hancke, and A. M. Abu-Mahfouz, "Practical challenges of attack detection in microgrids using machine learning," Journal of Sensor and Actuator Networks, vol. 12, no. 1, p. 7, 2023.
- [4] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, "Theory and Application of Zero Trust Security: A Brief Survey," Entropy, vol. 25, no. 12, 2023, doi: 10.3390/e25121595.
- [5] P. Jauernig, A.-R. Sadeghi, and E. Stapf, "Trusted Execution Environments: Properties, Applications, and Challenges," IEEE Secur Priv, vol. 18, no. 2, pp. 56–60, 2020, doi: 10.1109/MSEC.2019.2947124.



MINE MORE. BREAK DOWN LESS

Detect overheating,
misalignment, and
electrical issues,
before they cause
costly downtime.



FLUKE®

Learn More

Embedding climate change into the DNA of engineering practice



For engineering firms, climate change has been much more than a distant environmental concern for many years. As we design engineering solutions to address complex challenges, advise clients in both the public and private sectors, and seek to future-proof the built environment in which society can thrive, climate change is a defining reality.

*By: Eli Msimanga
Regional Safety, Health, and Environmental (SHE)
Lead, WSP in Africa*

The question of how climate change considerations are embedded into our own operational management frameworks is increasingly central to our credibility, competitiveness, and long-term sustainability.

At WSP, we often emphasise that being a responsible company is not just about what we report in our sustainability reports, but about how those commitments are translated into daily practice. The integration of climate change into management systems cannot be abstract. It must touch the way we work and report, the risks we account for, and the opportunities we pursue.

UNDERSTANDING THE FOOTPRINT

We can't manage what we can't measure. WSP is measured against three ISO standards: ISO 9001:2015 for quality management, ISO 14001:2015 for environmental management, and ISO 45001:2018 for occupational health and safety. Climate change is considered under ISO 14001 and is often framed through the lens of greenhouse gas emissions, waste management and resource efficiency. For an engineering consultancy, our direct (scope 1) emissions are relatively modest because we are not a manufacturing entity.

Scope 2, which includes electricity consumption, is more material. Here in South Africa, where grid power remains overwhelmingly coal-based, we cannot escape the reality that every kilowatt-hour carries a significant carbon footprint.

Although shifts are underway, only 17% of South Africa's electricity comes from low-carbon sources, and household solar PV installations account for 6.8 GW of this. Although we have seen a strong push towards decarbonisation in our energy sector, we must also seek other ways to mitigate the climate impact of our electricity consumption. We view reduced commuting as a positive contributor to lowering our environmental footprint, and this is one of the reasons we have adopted a hybrid working approach.

Scope 3 emissions, linked to our supply chains and business travel, remain relevant but are relatively contained within our business model. Still, they remind us that even simple daily habits, such as how we manage office waste, the lifecycle of products we consume, or our travel choices, form part of the wider emissions story.

RISK AND OPPORTUNITY IN EQUAL MEASURE

Every operational framework must manage both risks and opportunities, and climate change is no exception. For example, South Africa's energy insecurity, which was characterised by loadshedding for over a decade, has been viewed mainly as a power reliability issue. But it is also a symptom of an ageing, coal-dependent infrastructure. Here, the risk of disruption also creates an opportunity: to reimagine power generation.

When we are called to assess whether coal-fired stations can be refurbished or upgraded, the answer is not just about



technical feasibility. As visioneers, we also have an obligation to question whether doing so would perpetuate a carbon-intensive past. Increasingly, the opportunity lies in repurposing such sites into renewable or nuclear alternatives. WSP is already supporting projects in this space, advising on the conversion of an end-of-life coal-fired power station to a small modular reactor (SMR). This underscores how climate considerations are embedded into the choices we make, not only in design but in advising on energy strategy.

