

OMICRON Magazine



THE NEW CMC 500:
SIMPLY REVOLUTIONARY.



DEAR READERS,

At OMICRON, pushing the boundaries of technical feasibility to deliver top-notch value to our customers with our innovative solutions is part of our DNA. In the latest edition of the OMICRON Magazine, we're excited to introduce the newest member of the OMICRON product family: the CMC 500. This test set is lighter and more compact and significantly outperforms our flagship CMC models, offering cutting-edge features and setting a new benchmark in protection testing.

As the CMC 500 Product Manager, I'm eager to share my insights into the comprehensive and challenging process behind this engineering masterpiece. We've developed new analog output modules with unprecedented capabilities, significantly enhancing the versatility of this test set. We've implemented extensive cybersecurity measures to ensure top-tier performance alongside simplified workflows and enhanced user safety features.

If you'd like to learn more, turn to our cover story on page 6, "Simply revolu-

tionary. Revolutionarily simple," where you'll discover how our dedicated team crafted this innovative test set from the ground up.

This edition also delves into the PARADIMO 100, our cutting-edge solution for ultra-high-frequency partial discharge (PD) monitoring in GIS and GIL systems. Imagine a world where potential electrical insulation failures are detected early, ensuring the safety and reliability of your assets. With smart edge computing capabilities, it continuously monitors PD activity, automatically detects and classifies insulation defects, and provides instant alerts. Explore this comprehensive article on page 18 to see how PARADIMO 100 can transform your approach to PD monitoring.

As we investigate advancements in PD monitoring, we also turn our attention to vital infrastructure security. In the heart of Norway, Glitre Nett's engineers faced an enormous challenge: defending their infrastructure against complex cyber threats.

Publisher

Responsible for content

Editorial team and implementation

Picture credits

E-mail to the editorial team

OMICRON electronics GmbH, Oberes Ried 1, 6833 Klaus (AT)

OMICRON electronics GmbH

up! consulting, Industriering 10, 9491 Ruggell (FL)

OMICRON electronics GmbH, iStock.com (p. 5, 14–15, 24–25, 31–38, 40, 43–48), Shutterstock (p. 11, 22–23), Schweitzer Engineering Laboratories (p. 15–17), Siemens Energy (p. 28), Hikari Trading Co., Ltd. (p. 30), Glitre Nett (p. 32–33), Adobe Stock (p. 42–43)

magazine@omicronenergy.com

Our StationGuard intrusion detection system (IDS) proved its mettle, detecting every simulated attack with precision. Learn the gripping details of this real-world test and discover how innovation is shaping a secure future on page 32.

The stories in this edition reveal how OMICRON is not just keeping pace with

the industry but driving it forward, and I hope you find them inspiring.

Yours sincerely,



Stephan Geiger

CMC 500 Product Manager and
Product Management Lead, OMICRON

*«We pushed the
CMC 500 to the
limits of what is
technically feasible.»*

Stephan Geiger

TABLE OF CONTENTS



- 6 Simply revolutionary.
Revolutionarily simple.**



11 CMC SWIFT + CPOL3

Achieve maximum efficiency and flexibility with our wiring tests



12 United in power quality

FRANEO PQlyzer – Our new instrument transformer solution for power quality applications



14 Love at first sight

Why a protection expert can no longer do without RelaySimTest



18 Meet PARADIMO 100

Our ultra-high-frequency partial discharge monitoring solution for GIS and GIL



22 CMCheck RE

A tool for granting grid access to photovoltaic installations



**24 Managing complexity,
recognizing relevance**

Firmware updates for a secure and reliable energy supply



**28 CPC 100 – A valuable training
tool for SIEMENS Energy**



30 On site: OMICRON in Japan

Teruyuki Harada from Hikari Trading Co., Ltd. shares his insights into the power sector with us.



32 Preparing for cyber attacks

How Glitre Nett found the right intrusion detection system for their networks



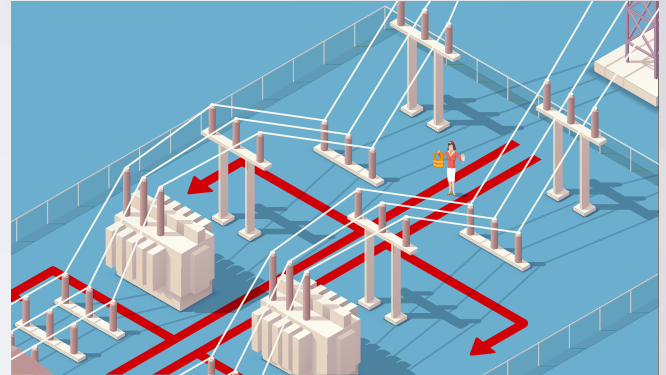
38 Generative Artificial Intelligence in the power industry

An exploration of generative artificial intelligence (GenAI) and how it can enhance our work and the power grid's efficiency



42 Say farewell to the time-consuming search for circuit breaker reference data

Welcome to the Circuit Breaker Testing Library (CBTL)! Our field-proven circuit breaker testing library provides you with reference values at the touch of a button



44 Life vests for test sets?

Why we're constantly thinking about improving safety measures



46 No protection testing, no kick-off

The importance of testing interconnection relays



49 StationScout navigates new waters

Support for IEC 104 RTU / Gateway testing



50 Celebrating 40 years of OMICRON

Four decades of innovation and customer loyalty



KNOWLEDGE



SUPPORT



INNOVATION



QUALITY

SIMPLY REVOLUTIONARY, YET REVOLUTIONARILY SIMPLE.



Introducing the CMC 500, the latest modular test set from OMICRON that elevates protection testing to a whole new level. Our development team invested extensive time, energy, and effort into designing the CMC 500 with one goal in mind: to ease the burden of utilities, service providers, and industrial companies. Now let's take you behind the scenes to explore the design process with the R&D team.

Stephan, OMICRON is setting a new benchmark in protection testing with the CMC 500. How were you able to accomplish this?

Our goal was to build on the success of our highly popular CMC 356 protection relay test set, so we started by engaging directly with utilities and service providers. With over 15,000 CMC 356 units in use — many for over 15 years — we knew the importance of understanding the real-world challenges that our customers face during protection testing and their day-to-day operations. We asked key questions: Are the amplitudes, the number of current and voltage channels, and the output power of the CMC sufficient? What additional tasks do protection testers have beyond protection testing itself? Is there anything we could streamline or eliminate? In many discussions with our customers,

«The CMC 500 is the result of decades of experience of collaborating with our customers in the field, **giving us a clear understanding of what the relay test set of tomorrow must achieve.**»

Stephan Geiger,

CMC 500 Product Manager and Product Management Lead, OMICRON



we also explored future possibilities by thinking outside the box. The feedback we gathered was invaluable in shaping the next generation of our protection relay test set.

So, what did their wish list look like?

It became clear that many customers wanted an even more compact and

lightweight device for field use without compromising output power. For example, when testing synchronizers, there's a demand for six voltage outputs. Some customers requested more current outputs to test busbars protection or three-winding transformers, while others desired higher current amplitudes to test the differential

characteristic of 5A relays at elevated levels or to verify the signal paths to the relay through a primary injection. Additionally, many testers wanted to know if their relay was connected to the correct current transformer core, if the latter's transformation ratio was accurate, and if the breaker connected to the relay was tripping correctly. ▶

«**It's frustrating to drive for hours only to realize you've left behind a critical piece of your test equipment.**»

Florian Fink,

Product Manager and Application Expert,
OMICRON

Discover all the advantages of the CMC 500:

 omicron.energy/new-cmc



These insights made it evident that we needed to design a field-ready device that not only could test protection relays, but also had the capabilities required for testing other key assets in the protection chain — a truly versatile system. Given our customers' diverse needs and requirements, we decided to move away from a "one-size-fits-all" approach and instead developed a platform with five different variants, each tailored to specific application areas.

Beyond versatility, what other aspects were most important to the customers you spoke with?

One critical issue that emerged from our discussions was user safety during testing. Customers have become more focused on complying with safety standards, such as EN 50191 in Europe, which outlines the requirements for constructing and operating both fixed and temporary electrical test installations. In response, we've put significant

thought into simplifying the rewiring process during testing, streamlining operations, and enhancing user safety.

Another key area of concern for our customers has been cybersecurity. The requirements have increased dramatically in recent years, and unsurprisingly, much of the expertise from our cybersecurity products has been incorporated into the CMC 500. This has led to it setting a new benchmark in cybersecurity standards.

Additionally, we recognized the importance of ensuring that existing test plans for Test Universe and RelaySimTest would also be compatible with the CMC 500. We made this a priority, knowing it would be crucial for our customers' ongoing operations.

«The CMC 500 is a wise financial investment for today's testing tasks. If requirements change in the future, the device can easily be upgraded.»

Christopher Pritchard,
Product Management Lead, OMICRON

How did you incorporate such extensive requirements into a single product?

We designed and built the device from scratch, including entirely new current and voltage generators. I'm amazed by how much we've been able to pack into our convertible generator modules. Their output accuracy is exceptionally high. They're extremely powerful with amplitudes of up to 300 V and 30 A and frequencies reaching 5 kHz, a technical achievement we take great pride in. For instance, our high-current module can output 60 A per channel, and in a single-phase setup, it can generate up to 180 A. By paralleling the outputs of all modules, we can even generate up to 450 A. We came up with an intelligent thermal concept to squeeze all these features into as small a space as possible and completely redesigned the housing.