FRAMEWORKS THAT DRIVE ACCOUNTABILITY

Our sector benefits from internationally recognised standards and frameworks that ensure climate considerations are not optional add-ons but embedded requirements. ISO standards, environmental impact assessments, and sustainable finance principles are now integral to the typical operating environment for engineering firms and their clients. For example, before significant developments even begin, our environmental teams conduct impact assessments that explicitly consider climate risks and long-term sustainability.

Internally, frameworks such as the Plan-

Do-Check-Act (PDCA) cycle place management at the centre of emissions control and reduction. However, success is not the sole responsibility of leadership. Each person, from switching off unnecessary lights to rethinking material use, contributes to the overall compliance picture. Embedding climate change in operational frameworks means embedding responsibility across every level of the organisation.

THE ROLE OF TECHNOLOGY AND KNOWLEDGE

Digital solutions, including artificial intelligence (AI), are increasingly being applied to help monitor emissions, manage resources, and optimise sustainability outcomes. Yet technology alone is insufficient. Embedding climate change considerations requires equipping people with the knowledge and skills to interpret frameworks, implement changes, and innovate solutions.

For many South African organisations, including ours, the formation of ESG teams often draws expertise from health, safety, legal, and governance functions, as there are usually no specifically trained ESG professionals available. Though this demonstrates a positive shift toward integrated, cross-

disciplinary approaches, it also means that additional learning opportunities may be needed to empower these newly formed ESG teams. For professionals in related spheres to thrive, organisations must support their growth as they work to supplement their existing expertise with new knowledge and skills.

THE ROAD TO 2050

Globally, the Paris Agreement sets a clear ambition: achieving NetZero by 2050. Achieving this requires a relentless focus on continual improvement, measurable progress, and the pursuit of both low-hanging fruit and systemic change. For engineering firms, our role is twofold: to lead by example in our internal operations and to assist clients and governments in designing and delivering climate-resilient, low-carbon solutions.

Embedding climate change into operational management frameworks is not just about compliance; it is also about driving innovation. It is about driving leadership. As engineers, we are trained to solve problems. Climate change is the defining problem of our time, and the extent to which we embed it into our daily practice will define not only the future of our industry but also the legacy we leave for generations to come. **Wn**

Navigating AI, Robotics and Human Skills in South Africa



Artificial intelligence (AI) and robotics are no longer abstract concepts in South Africa's business community. They are here, changing how industries operate and reshaping workforce expectations.

By: Shiksha Benimadho

Accenture Development Partnerships and Talent & Organisation Lead for Africa

Studies show that the next frontier is not about replacing humans with machines, but about designing a Human+ workforce—one that combines the strengths of human creativity and adaptability with the precision, scale, and speed of digital and robotic agents. For South African executives, this presents both opportunity and challenge.

Across sectors, a quiet yet accelerating shift towards automation is underway. South African banks, for instance, are deploying AI-powered chatbots to manage customer service, reduce waiting times, and free up staff for higher-value work. Mining companies, traditionally reliant on intensive human labour, are piloting robotic inspection systems to minimise safety risks in deep-level mines. Even in agriculture, AI-driven drones and sensors are being tested to optimise crop yields, helping farmers mitigate the effects of erratic weather patterns linked to climate change. These are not experiments for tomorrow—they are operational realities today, influencing decisions on cost, risk, and workforce planning.

The South African context, however, adds layers of complexity. Unemployment remains stubbornly high, sitting above 32% in the first half of 2025, with youth unemployment still exceeding 43%. Against this backdrop, conversations about automation inevitably raise concerns about job losses. Business leaders need to acknowledge this tension while also recognising that AI and robotics, when applied responsibly, can unlock new types of work and

stimulate growth. The challenge lies in balancing efficiency with social responsibility, ensuring that technology augments rather than sidelines human potential.

Our research, “Humans, AI, and Robots: The Economics of Reinventing Work and the Workforce,” highlights that blending human and machine work is not universally beneficial. In areas where AI decisively outperforms humans, such as pattern recognition or classification, autonomous systems may be more effective. Conversely, where human judgment, empathy, or creativity are crucial, augmentation is most effective. For South African businesses, this means carefully mapping functions. In healthcare, AI tools are already assisting radiologists by flagging anomalies in scans, but the ultimate diagnosis still requires a doctor's expertise. In retail, automated warehouses can handle inventory management, but human staff remain central to customer-facing interactions.

Economically, the integration of AI and robotics compels a rethink of business models. Local firms are already experimenting with different pricing structures for AI-driven services. Some financial institutions are testing outcome-based models, where costs are tied directly to the results delivered by AI systems, such as fraud detection success rates. Others prefer subscription-style arrangements for predictability. For businesses under pressure from rising electricity tariffs and fluctuating logistics costs, the ability to calibrate technology



investments against return on invested capital is a differentiator. Leaders who understand not only the capabilities but also the economics of AI adoption will be better positioned to extract value without eroding margins.

Yet technology adoption is not only about costs and profits. It has profound implications for workforce skills and societal equity. South Africa's education system already struggles to produce enough graduates with advanced technical skills, particularly in STEM fields. Without urgent investment in reskilling and upskilling, there is a real risk of widening inequality, where a small segment of the workforce thrives in high-tech roles. At the same time, many are excluded from meaningful employment. Encouragingly, initiatives are emerging to close this gap. The Department of Higher Education and Training has begun partnering with private sector players to expand digital skills academies. At the same time, multinational firms operating in South Africa are leveraging global capability centres to provide training not only for their own staff but also for local small businesses that form part of their supply chains.

Trust remains central. Recent surveys of South African executives suggest that while optimism about AI's potential

is high, concerns about bias, data security, and governance persist. This reflects global findings, where leaders emphasise that the full benefits of AI will only be realised if the technology is deployed transparently and responsibly. For businesses in South Africa, building trust is particularly important, given the country's historical inequalities and sensitivities surrounding fairness. Ethical frameworks must therefore transition from theory to practice, guiding not only compliance but also everyday decision-making in recruitment, performance evaluation, and service delivery.

The pace of change is another pressing consideration. Unlike previous industrial shifts, today's wave of AI and robotics is unfolding at unprecedented speed. South African companies that wait for regulatory clarity or perfect certainty risk falling behind. Consider logistics: global competitors are already deploying AI-powered digital twins to simulate warehouse operations, dramatically reducing inefficiencies. If local logistics providers do not adopt similar innovations, they may find themselves outpaced by multinational entrants that can offer faster and cheaper services. The same applies to financial services, where fintech disruptors using AI-driven risk models are expanding access to credit at lower cost. Incumbent institutions cannot afford complacency.

Despite these risks, there is a unique opportunity for South Africa to leapfrog. With its dynamic entrepreneurial ecosystem, the country can become a testbed for AI applications that address distinctly local challenges. In healthtech, AI-driven mobile platforms can expand access to rural patients who struggle to reach urban clinics. In education, adaptive learning platforms powered by AI can help bridge gaps in under-resourced schools. In agriculture, combining robotics with indigenous knowledge could offer sustainable solutions to food security. These examples illustrate that the Human+ workforce is not only about corporate profit but also about broader societal benefit.

For business leaders, the imperative is clear. AI and robotics should not be viewed as a future inevitability but as a present strategic choice. The question is not whether to adopt, but how—and at what pace—to ensure both competitiveness and social impact. Those who invest in thoughtful integration, who reskill their people, and who design with responsibility at the centre, will not only improve their bottom lines but also contribute to a more resilient South African economy. The art of the possible is already here; what matters now is how decisively and responsibly we act. **Wn**

Trust nothing, verify everything

- WHY ZERO TRUST IS ESSENTIAL FOR CLOUD SECURITY



The shift to remote work and cloud storage has rendered traditional security strategies, designed for a world of office buildings and centralised networks, ineffective. With users working remotely, data stored across multiple cloud platforms, and systems accessed from a variety of devices and locations, the traditional model of defending the perimeter has become less relevant.