«Whenever several groups are working in a substation, **ensuring the safety of the testing personnel and everyone else on site is critical.**»

Marcus Stenner,
Application Expert, OMICRON

We racked our brains to develop a test set that could enhance our customers' ease of use while maximizing user safety. All the terminals are located on the front, reducing tripping hazards, and we implemented a multi-stage safety system to minimize electrical risks. This includes an INTERLOCK key, an operating mode button and – coming soon – an external emergency switching off button with clearly visible signal lights.

Packing such a powerful and versatile system into a compact, lightweight product was no small task for our developers. However, with many years of experience, including the development of the CMC 356, the team was more than up to the challenge.

How did you oversee such a complex and wide-ranging development program?

The project certainly was highly complex and required the seamless cooperation of everyone involved – from the developers of the electronic assemblies and mechanical engineers to representatives from various ▶



disciplines, including purchasing, manufacturing, production, test equipment, embedded software, client software, and product management. To handle this complexity, we enhanced our project management approach by adopting agile methods, that were primarily used in software development. This ensured team coordination was as efficient as possible.

This high level of collaboration was extremely important when it came to cybersecurity. During our conversations, it became clear that many customers would eventually operate both conventional and digital installations side-by-side. A future-proof test solution is one that reliably supports emerging digital technologies. Therefore, we knew we had to consider the implications of cybersecurity from the very beginning. After all, Cybersecurity by Design goes beyond implementing safeguards into hardware and software; it also influences the allocation

of responsibilities, internal workflows, and approval processes. Fortunately, cybersecurity has always been a priority for us, particularly since our customers scrutinize anything with an Ethernet port (laughs).

Did everything go according to plan during development?

We certainly pushed the boundaries with this project. We had to overcome several challenges to meet all the technical and functional requirements, and there were some unexpected expenses

along the way. For instance, additional board revisions were needed as several components were discontinued during the COVID pandemic. However, we took the time necessary to resolve these issues because one thing was always clear to us: we wouldn't compromise our standards of quality and reliability. Our goal was to set a new industry benchmark with the CMC 500, and I'm proud to say that we achieved everything we set out to accomplish.

Thank you for speaking with us. ■

«The CMC 500 stretched us to the limits of what is technically feasible.»

Stephan Geiger,

CMC 500 Product Manager and Product Management Lead, OMICRON

«A tall iron gate beside a small hedge is useless. It's always the weakest link in the chain that defines the level of cybersecurity.»

Cristian Marinescu,

Embedded Software Development Lead, OMICRON

Read more about the versatility, work security, cyber security and future security of the CMC 500:

 omicron.energy/cmc-story





CMC SWIFT + CPOL3

Achieve maximum efficiency and flexibility with our wiring tests

Using CMC Swift, you can quickly control your CMC test sets remotely from your smartphone without sacrificing your freedom of movement. The latest version of CMC Swift enhances your workflows, especially when performing wiring tests, with our new handheld device for testing polarity and wiring: CPOL3.

Time-saving combination for wiring tests

CMC Swift lets you remotely use your test set's voltage or current outputs to produce a DC-free saw-tooth signal for wiring tests. This waveform prevents unwanted magnetization of the energy transducer. The three-phase polarity check is also supported with CPOL3, enabling simultaneous polarity checks and phase identification. The result is fewer test steps with improved test quality and efficiency.

CMC Swift for remotely controlling a CMC test set

CPOL3 features a high-contrast OLED display that is readable from any angle and can detect polarity test signals

with a saw-tooth waveform, as well as DC and AC signals. It also measures voltage levels (real RMS), enabling simultaneous polarity checks and burden measurements. An „oscilloscope“ mode displays the measured signal waveform, providing greater insight into errors. A low input impedance mode (LoZ) is also available for situations where coupled signals interfere with the measurement.

Wiring and polarity checks with CPOL3

CPOL3 allows you to perform a wide range of testing tasks with greater

efficiency and convenience. For more details about CMC Swift and CPOL3, visit on our website:

omiconenergy.com/cpol3

DOWNLOAD NOW

Try CMC Swift now and leave your laptop behind for easier checks in the future:

omiconenergy.com/cmcsswift

LISTEN TO THE PODCAST

Interested in this topic?



Then check out our podcast episode "CMC Swift: Developing a mobile test app for CMC test sets". Scan the QR code or visit:

omicon.energy/episode64



UNITED IN POWER QUALITY

FRANEO PQlyzer – Our new instrument transformer solution for power quality applications

One of the secrets of a happy marriage is sharing common interests and complementing each other in meaningful ways. The FRANEO 800 main device and the EIC1 accessory, combined with the new FRANEO PQlyzer Instrument Transformers' software, is a partnership that does just that. This new combination is the perfect match for wideband accuracy instrument transformer measurements for power quality applications. So, now it's time for us to celebrate this pair in style with "something old, something new, something borrowed, and something blue"!

A true partnership

In a world rapidly approaching renewable energy generation, precise power quality measurements are key. Instrument transformers (ITs) play a vital role

in the power quality measurement chain. The wideband ratio and phase accuracy of these ITs need to be evaluated across their entire frequency range. That's where the solid partnership our new FRANEO PQlyzer offers truly shines.

The FRANEO 800 is well-known, or "something old". It's the industry standard for ensuring power transformer windings' mechanical and electrical integrity. Its sweep frequency response analysis (SFRA) is a testament to its reliability and a cornerstone of transformer diagnostics.

On the other hand, the Electronic Impedance Converter EIC1 and the FRANEO PQlyzer software are "something new", that bring wideband ratio measurements for instrument trans-

formers to the table. It extends the capabilities of instrument transformer testing with dedicated software that streamlines workflows. Comprehensive reporting capabilities for detailed test reports solidifies the partnership between the old and the new.

Together, these two products form a union that's much more than a marriage of convenience. It's a bond that promises a future with guaranteed precision and reliability.

Sharing is caring

Our shared knowledge, is "something borrowed". It's the foundation of our partnerships. We bring decades of expertise to the table, ensuring that the solutions we provide are effective

*«By ensuring the accuracy of your power quality data, provided by the instrument transformers, **you can make informed decisions for optimizing grid performance, maximizing asset life, and enhancing overall power system reliability.**»*





LEARN MORE

You can find more information about this new product here:



omiconenergy.com/eic1

and imbued with years of industry leadership wisdom.

Why are instrument transformer wideband accuracy measurements important? Because the impact their ratio or phase accuracy has on the harmonic frequency range can be significant. Distorted data received by power quality measurement devices can lead to:

- › Misinterpretation of power quality events
- › Ineffective implementation of corrective actions based on faulty data
- › Increased risk of equipment damage due to undetected power quality issues

“Something blue” refers to the signature blue color of our Devices. However, the FRANEO 800 PQlyzer product is more than a tool; it’s a statement for testing instrument transformers’ wideband accuracy. A statement that says, “We care about the future of your assets, and you’re getting more than a measurement; you’re getting quality assurance that meets the new wideband classes introduced by the IEC 61869 standard’s 2.0 Edition.”

A union for the future

As we look to the future, the union between the FRANEO 800 and EIC1 represents a new chapter in electrical testing, a chapter where the old and the new come together to create something extraordinary. The

FRANEO PQlyzer combines advanced hardware and user-friendly software, empowering you to perform comprehensive wideband tests on your instrument transformers. By ensuring the accuracy of your power quality data, provided by the instrument transformers, you can make informed decisions for optimizing grid performance, maximizing asset life, and enhancing overall power system reliability.

Join us in celebrating this perfect combination by embarking on a journey towards a future where precision is not simply a goal but a reality. ■

Watch the video about FRANEO PQlyzer:

youtu.be/8UU1WIY52cgg



LOVE AT FIRST SIGHT

Why a protection expert can no longer do without RelaySimTest

Time flies: This year, the RelaySimTest simulation software is celebrating its 10th anniversary! Ronald Jogaib has been a devoted fan from the very beginning. In Brazil, he used RelaySimTest to test the behavior of protection systems in transmission grids and to determine the optimal dimensioning of protection components. Today, he is on the other side of the world, evaluating the capabilities of modern protection relays in Australia. There was no question about choosing the perfect software solution for that particular task.

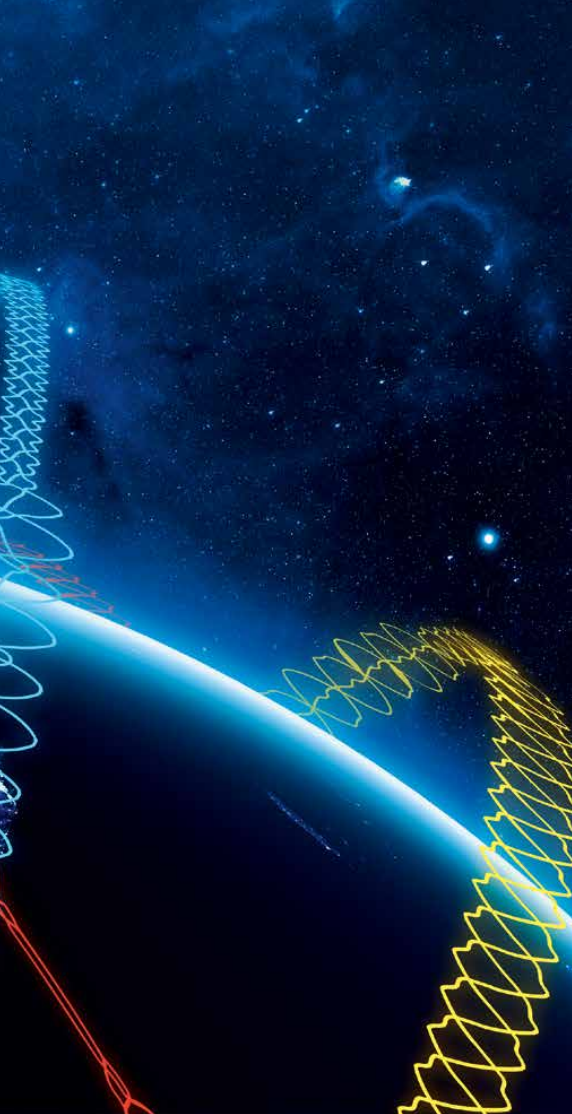
Ronald, you have been using RelaySimTest for a long time and never tire of emphasizing how much you like the software. Why is that?

Ronald Jogaib: RelaySimTest allows you to examine complete protection systems in greater depth. It adds influences that are present in a real system to the test, which is the most important aspect of protection testing for me.

Recreating complex, realistic scenarios helps me understand the protection system's behavior in detail. With this software, I can easily test how indi-

vidual protection functions or entire protection devices behave under difficult conditions: with current transformer saturation, with inrush currents when a transformer is energized, in the event of fault currents with varying resistance at the fault location, or with power swings.

In my opinion, many problems in the protection system simply cannot be detected with static, parameter-based tests. There are still many people responsible for protection who only test protection in the "traditional way". I believe this approach requires some



«If the software is not intuitive,
it definitely was not made
by OMICRON. **I love its
ease of use.**»



Ronald Jogaib,
Application Engineer – Protection,
Schweitzer Engineering Laboratories

rethinking. Of course, it is important to monitor relay characteristics. However, I have found that incorrect protection actions cause most shutdowns due to problems with the settings, logic, or equipment dimensioning.

Can you think of an example of this?

I remember that a circuit breaker tripped when a transformer was energized, even though a fault had not occurred. With RelaySimTest, we could see that DC components on two phases caused a current transformer to saturate when the shunt reactor was energized. Thanks to the simulation, we recognized that the CT used was dimensioned too small and did not transfer the current correctly during the energization process. ▶

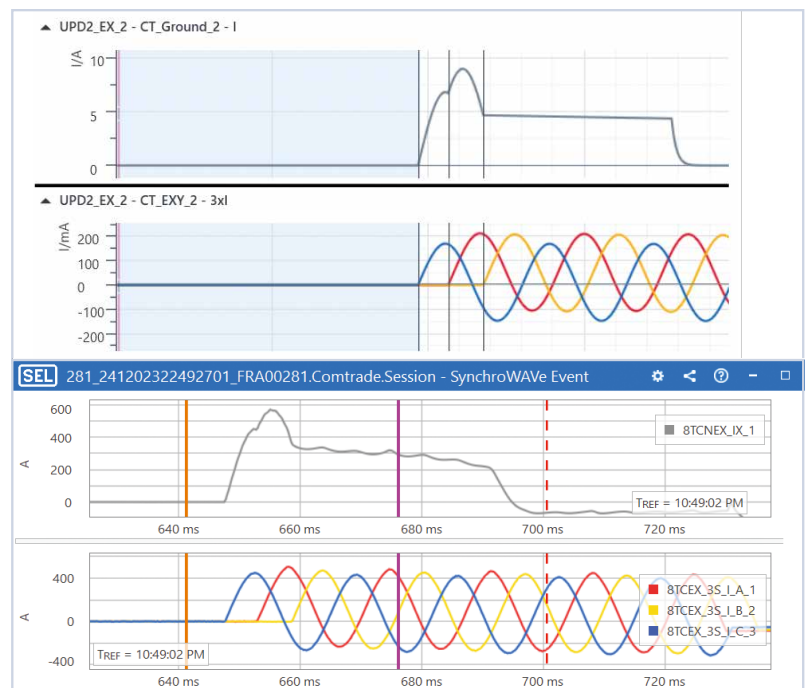


Image 1: Exactly as predicted: The simulation of a shunt reactor energization demonstrates the precision of RelaySimTest. On the top, the currents of the saturating current transformer are calculated with RelaySimTest. The real fault recording of the relay is on the bottom for comparison.

We then simulated other real faults that had occurred in the past and compared the calculated values with the real ones. It was really amazing how precisely the voltages and currents from the simulation matched the real circumstances (image 1 on page 15). That's why we started using RelaySimTest to dimension our current transformers correctly.

Another example I recall is obtaining the best philosophy to protect an autotransformer bank. The software's ability to simulate internal faults in an autotransformer clearly demonstrates the different results between sensitive earth fault protection and transformer differential protection according to the ampere-turn balance or Kirchhoff's principle. This enabled me to adapt my protection concept to my transformer bank.

Finally, I have fond memories of using RelaySimTest with the Digital Twin during a commission application. Our utility's busbar protection received a

new line transmission, and I was able to test this new bay completely from home – in my pajamas! (laughs) I then sent out the new settings of the tested relay. This allowed the commissioning team on site to be sure that the relay settings and logic were correctly defined, allowing them to turn their focus to the cable connections.

You can actually use the software to determine the entire current and voltage behavior without purchasing a license. This means that RelaySimTest can also be used as an effective offline tool to explain unique processes in the protection system. For example, I showed my teammates the phase shift of a transformer with a delta-wye winding and the effect of in-feed and outfeed for external short circuits in line transmissions. So, I can only encourage all those responsible for protection to download the software and use it!

Were you able to understand the software right away? Modern

protection systems can become quite complex, with numerous influencing variables and interactions – especially with the growing number of regenerative feeders in the grid.

I would say RelaySimTest is an easy-to-understand solution for a very complex topic. I love the simplicity of the software. I didn't need any training and could teach myself everything I know. I sent a few final questions to OMICRON and got an answer immediately. That was it. I've had different experiences with other software solutions in the past: Even after two days of training, it was so complicated and confusing to enter data, start a simulation or close a circuit breaker that I lost interest. I also paid for the training with my own money, making it doubly frustrating.

To be honest, in day-to-day life you often don't have time to deal with different software solutions in detail. You have to be able to use these tools properly in a short window of time. Fortunately, this is the case with

Image 2: When he was in Brazil, the self-described devoted fan hung the RelaySimTest poster on his wall. RelaySimTest also helps him keep track of things in his new home country of Australia.



OMICRON. In other words: If the software is not intuitive, it definitely was not made by OMICRON.

What I also find fascinating about RelaySimTest is that normally, protection engineers find it difficult to provide all the necessary data for test software so it can realistically simulate the processes in transient systems. This is where the OMICRON test solution is truly unique: Just a few parameters, which can usually even be taken from the nameplate, are enough to produce an excellent simulation that comes very, very close to reality. That's why when it comes to RelaySimTest, there's no alternative for me. In my opinion, a comparable solution in today's market doesn't exist.

Today, as an application engineer with a relay manufacturer, you deal with different topics than before. Why have you remained loyal to the software?

Yes, I have a different job. However, RelaySimTest is also a significant

benefit to us as a manufacturer. I use a system simulation for our customers to demonstrate how our protection devices behave during faults in IEC 61580 environments. For example, if saturation is present (image 3). Or I show them how a communication failure in which the merging unit no longer sends Sampled Values streams does not immediately lead to protection tripping. Furthermore, the protection device does not block anything, and it reliably detects a fault and triggers protection when communication is restored. This is very reassuring for our customers. During some customer presentations, I was so enthusiastic that I was even asked whether I wanted to sell the relay or the software (laughs).

And I also find the way you're able to handle these simulations to be amazing. For example, when I output test signals via GOOSE and Sampled Values, I can simply change the data streams of the CMCs by graphically opening or closing circuit breakers. It's not neces-

sary to manually adjust individual bits in the data streams.

It's simply fun to work with OMICRON. I don't just mean the hardware and software. The support provided by the experts really adds exceptional value to my work in addition to their excellent testing solution.

This of course has to do with personal relationships and trust. What changed after you moved to another continent?

The country and the company may have changed, but the cooperation I receive from OMICRON is still fantastic. They always strive to maintain a deep customer relationship. You can feel that, and it's great. If I need help with a situation, I e-mail the support team and quickly receive a thorough answer. Or, I simply call them and we talk about the issue directly. It's the same here in Australia as it used to be in Brazil.

With surgical precision, the OMICRON specialists have supported me through challenging situations with the Sampled Values configuration and synchronization I was responsible for during setup. I was even able to contact the support team during the Easter holidays. An OMICRON colleague I was in regular contact with in South America, still supports me today with solid explanations from the other side of the world. These are the real highlights for me.

Thank you very much for the interview!

Thanks for allowing me to talk about this fantastic software that's helping to elevate the knowledge of protection engineers. 🟡

Image 3: Ronald Jogaib uses RelaySimTest to demonstrate to his customers the correct behavior of SEL protective devices in case of a fault.