By: Kumar Vaibhav

*Lead Senior Solution Architect
Cybersecurity at In2IT*

Zero Trust architecture provides a smarter and more secure approach. It doesn't rely on location or assumed safety. Instead, it treats every user, device, and request as potentially untrusted, continuously verifying before granting access. This isn't a brand-new idea. It's a maturing, tested security model that's proving essential for protecting cloud environments.

WHEN ASSUMPTIONS BECOME A THREAT

In a perimeter-based model, users and systems inside the network were considered safe. Once they were "in," they could move freely. That worked when everything was centralised, but in modern environments, where users log in from anywhere and data lives in the cloud, that assumption becomes dangerous.

If an attacker gains access through a single compromised account or device, they can often move laterally across the network undetected. Zero Trust counters this by removing default trust. Every request is evaluated based on who is making it, the device being used, and the conditions surrounding the access, whether it's a familiar location, a secure device, or typical behaviour. The proactive approach ensures that potential threats are identified and addressed before they can cause harm.

This requires coordination between identity systems, access policies, and endpoint protection, something that IT providers are uniquely equipped to manage. They tighten security and design it intelligently around business operations.

IDENTITY AND CONTEXT, NOT LOCATION

In a Zero-Trust framework, identity becomes the foundation for access decisions. Rather than relying on whether a user is inside the network, the system asks: who is this, what are they trying to access, and should they be allowed to?

Context matters. A staff member logging in from a managed laptop during business hours might be granted access immediately.

However, accessing the same account from an unfamiliar IP address or an unmanaged device could trigger step-up authentication or a block. It's not about making life harder for users; it's about making smarter access decisions in real-time.

Building an adaptive access system can be complex, especially for businesses that have a mix of legacy applications, SaaS platforms, and diverse user groups. This is where IT providers play a vital role. They help integrate identity providers, develop tailored policies, and implement risk-based access controls without compromising operational efficiency.

SECURING REMOTE WORK WITHOUT CREATING BOTTLENECKS

Remote and hybrid work are here to stay, and they've exposed the limits of traditional tools like Virtual Private Networks (VPNs). VPNs often provide broad access, create performance issues, and increase risk by allowing too much trust too quickly.



Zero Trust replaces this with application-specific access. Instead of connecting to the entire network, users are granted access to only what they need based on verified conditions. It's faster, more secure, and more aligned with how people work today.

For businesses unfamiliar with these models, IT providers help simplify the transition. They know how to modernise access without disrupting productivity and can provide recommendations tailored to a company's size, structure, and cloud maturity. Their expertise and guidance can make the adoption of Zero Trust a smoother and more manageable process.

LIMITING THE BLAST RADIUS WHEN BREACHES HAPPEN

No security model can prevent every threat. But the ability to contain an incident can make a massive difference. Zero Trust limits how far an attacker can move, even if they manage to get in.

Through techniques like micro-segmentation and least-privilege access,

Zero Trust ensures that a compromised account doesn't open the door to the entire network. For example, if a phishing attack exposes a user's credentials, strict access boundaries and real-time monitoring help ensure that exposure is contained and identified quickly.

To get this right, organisations need more than software. They need strategic guidance to map out their environment, identify high-risk access paths, and define policies that align with business roles and processes. Experienced IT providers bring this visibility and help businesses avoid common missteps that lead to gaps or friction.

WHY IT PROVIDERS MAKE THE DIFFERENCE

Adopting Zero Trust isn't about buying a single tool. It's about building a coordinated security model that touches identity, endpoints, applications, and networks. It's a strategic shift, and for many organisations, trying to do it alone leads to delays or partial solutions.