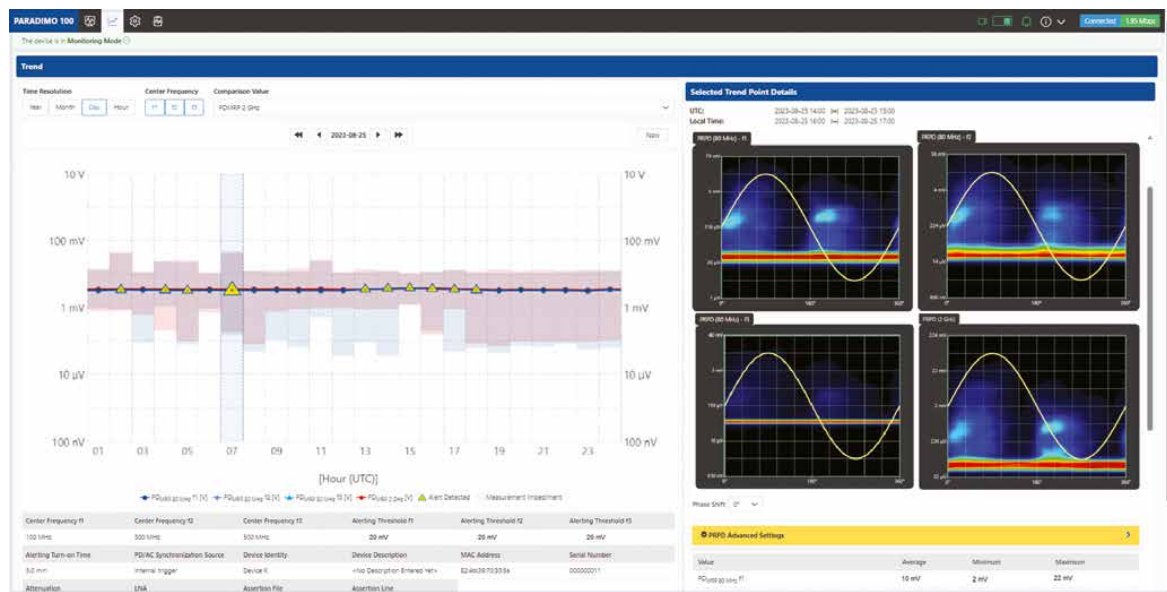
MEET PARADIMO 100

Our ultra-high-frequency partial discharge monitoring solution for GIS and GIL

Partial discharge (PD) activity in Gas-Insulated Switchgear (GIS) and Gas-Insulated Lines (GIL) is a critical warning sign of a potential catastrophic failure in the electrical insulation. Immediate action is required to prevent such failures. Sensitive PD diagnostics can detect typical insulation defects, such as free metallic particles, particles on insula-

tion, sharp protrusions on high-voltage electrodes, or loose GIS/GIL parts.

According to the CIGRE Technical Brochure 654, continuous PD monitoring in the ultra-high frequency (UHF) range for GIS/GIL ensures the detection and interpretation of signals from incipient PD defects.



The trend overview of recorded PD activity shows PD signal levels over specific time periods (year, month, day, hour).





This allows asset managers to take prompt and appropriate actions to prevent equipment malfunctions.

A complete monitoring solution for GIS/GIL

PARADIMO 100 is our new smart edge computing device that continuously monitors PD activity in GIS and GIL. It automatically detects and classifies the type of insulation defect in your assets and generates alerts for reliable risk assessment.

PARADIMO 100 simultaneously monitors PD activity across ultra-high frequency (UHF) ranges using pre-installed sensors in GIS and GIL systems. Wideband and medium-band UHF filters ensure optimal signal-to-noise ratios, providing greater measurement sensitivity and reliable assessments in noisy environments.

Remote data access

A convenient web user interface allows easy network access from a PC or tablet computer for remotely configuring ▶

DID YOU KNOW?

CIGRE's Technical Brochures 654 and 933 recommend using UHF sensitivity checks, PD signal attenuation measurements, and profile evaluations to set the optimum signal amplitude threshold value for UHF sensors. These criteria help define the PD monitoring system's response when threshold levels are exceeded. Additionally, accurate and reliable automated algorithms for PD defect-type recognition algorithms are essential to minimize false alarms and detect critical defects. PARADIMO 100 meets these requirements effectively.

Additionally, the technical brochures recommend combining UHF PD measurements with monitoring to detect and identify developing faults early, thereby preventing failures in GIS. We offer our UHF 800 system for UHF PD measurements, which is ideal for routine factory testing, on-site commissioning, and periodic in-service measurements. For continuous UHF PD monitoring, we provide the PARADIMO 100. Please contact us for more information.

measurement and alert settings, as well as viewing real-time PD data and recorded trends.

Monitor specific sections or entire GIS/GIL systems

PARADIMO 100 devices can easily be relocated to monitor PD activity in different areas of your GIS or GIL. Multiple PARADIMO 100 devices can also be connected in series via a fiber-optic network. This setup enables multiple monitoring points, facilitates PD activity trending, and automatically classifies defect types for reliable risk assessment of your entire GIS or GIL.

PARADIMO 100 key benefits:

- › Peace of Mind – Receive automatic alerts and reliable defect classification to assess risks and avoid potential failures.

- › Minimal Operator Intervention – The system records, saves, and automatically evaluates the monitoring data, generating alerts when predefined limits are exceeded.
- › Convenient Web User Interface – No additional software is needed on a PC or tablet. The Web interface provides easy access for configuring settings, viewing real-time PD data and reviewing recorded trends.
- › Built-in PD Expertise – You don't need to be a PD expert to interpret the results. The system detects and automatically classifies all PD-related defects, ensuring accurate risk assessment. ■

More information at

 omicronenergy.com/paradimo100



LISTEN TO THE PODCAST

Interested in this topic?



In Episode 76 of our Energy Talks podcast series, partial discharge (PD) expert Caspar Steineke explores the advantages of PD monitoring for GIS and GIL and explains how PARADIMO 100 ensures reliable insulation defect detection and risk assessment.

Scan the QR-Code or visit:



 omicron.energy/episode76

WATCH OUR VIDEOS AND LEARN ABOUT PARTIAL DISCHARGE TESTING



Partial discharge (PD) is both a predominant cause and a reliable indicator of insulation defect development in electrical equipment, which can eventually lead to failure. Learn more about PD in our six-part video series, Essentials of Partial Discharge Testing (available in English). This informative video series highlights various aspects of PD testing on medium-voltage and high-voltage electrical equipment.

Caspar Steineke, PD expert and co-developer of our MPD PD testing technology, presents each video and covers topics such as the importance of PD testing, when and how it is performed, how to overcome the effects of external noise during PD measurements, and how to analyze and interpret PD data to prevent insulation failure and costly electrical equipment

outages. Lastly, Caspar presents the benefits of using our MPD 800 for complete and reliable PD testing.

Learn about the essentials of PD testing

Scan the QR code and watch all six videos.

- › Video 1: The Importance of PD Testing
- › Video 2: When to Measure PD
- › Video 3: How to Measure PD
- › Video 4: Minimizing External Noise
- › Video 5: Analyzing PD Data
- › Video 6: Discover MPD 800 for PD Testing

 omicron.energy/essentials-pd





CMCheck RE

A tool for granting grid access to photovoltaic installations

An industry in transition

Renewable energy has been growing at a remarkable rate in recent years. However, there's still a lot of untapped potential in this sector. To further accelerate growth, we need to address several challenges, including grid access, bureaucratic hurdles, and a shortage of skilled labor.

The impressive growth of renewable energies is largely due to companies specializing in installing renewable power plants and systems, and connecting them to the public grid. With a constant influx of orders and new projects, there's an increasing need for highly skilled personnel and effective testing solutions to meet this demand.



Technician testing a photovoltaic installation



CMCheck RE lightens the load



Simple, quick, and cost-efficient: The CMCheck RE test software delivers the exact functions needed to test grid access for renewable energy sources. It pairs seamlessly with the affordable CMC 310 test set, renowned for its portability and ease of use.



Targeted and effective: Preselectable test templates for all relevant connection standards ensure that necessary values are recorded and reduce manual configuration. Clear test reports are also generated, focusing solely on the information required for certification.



Intuitive and easy to use: The CMCheck RE user interface is designed to align with the test procedures' sequence, using terminology familiar to field technicians. This makes the software easy to use, even for occasional users.



Minimal training: No special training is needed to use CMCheck RE. Technicians can quickly learn how to use the test software with our free application videos, offering flexibility for training new staff or refreshing existing skills.

Fully equipped for the future

Given the rapidly evolving nature of the renewable energy sector, it's crucial to be prepared for any scenario. New testing requirements may emerge, or a company's range of services may expand as it grows. The CMC 310 is

designed to cover all these possibilities. If needed, it can be upgraded to the CMC 353 and used with Test Universe software for additional functions, such as Q-V protection, overcurrent protection, or distance protection. ■

Find out more about CMCheck RE and renewables by scanning the QR-code or visiting:

[omicron.energy/lom-protection](https://www.omicron.energy/lom-protection)



MANAGING COMPLEXITY, RECOGNIZING RELEVANCE

Firmware updates for a secure and reliable energy supply

Firmware has a decisive influence on the functionality of devices in secondary technology. It serves as the interface between hardware and software, enabling the control, management, and interaction of highly complex components.

Many of us have mixed feelings when we receive a notification that a firmware update is available for our smartphone. We might be unsure if we'll get used to the update, whether everything will work, and whether we can still access all our data. At the same time, we expect better security and look forward to improvements, as firmware updates are also intended to fix known security vulnerabilities and protect sensitive data.

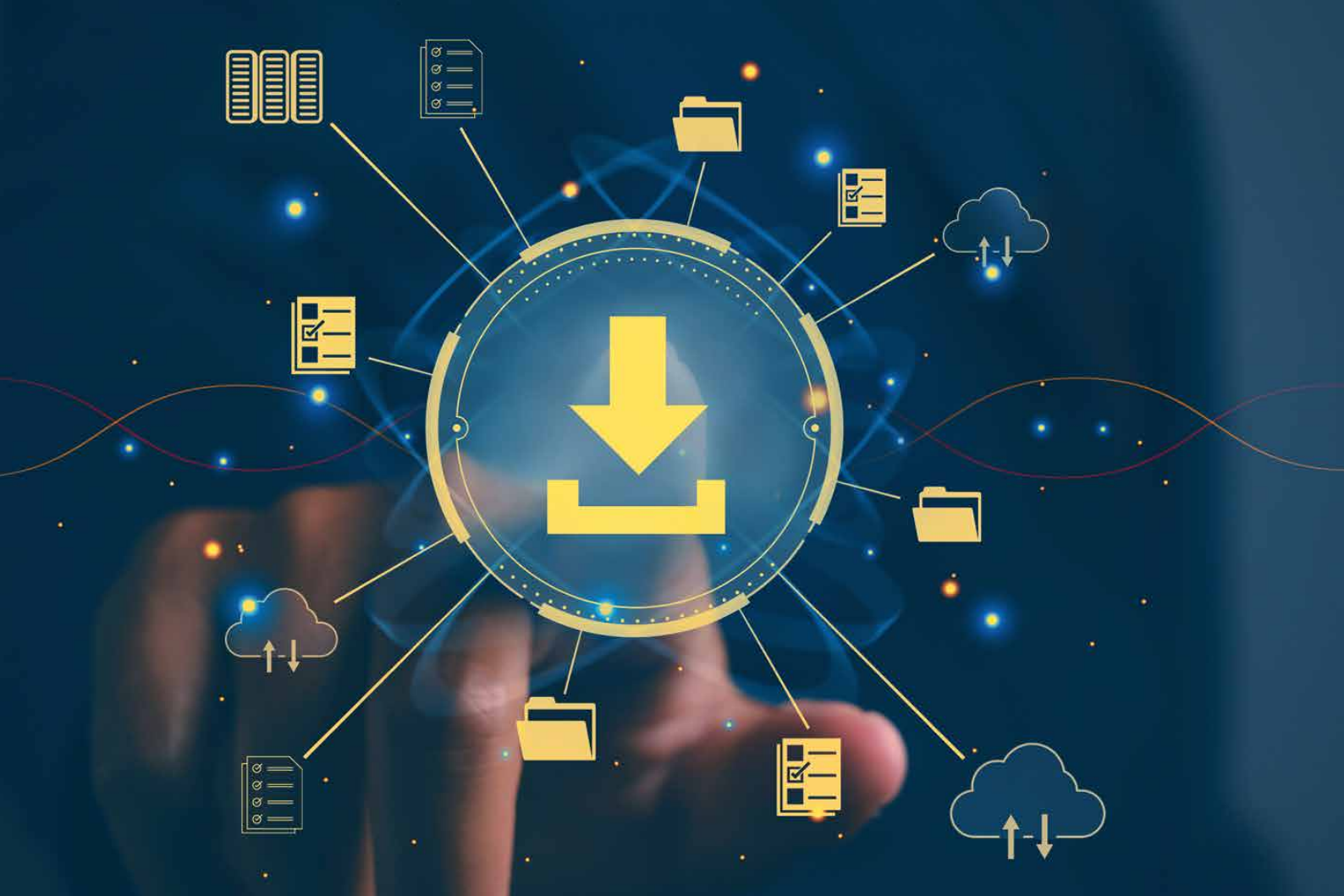
Challenges, legal requirements, and the future of cybersecurity

Firmware updates are also relevant for secondary systems when it comes to tackling one of the biggest challenges of all—protecting against cyberattacks. Authorities and industry associations have realized this and responded by issuing various rules, guidelines, and recommendations for action to identify potential threats, assess risks, and promptly fix any loopholes.

Examples of German and international legislation and guidelines:

- › NIS2
- › ITSIG 2.0
- › ISO/IEC 27001 and 27019
- › IEC 62443
- › BSI Standard 200-3
- › IT security catalogs in accordance with Article 11 Para. 1a/b EnWG (Energy Industry Act)

This legislation addresses all aspects of IT, OT, and installation security, guaranteeing optimum security and ensuring the grid can operate without interruption. Some legislation centers on individual measures such as firmware updates. We also expect to see more specific and detailed provisions that may result from the EU's response to NIS2 requirements, which will go into effect at the end of 2024.



Firmware updates: Delivering security and functionality with a comprehensive approach

From a legislative perspective, the primary aspects of firmware updates are a reliable power supply and protection against cyberattacks. There are many reasons why it is essential to keep firmware up to date:



Security: Security patches are used to close security loopholes that have been identified.



Troubleshooting: Software errors or functional problems in earlier versions are fixed.



More functionality: Updates enhance or optimize features in line with current market and customer requirements.



Interoperability: Updates may be necessary to ensure communication and interoperability between different network devices.

Risk assessments, approval processes, and comprehensive testing

Various factors will determine if a firmware update needs to be carried out on a larger scale.

First, power supply facility operators have to consider whether or not a new firmware release will require action on their part. Asset inventory solutions such as ADMO can help by providing a fast and comprehensive overview of all the firmware versions being used by individual IEDs.

Following that, a multi-stage risk assessment, or risk analysis, is needed to assess the likelihood of firmware defects and the potential damage they could cause. The approval and rollout process also plays a significant role in the overall assessment.

During the approval process, it's critical to decide if it's necessary to carry out comprehensive approval testing prior to the rollout. Updates can potentially create new risks after they're carried out if the substation or individual devices are not ►

«Tools such as ADMO help maintain an overview of devices and firmware while speeding up risk analyses. Substation owners and operators also need to understand the significance of firmware updates and take a proactive approach to the challenges they pose.»



functioning correctly. This is why many operators carry out extensive approval testing ahead of time to verify functionality.

These tests require a lot of time and expertise and typically consist of iterative processes such as laboratory tests, field tests, individual tests or site acceptance tests (SAT).

Currently, general standards or guidelines for this type of testing have yet to be created. So naturally, the question of which tests need to be carried out and at what scale arises. The following approach has become an industry standard:

1. Troubleshooting tests

These tests ensure that the update will fix all errors as planned.

2. Data integrity tests

Checks the integrity of the saved data and settings to rule out damage to the data or changes in the data model.

3. Functionality tests (algorithm)

Verify that all device functions are working correctly. Testing is performed on essential and unique functions, such as logical links, that enhance the functionality of protection devices.

4. Compatibility and interoperability tests

Ensure that the firmware is compatible with all hardware and software components it is meant to interact with.

5. Regression tests

Check if the update unintentionally impacts other parts of the firmware. Protection devices often have multiple firmware versions for different areas, such as the algorithm and communication, which must work together.

6. Communication tests

Test communication interfaces to verify proper connectivity with other devices in the network, such as SCADA systems or IEDs.

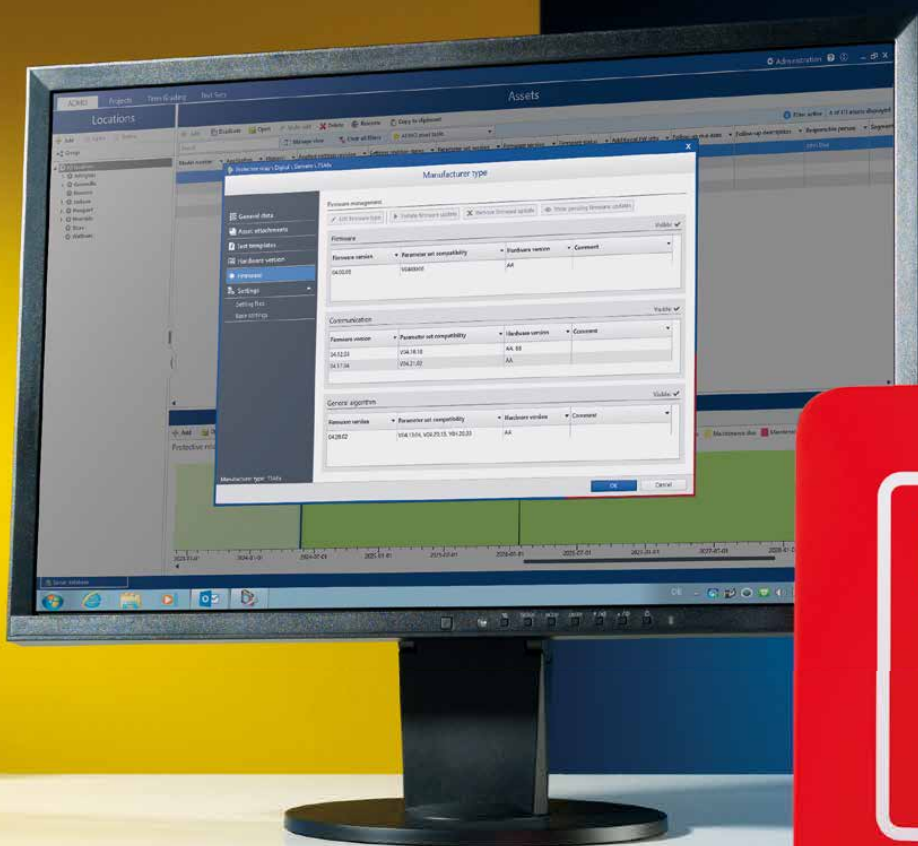
7. Performance tests

Check whether the update has led to changes in device behavior related to signal processing and reaction time.