IT providers bring structure to the

process. They help prioritise rollouts, starting with high-risk users or critical systems. They provide the technical depth needed to integrate tools, define realistic access policies, and ensure systems are continuously monitored and tuned. Just as importantly, they help manage change by educating internal teams, reducing resistance, and ensuring that security enhancements don't block business goals.

For many companies, the difference between Zero Trust, which works in theory, and Zero Trust which works, lies in the guidance and partnership of an experienced provider.

Security built for the way we work today Zero Trust doesn't assume safety; it demands proof. By verifying every request based on identity and context, it delivers smarter, more resilient protection for cloud-first operations. As businesses continue to evolve, adopt new tools, and support flexible work, Zero Trust offers a clear path forward. And with the right IT partner, it becomes not just possible but practical. **wn**

Navigating the complexities of AI in the GRC landscape



Governance, Risk, and Compliance (GRC) is an essential part of sustainable business, helping organisations manage risk, stay up to date with legislation, and ensure that processes are well-managed. One of the biggest challenges, however, has always been finding the right skills, as well as adapting to the changing regulatory landscape.

*By Ryan Boyes
Governance, Risk and Compliance Officer
Galix*

Artificial Intelligence (AI) is transforming GRC processes by enabling enhanced efficiency, improved risk detection and stronger compliance frameworks, but this comes with cost implications. It also has the potential to add further layers of complexity, particularly in terms of technical aspects, while ensuring transparency and accountability.

This is where an expert partner can be invaluable, by providing guidance, skills and experience to help organisations develop AI strategies, manage compliance risks, and optimise AI-driven processes for maximum impact.

Addressing the challenges of AI in GRC When it comes to integrating AI into GRC frameworks, several factors are stumbling blocks. These may include data quality issues, uncertainty created by a constantly shifting regulatory framework, and the high costs of implementing the latest technology.

It is essential to develop clear AI strategies to optimise costs and minimise unnecessary expenses, and to have a well-defined business case for technology before investing significant time and energy into its adoption. It is also essential to invest in data quality.

Ultimately, the success of an AI-driven compliance strategy depends on the right combination of technology, expertise, and knowledge of the compliance landscape. It is essential to invest in upskilling employees and hiring the right talent, but beyond that, partnering with an external compliance

specialist can help to bridge skill gaps and drive effective implementation.

The upfront investment in AI can be substantial; however, businesses must consider the long-term benefits, including improved compliance monitoring, faster risk identification, and reduced operational expenses. Organisations can balance expenses by adopting AI in phases, prioritising high-impact areas, and leveraging cloud-based AI solutions to reduce infrastructure costs.

Strategies for effective AI-driven GRC Machine learning and Natural Language Processing (NLP) enhance predictive analytics by identifying patterns in large datasets, flagging potential compliance risks, and automating monitoring processes.

These capabilities allow organisations to shift from reactive to proactive risk management. However, since AI systems rely on high-quality data to achieve this, data quality is crucial. It is essential to ensure that robust data governance practices are in place and that data intended for AI purposes is accurate, complete, and reliable. It is also necessary to ensure AI models are continually updated to avoid both bias and inaccuracy.

Additionally, AI-driven compliance must align with evolving ethical guidelines and regulations. Expert partners can help organisations interpret complex regulatory requirements, implement ethical AI governance, and ensure that

AI applications meet global compliance standards. For AI-driven GRC frameworks to be effective, organisations must maintain transparency in decision-making processes. Implementing explainable AI models, establishing audit trails, and incorporating human oversight ensure accountability and build trust in AI-driven compliance solutions.