8. Cybersecurity tests

Runs security checks on the firmware to rule out new vulnerabilities. This may consist of penetration tests on known vulnerabilities.

Many operators may be unable to carry out these extensive tests, and if updates occur infrequently, it can become problematic.



Outsourcing approval testing in one of the early stages, such as laboratory testing, might be one way of addressing a lack of resources. Taking this approach could also have a positive influence on the risk assessments of power supply facility operators, who currently avoid approval testing.

Power supply facility operators can support one another by making their testing insights and assessment processes available to other operators. However, approval testing should be carried out according to guidelines or by certified test centers to ensure corresponding quality standards.

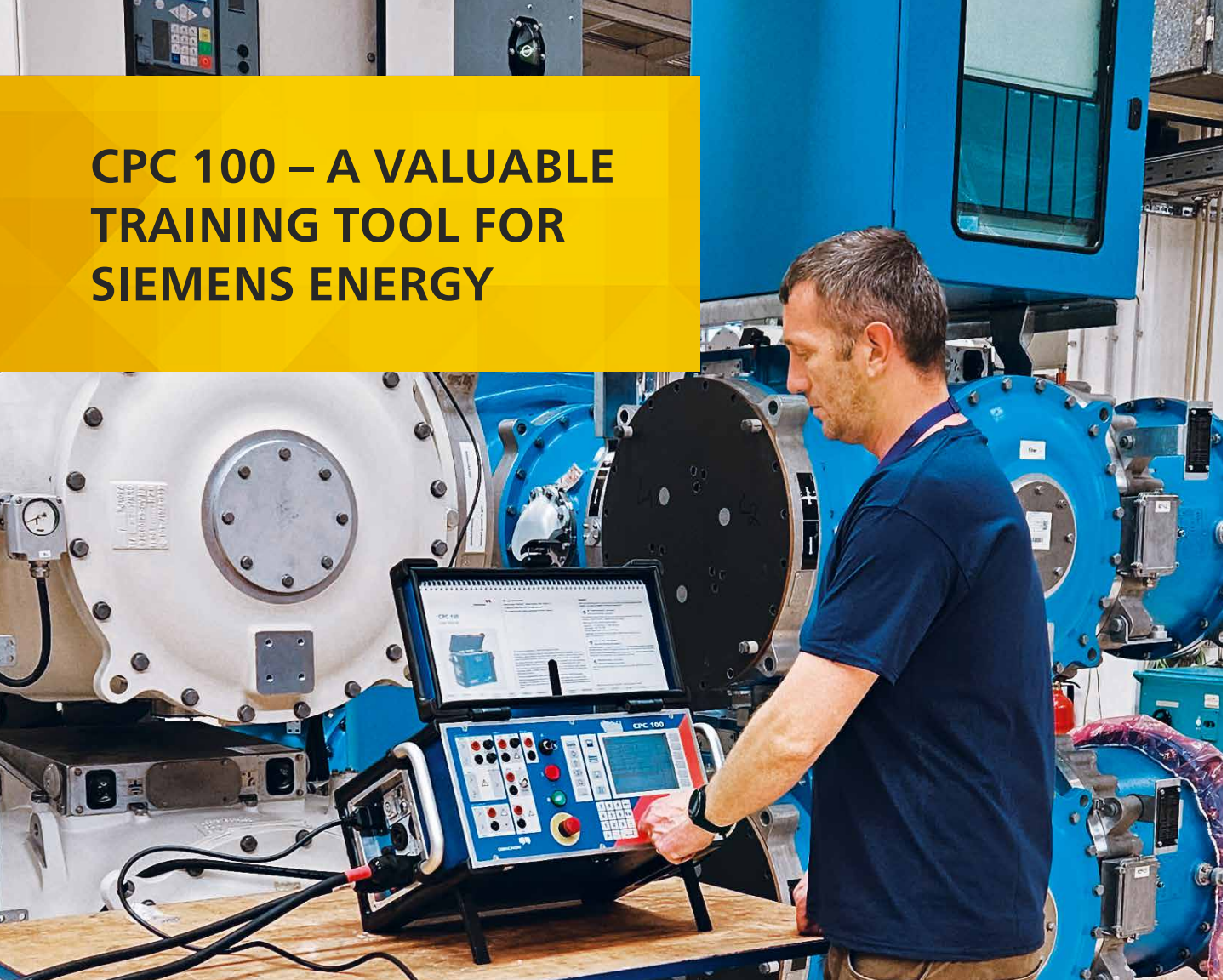
We are here to support you

Thorough, systematic testing is essential for ensuring new firmware is secure and error-free. An automated test system can accelerate and standardize the entire process. We are here to support you with testing solutions, methods, and asset inventory tools for approval tests on new firmware.

One thing is certain: firmware updates are a vital component for guaranteeing the reliability and security of our energy supply. Multiple challenges are involved in firmware updates, ranging from network security to complying with legal provisions. Comprehensive testing prior to implementation is a must. This guarantees functionality and reliability and prevents new vulnerabilities from being introduced. Utilities need adequate resources to do this, and outsourcing approval testing can reduce their resource demands.

Tools such as ADMO help maintain an overview of devices and firmware while speeding up risk analyses. Substation owners and operators also need to understand the significance of firmware updates and take a proactive approach to the challenges they pose. This is the only way they can ensure the secure and uninterrupted operation of their infrastructure. ■

CPC 100 – A VALUABLE TRAINING TOOL FOR SIEMENS ENERGY



“OMICRON has been supplying measurement equipment to both Siemens and Siemens Energy for many years for the commissioning of our equipment,” says Stefan Boetticher, who has overseen the SIEMENS Energy Training Center in Berlin, Germany, for several years. Siemens Energy has operated its Berlin training center for over 40 years, providing certified technical training on the assembly, commissioning, and maintenance of its gas-insulated switchgear (GIS) and air-insulated switchgear (AIS) to customers and internal colleagues.

“We consider OMICRON’s CPC 100 multi-functional testing device to be a valuable tool for hands-on training,” says Stefan. “We use it to instruct our course attendees to perform diagnostic tests on voltage and current transformers and low-power instrument transformers in GIS.”

If you’re a SIEMENS Energy GIS or AIS customer, be sure to contact them to register for a training course at their Berlin Training Center to gain experience with our CPC 100 multi-functional testing device. ■

«We’re very satisfied with the CPC 100. The device is reliable, easy to operate, and its instructions are understandable.»

Stefan Boetticher,
Head of Training,
SIEMENS Energy Training Center, Berlin

Technical Customer Training
omicon.energy/siemens-training





Safety at **new heights**

Whether you're heading off on an adventure or carrying out tests in a substation, reliable safety measures protect us against serious accidents in our daily lives.

The CMC 500 takes your safety to a new level. Sophisticated functions and workflows prevent potential electrical accidents and signal impending dangers.

Discover the new safety functions of the **CMC 500** and easily satisfy international standards for safe test setups.



omicron.energy/new-cmc

OMICRON 





ON SITE: OMICRON IN JAPAN

Teruyuki Harada from Hikari Trading Co., Ltd. shares his insights into the power sector with us.

Hikari Trading Co., Ltd. is an electrical safety equipment manufacturer founded in 1949. They specialize in developing and supplying ground fault protection relays and insulation level monitoring devices. They also handle a wide range of products from leading domestic and international manufacturers, including OMICRON. Hikari Trading Co., Ltd. is committed to developing new technologies and products that contribute to creating a safe and comfortable electrical society.

How is the energy grid structured?

Teruyuki Harada: Historically, Japan's transmission and distribution network has been developed based on power companies' supply areas, with different electrical frequencies between Western and Eastern Japan. The Eastern side of Japan uses 50 Hz, while the Western side uses 60 Hz. Given these circumstances, transmitting electricity and facilitating the power interchange between regions within the country is challenging. Until electricity retailing was fully liberated in 2016, power sales were monopolized by ten major power companies in their respective regions.

What resources are being used to generate power?

In Japan, domestic power generation is dominated by fossil fuel-based generation, commonly known as thermal power generation, accounting for over 70% of total generated power. This is followed by solar power (9.2%), hydro-power (7.6%), nuclear power (5.6%), biomass (3.7%), wind power (0.9%), and geothermal power (0.3%). The electricity generated from renewable energy in Japan is less than 30%, and it still relies heavily on fossil fuels. Compared to other major countries, Japan is lagging and needs to increase the amount of electricity supplied by renewable energy.

What are the current hot topics in the energy supply market?

The international IEC 61850 standard is one of the current hot topics in the Japanese energy supply market. Product sales related to IEC 61850 have grown rapidly in Japan

recently. Preparations are also underway for the introduction of digital substations. In September 2023, we organized a digital substation workshop in Tokyo that was attended by power companies and manufacturers from all over Japan.

What kinds of challenges are your customers facing?

As I already mentioned, in Japan, approximately 70% or more of power generation relies on fossil fuels such as oil, coal, and natural gas. This highlights Japan's dependence on foreign energy sources, and the country has increased its focus on renewable energy to address this situation. Additionally, Japan intends to achieve carbon neutrality by the year 2050. To reach this goal, Japan plans to increase its amount of renewable energy to 36–38% by the fiscal year 2030.

When looking towards the future, where do you see the biggest challenges in the power sector and in general?

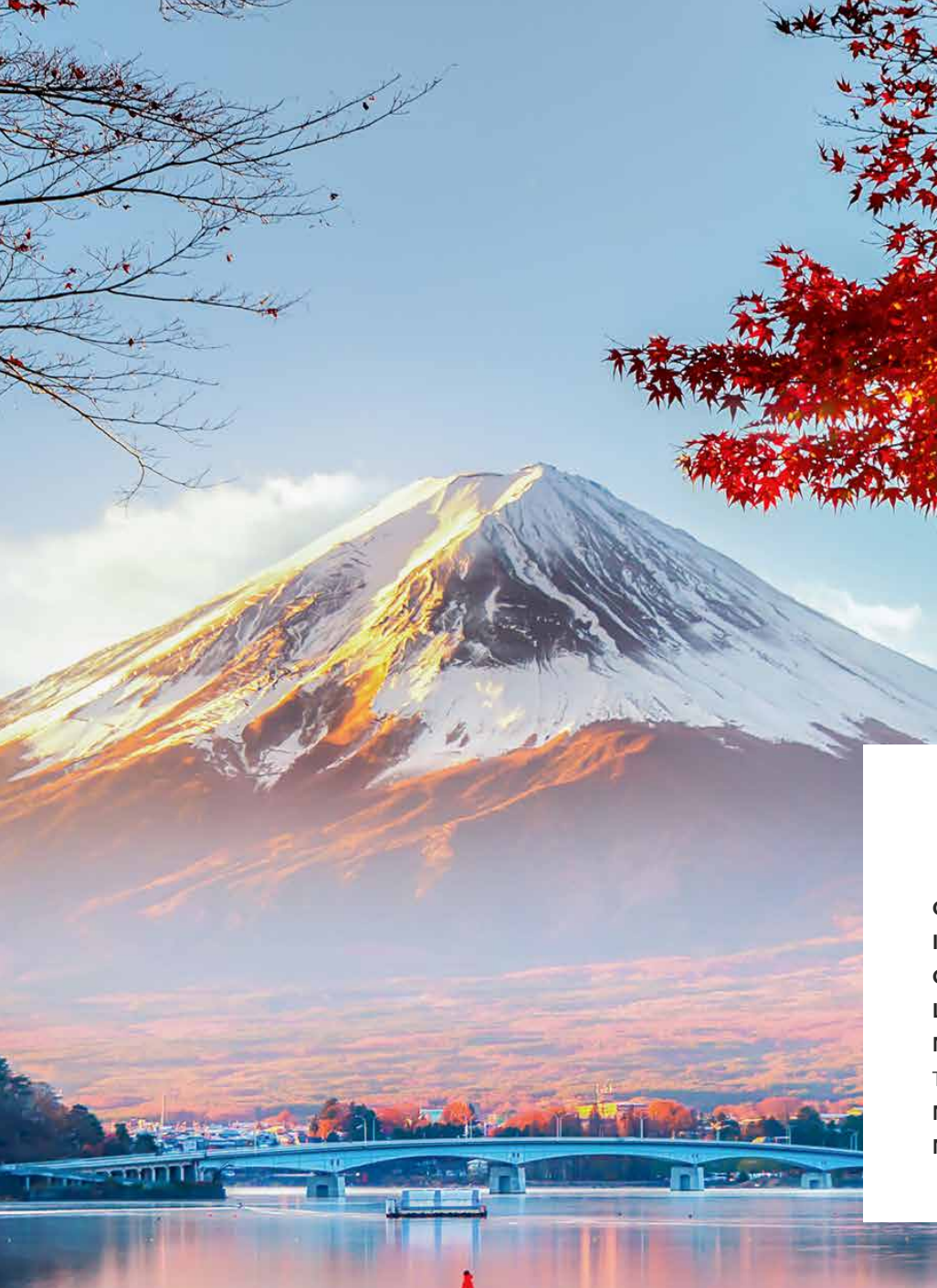
Our biggest challenge is implementing and promoting IEC 61850. In recent years, facilities have been aging and there are many issues related to the maintenance and operation of those facilities. In addition, aging workers and a shortage of human resources in Japan are some other obstacles. In the future, we will face the challenge of introducing digital substations that can be monitored remotely in real-time without workers needing to patrol them.

Thank you for the interview. ▀



Teruyuki Harada,
Director, Overseas Sales Division,
Hikari

 www.hikari-gr.co.jp/products/foreign/omicron.html



ABOUT JAPAN

Capital: Tokyo

Inhabitants: 123,000,000

Currency: Japanese Yen (JPY)

Language: Japanese

National Dish: Sushi, Ramen,
Tempura

National Drink: Green Tea, Sake

National Sport: Sumo, Baseball

DOS AND DON'TS IN JAPAN

- › **Remove shoes:** It's common to take off your shoes and wear slippers indoors.
- › **Bow:** Bowing is a way to greet, thank, or show someone respect.
- › **Don't make phone calls on trains:** Refrain from making calls on trains and set your phone to silent mode.

Mount Fuji and Lake Kawaguchiko

PREPARING FOR CYBER ATTACKS

How Glitre Nett found the right intrusion detection system for their networks

Our StationGuard Solution has been recognized for its exceptional performance in a recent attack simulation conducted by Glitre Nett, the largest electricity distribution system operator (DSO) in the south of Norway. Our intrusion detection system (IDS) excelled by detecting complex threats, highlighting its robust capabilities and effective integration in critical infrastructure environments.

The devil is always in the details

In the dimly lit office room, Ozan sat at his workstation, surrounded by the rhythmic hum of computer fans and the soft glow of multiple screens. The atmosphere was tense as the team sifted through the data, deciphering the recent cyber attack.

Ozan's eyes flew across the information on his screen. At the same time, he reflected on recent critical infrastructure attacks—such as the Ukrainian power grid incidents and breaches of Danish energy suppliers. These events underscored a sobering reality: attackers were becoming increasingly sophisticated, particularly with control systems. He wondered if these attackers were inexperienced individuals exploring new attack vectors, professionals seeking financial gain, or the most dangerous of all—state actors with advanced capabilities and resources.

"Check this out," Christoph called tensely. Ozan approached his colleague's workstation. "See that?

This device isn't sending data as expected. We've got gaps," Christoph scrolled through the interface of the StationGuard IDS and quickly accessed the device overview. "Here and here, and some suspicious activities."

Ozan frowned, absorbing the information. "What suspicious activities?"

Christoph pointed to a series of red alert icons. "After reconnecting, it sent a Gratuitous ARP, trying to validate its IP address by broadcasting it across the network. It also attempted to connect to the DHCP server but used an automatically generated private IP address. Look at the MAC address."

"It looks like it tried to reconnect after it was disconnected."

"Exactly," said Christoph, excited about his discovery. "I'm pretty sure we've got a device replacement scenario here. The device was cloned and planted, then reconnected to the network."

"They know that new IPs entering the network would trigger an alert, but if they replace a device by spoofing the IP and MAC address ... many IDSs wouldn't pick up on that." Ozan sighed. "They needed physical access to the station. It's not easy, but not impossible either. It's particularly dangerous for these remote substations that are only visited once every few months. Let's take a look at all the devices this cloned device has been in contact with and find out if anything else might be compromised."

Christoph began going through the list out loud, "An exploited remote connection, a portable device plugged in by an unsuspecting employee, and now a physical attack ... Did you check the GOOSE messages?"

"That's easy," said Ozan as he smiled, returning to his workstation. "I'd rather you check out any unauthorized HTTP messages sent to the switches." Then he added, "I sure am curious what else Glitre Nett's engineers have in store for us with this attack simulation."