THE PATH FORWARD FOR AI-DRIVEN GRC

AI presents significant opportunities for enhancing GRC processes, but its successful implementation requires a strategic approach. By addressing key challenges, investing in the right expertise, and adopting best practices for AI-driven risk management, organisations can achieve greater compliance efficiency and resilience in an increasingly complex regulatory landscape. **wn**



Crabtree

THAT WHICH IS BUILT SOUNDLY ENDURES WELL

EMBRACE A NEW LEVEL OF
REFINEMENT & MAKE A
STATEMENT



NEW ARRIVAL - CLASSIC FERRO GRAIN RANGE

Empowering The South African Dream

- UNLOCKING THE POTENTIAL OF SA INCORPORATED ("SA INC") THROUGH AFFORDABLE ELECTRICITY ENERGY ACCESS



This article examines the South African Incorporated (SA Inc.) perspective as a vital framework for unifying the nation and addressing the country's pressing socio-economic challenges.

*By: Professor Vally Padayachee,
CEng; CD(SA); MBA; MSc (Eng); Pr CPM; Pr Cert
Eng; EDP (Wits).*

With approximately 60% of the population grappling with poverty, and unemployment, the SA Inc. mindset emerges as a clarion call for hope and collaboration, urging citizens to actively engage in forging a brighter future.

Central to this discussion is the electricity sector, highlighted as a critical pillar for economic and social development. We examine how innovative mechanisms, such as "willing buyer, willing seller" and competitive bidding in renewable energy auctions, can enhance revenue generation for Eskom and municipalities, provide significant relief to large power users, and mitigate the anticipated impacts of the EU-imposed Carbon Border Adjustment Mechanism ("CBAM") taxes and the current debilitating high USA tariffs being levied on SA goods sold in the USA.

Furthermore, the article examines how the SA Inc. mindset can evolve into a broader South African Dream, similar to the American Dream, galvanising the populace to transcend individual interests in favour of collective progress. Drawing parallels with the historical recoveries of nations like Germany and Japan after World War II, and the visionary leadership of Singapore's late and longest-serving post-independence Prime Minister Lee Kuan Yew, it emphasises the importance of unity and collaboration in overcoming adversity. By addressing the challenges in the electricity sector and promoting the principles of energy democracy, access,

and sustainability, this piece illustrates how the SA Inc. mindset framework can empower citizens and foster a vision of sustainable, inclusive progress. Ultimately, it advocates for a concerted effort among all South Africans to create a society where everyone has the opportunity to dream, thrive, and contribute meaningfully to the nation's collective success.

INTRODUCTION

The South African Incorporated (SA Inc.) perspective is a critical concept that holds tremendous potential for shaping the future of South Africa. As the nation stands at a pivotal crossroads, the urgency for hope and collaboration has never been more pronounced. With around 60% of the population grappling with poverty, inequality, and unemployment, every citizen must engage actively in collectively forging a brighter future. The SA Inc. framework serves as a unifying vision, promoting shared responsibility and common aspirations for progress.

This article will explore how the electricity sector emerges as a vital pillar of economic and social development. Utilising innovative mechanisms such as "willing buyer, willing seller" and competitive bidding in renewable energy auctions can enhance revenue generation for Eskom and municipalities, provide significant relief to large power users, and help offset the impending EU-imposed CBAM taxes and high US tariffs on imported South African goods.



THE CURRENT STATE OF AFFAIRS

South Africa's present reality is steeped in significant socio-economic challenges. The ongoing electricity crisis, characterised by high electricity prices, frequent load reduction and inefficiencies, profoundly impacts our economy and communities.

This crisis arises from a complicated history marked by apartheid and colonialism, which has entrenched systemic inequalities.

The staggering statistic that around 60% of the population is affected by poverty, inequality, and unemployment underscores the immediate need for tangible solutions. Additionally, South Africa's Gini coefficient of 0.63—indicative of extreme income inequality—highlights a substantial divide between wealthy and impoverished sectors of society.

This urgent environment creates a pressing need for hope that can galvanise individuals and communities to rise above their circumstances.

THE ROLE OF UNITY

A cornerstone of the SA Inc. framework is unity. It emphasises that actual progress can only be achieved when all citizens come together, transcending personal interests for the greater good. This perspective instils a sense of community and encourages every South African to take an active role in shaping the nation's future.

By collaborating towards shared goals, we can cultivate an environment in which sustainable development flourishes, achieving real progress that uplifts everyone as a cohesive unit.

THE ELECTRICITY SECTOR AS A PILLAR FOR DEVELOPMENT

The electricity sector is fundamentally linked to the broader development of South Africa. It serves as the backbone for economic growth, allowing businesses to operate, communities to thrive, and individuals to enhance their overall quality of life. Let us not forget that "electricity" as a commodity is a public good and must be treated as such.

The SA Inc. vision recognises that addressing the electricity crisis, including energy poverty, is directly related to the nation's progress. By confronting these challenges head-on, South Africa can unlock its potential for growth, innovation, and inclusive development.

THE IMPACT OF RENEWABLE ENERGY PROCUREMENT

Renewable energy auctions, combined with competitive bidding, represent one of the most promising pathways to a sustainable energy future. These initiatives can significantly lower electricity costs, attract investments, and reduce our carbon footprint amid looming EU tariffs.

a) Financial Benefits

Engaging in competitive bidding for renewable energy yields substantial financial benefits for Eskom and municipalities. Auctions can attract a diverse range of participants, creating price competition that may lower electricity costs for consumers while enhancing revenue streams through successful bids.

b) Offsetting CBAM Taxes

Proactively acquiring renewable energy sources provides a compelling defence against impending CBAM tariffs. By increasing their share of renewables in the energy mix, Eskom and municipalities can effectively reduce carbon emissions, thereby minimising costs associated with EU carbon tariffs while strengthening market competitiveness.

c) Development of Local Renewable Markets

Through participation in renewable energy auctions, Eskom and municipalities can stimulate local renewable energy markets. This engagement encourages investment in clean technologies, creating job opportunities and fostering entrepreneurship.

A NOBLE ROLE FOR ESKOM AND MUNICIPALITIES

Eskom and municipalities have a unique opportunity to redefine themselves as champions of sustainable development and social equity rather than merely electricity providers.

By engaging in initiatives such as renewable energy, they can lead the charge toward a sustainable energy future, combating climate change while addressing systemic inequalities.

ADDRESSING UNIQUE CHALLENGES

As South Africa grapples with multiple crises—ranging from socio-economic issues to shifts in the energy landscape—it is crucial for Eskom and municipalities to embrace innovative solutions that reflect the SA Inc. principles.

The establishment of a new electricity market in April 2026 presents both challenges and opportunities. Stakeholders must embody principles of transparency and accountability, ensuring equitable benefits for all South Africans.

THE NEED FOR AN SA INC. MINDSET

The SA Inc. mindset must serve as a rallying cry for citizens to prioritise collective progress over individual interests. This mentality echoes the spirit that fuelled post-war recoveries in nations like Germany and Japan. By fostering interconnectedness, we reinforce the idea that communities thrive when they work together.

THE SOUTH AFRICAN DREAM: A VISION FOR NATION-BUILDING

The SA Inc. mindset can evolve into a powerful South African Dream—an inspiring vision that emphasises shared opportunities, social justice, and economic empowerment. This dream encourages citizens to engage in their

communities actively and fosters a cohesive society.

CONCLUSION

The South African Incorporated (SA Inc.) mindset offers a powerful opportunity for the nation to transcend its historical challenges and strive for a vision rooted in equity, justice, and progress. By embracing the South African Dream, citizens can cultivate a collective identity that inspires action and renewal.

While the challenges confronting South Africa are significant, the potential for transformation lies within the collective will of its people. By investing in one another's success, we pave the way for an inclusive future.

Let us harness the potential of the electricity sector and the spirit of collaboration to ensure that every citizen has the opportunity to dream, thrive, and contribute meaningfully to the collective success of our great nation.

Together, we can build a future where every South African aspires to a life of dignity, opportunity, and hope—a future that honours the resilience and spirit of all its people. **wn**



A single flaw can break an entire system

IN ENGINEERING, PRECISION IS NON-NEGOTIABLE.

THE SAME PRINCIPLE SHOULD APPLY
TO YOUR DATA SECURITY AND PRIVACY PROTOCOLS.



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

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

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

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

CONTACT US FOR A DISCUSSION REGARDING YOUR NEEDS TODAY



Jodi Poswelletski

DIRECTOR
SPECIALIST IN DATA PRIVACY AND POPIA

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

Clifton Motshepe

ASSOCIATE

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



SAIEE OFFICE BEARERS



V RAMNARAIN
2025 SAIEE PRESIDENT



P MADIBA
DEPUTY PRESIDENT



PROF W CRONJE
SENIOR VICE PRESIDENT



J MOTLADIILE
JUNIOR VICE PRESIDENT



P MOTSOASELE
IMMEDIATE PAST PRESIDENT



PROF P NAIDOO
HONORARY TREASURER

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

PAST PRESIDENTS

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

FELLOWS

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

SENIOR MEMBERS

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

MEMBERS

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

SECTION CHAIRPERSONS:

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

CHAPTER CHAIRPERSONS:

Cybersecurity Chapter:	M Taljaard	csc@saiee.org.za
Entrepreneurship Chapter:	Y Mabuto	entrepreneurchapter@saiee.org.za
Financial Services Chapter	P Naidoo	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

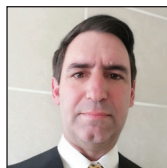
E | scc@saiee.org.za



Vaal Centre

Chairman | Vacant

E | vc@saiee.org.za



Western Cape Centre

Chairman | Heinrich Rudman

E | admin.wcape@saiee.org.za

OCTOBER 2025

CALENDAR

01/10/2025	Smarter Mobility Africa Summit
07/10/2025	Power Systems Protection
14/10/2025	Incident Investigation and Management (Root Cause Analysis)
15/10/2025	Management of Electricity Distribution Assets Section 1 – Powerline Asset Data
15/10/2025	Photovoltaic Solar Systems - Gqheberha
21/10/2025	Hack Lab
22/10/2025	High Voltage & Engineering Conference
23/10/2025	Legal Liability: Mine Health and Safety Act
28/10/2025	SANS 10142-1 Edition 3.2 2020
30/10/2025	Technical Report Writing
30/10/2025	New Engineering Contract (NEC)

NOVEMBER 2025

04/11/2025	Finance Essentials for Engineers
06/11/2025	Block Chain and Money
07/11/2025	Road to Registration for Engineering Candidates
11/11/2025	Fundamentals of Medium Voltage Protection
12/11/2025	Introduction to 5G Communication Networks
14/11/2025	Professional Registration with ECSA for Mature Candidates
18/11/2025	Fundamentals of Developing Renewable Energy Plants
18/11/2025	Operating Regulations For HV/MV Systems - ORHVS
19/11/2025	Constructions, Regulations from a legal perspective
26/11/2025	Cable Jointing, Termination & Testing



SAIEE Sections, Chapter & Centre Events

SAIEE Academy Online Training

SAIEE Academy Classroom Training

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



artsolarTM

local | powerful | guaranteed



ARTsolar proudly stands for **African Renewable Technologies**. Established in 2010 and 100% locally owned. As pioneers in the industry, we provide trustworthy, dependable and cutting-edge turnkey solutions.

We manufacture from a silicon based crystalline cell to module, assemble components and test offshore modules according to global standards. We are a certified OEM for various Tier 1 Manufacturers and an approved distributor of renewable energy products.

**Effortlessly Switch to
State-of-the-ART!**

CONTACT US

+27 31 100 1019 | +27 11 568 2008
+27 83 574 8984 | info@artsolar.net