Innovative security

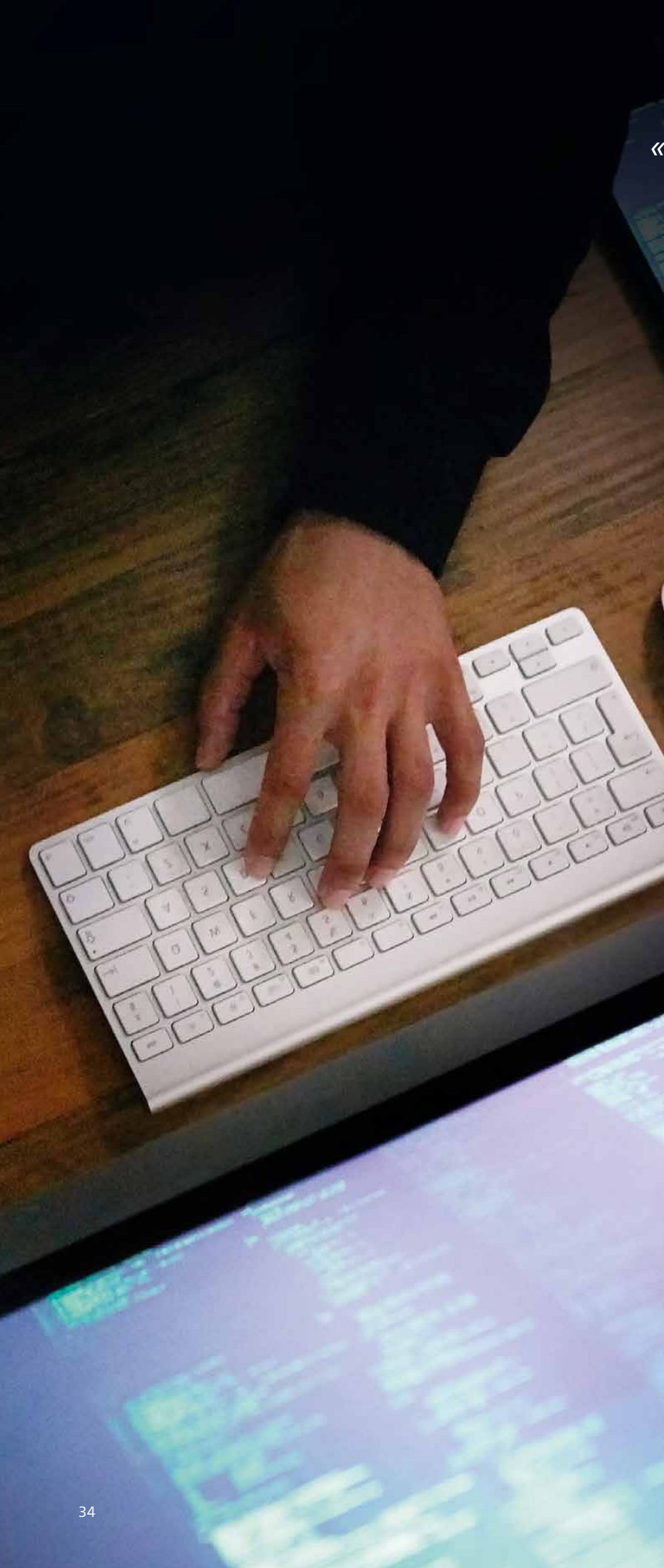
A similar scene has likely occurred during the attack simulation analysis, but let's draw back the curtain for this test. When it comes to an innovative approach to critical infrastructure, Glitre Nett, the largest DSO in Southern Norway, is recognized as a pioneer. Atle Ripegutu, the department head of Process Control at Glitre Nett, underscores the importance of this proactive stance: "For companies in critical infrastructure, innovation isn't just beneficial – it's essential. It's about being proactive and ready. If a major security incident occurs, the cleanup is a nightmare. Investing upfront may not be cheap, but it prevents much larger expenses further down the line."

To this end, Glitre Nett decided to test and evaluate IDSs by simulating real-world attacks within their live substations. This evaluation included solutions from multiple vendors. It evaluated the installation, configuration, and detection capabilities, the scalability and flexibility, the ►

**«If the grid goes down
for ten days, it's anarchy.
This project was about
preparing for critical
scenarios like these.»**



Vetle Norman,
System Engineer,
Glitre Nett



«They explored possibilities like an intruder leaving a disguised component or using an UDP trace route to discover the network topology.»

user-friendliness, the accuracy of alerts, the reporting, as well as the effectiveness of the support provided by each system.

Atle Ripegutu notes the unique challenges faced by substation networks compared to control centers: "Once you leave the station and use various protocols, much information is lost, making it difficult to monitor and secure the pipeline." With legacy codes, evolving IT needs, and the upcoming NIS2 directive being incorporated into Norwegian law, the demand for a comprehensive IDS solution is overwhelming.

After extensive evaluation, Glitre Nett selected our solution alongside those of two other candidates to participate in their attack simulation.

An attack simulation in a live substation

Glitre Nett was concerned about testing a running system, but they believed real-world scenarios offered the most accurate insights. Vetle Norman, a System Engineer at Glitre Nett explains the limitations of theoretical tests: "Research centers

«Given the critical nature of their infrastructure, even the most unlikely vulnerability required a thorough examination.»

ATTACK INDICATORS FOUND BY STATIONGUARD SENSOR

- › New IP and MAC addresses in the network
- › Illegal MMS interactions
- › Disappearing GOOSE messages
- › ARP spoofing
- › NetBIOS reconnaissance activity incl. UDP trace route, ping sweeps, and port scans

like EFA in Norway produce valuable theoretical case studies, but they often fall short of capturing the complexities of actual incidents. Real-world attacks unfold differently, and that's what we aimed to simulate."

Vetle Norman's team focused on recreating plausible intrusion scenarios and attack vectors in their operational substations. They explored possibilities like an intruder leaving a disguised component or using an UDP trace route to discover the network topology. Given the critical nature of their infrastructure, even the most unlikely vulnerability required a thorough examination.

Once each participant's system was installed and set up, all system access verifications were implemented, and operational stability was confirmed. Then, the systems ran autonomously for several months, gathering data and performing their assigned tasks before the test commenced.

Following the attack simulation, Vetle Norman requested a detailed analysis from each vendor, including recommendations based on their findings. "We needed to see how each IDS

performed under real-world conditions. Every storm tests the capacity of our control systems and breakers. The same applies to IDS. If nothing happens, you never know what it can detect," explains Vetle Norman. "This was OMICRON's exam. The results were insightful and helped determine our manufacturers' effectiveness and solutions."

Powerful IDS for detailed analysis

Between late 2022 and mid 2023, our StationGuard sensor was deployed in Glitre Nett's substation. The attack simulation test was conducted on two consecutive days, with all participating IDS providers unaware of the test's timing or attack scenarios. Glitre Nett only released the data they collected to each vendor after completing the exercise.

Our approach to data analysis is defined by a multi-disciplinary team. It includes OT engineers and protocol experts skilled in IEC 61850 and IEC 104 and is further enhanced by IT cybersecurity specialists. Fusing this knowledge is crucial for addressing a broad spectrum of security challenges. "Our dual expertise in power systems

and cybersecurity enables us to tackle complex issues effectively," says Cybersecurity Product Manager, Ozan Dayanc. "The collaboration between IT and OT is essential for robust incident response. It ensures informed decisions are made for alerts and incidents."

During the test, StationGuard and its central management system GridOps, collected critical data from Glitre Nett's network. Glitre Nett set up a remote connection to the StationGuard sensor that allowed us to obtain the system's configuration files, event logs, and packet captures (pcaps). We used these to analyze Glitre Nett's system communications, while GridOps helped organize the data into specific areas.

"This structured methodology enabled us to detect and categorize various potential attacks based on the patterns and anomalies we observed," explains Ozan.

"Initial analysis revealed common issues such as unauthorized devices, well-known attacks like TCP and UDP port scans, and ARP spoofing." Subsequent analyses focused on more sophisticated incidents, including physical and ▶

person-in-the-middle attacks. "After putting our findings together in a detailed report that we submitted to Glitre Nett, we were eager to find out how well we did," adds Ozan.

Attack simulation results

"After reviewing the results of the vendor analyses, OMICRON emerged victorious in the evaluation test. Their solution won by a landslide," asserts Atle Ripegut. StationGuard and the team not only detected 100% of the attacks and provided a detailed report with an accurate attack timeline but they were also the fastest team by far.

Vetle Norman's endorsement further underscores the success of our IDS solution: "I want StationGuard in all my substations," he declared. "It exceeded the capabilities of all the other IDSs. Firstly, the configuration process is surprisingly easy. You simply upload the configuration file, and it's ready to go. Secondly, merging devices is a seamless task. You can combine a

firewall, a switch, and a gateway into a single unit, which is perfect." He also highlights the intuitive user interface: "A system that can detect security incidents but requires lots of training and is difficult to use doesn't make sense for us operationally. The UI is straightforward, with simple commands for setting roles and communication paths, making working with it a joy."

Vetle Norman also praised StationGuard's dual-focus capabilities for system functionality and security: "StationGuard offers functionality analysis that other vendors can't provide. It fits perfectly, requiring minimal setup. It also integrates well with SCADA systems, RTUs, and signaling. From what I've seen, its level of integration and capability is unmatched."

Glitre Nett's feedback concluded with additional commendations for our service and customer engagement. Atle Ripegut remarked, "You gave an exemplary performance in every

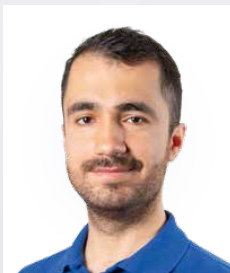
aspect of service—from handling equipment to on-site assistance. All inquiries were thoroughly addressed, and every issue was promptly resolved. The collaboration was exceptionally smooth, without a single problem remaining unresolved."

A promising future

The analysis of the attack simulation test underscores the critical role of an IDS for identifying cyber attacks. "By taking the testing out of the lab environment, the real comprehensiveness of an IDS solution can be properly evaluated," says Ozan. The evaluation demonstrated that many threats are detected accurately by an OT-specialized IDS like StationGuard, where even a single alert can potentially signal a serious attack.

Collaborating with Glitre Nett has been excellent. "We look forward to continuing our partnership and seeing where it takes us," says Vetle Norman. "We need your support and testing equip-

«It was a great experience for us. It verified our solution's capabilities and made us aware of our strengths and potential weaknesses.»



Ozan Dayanc,
Cybersecurity Product Manager,
OMICRON

GLITRE NETT

- › Founded: 2022 – merger between Agder Energi Nett (2000) and Glitre Energi Nett (1993)
- › Headquarters: Drammen, Norway
- › Employees: 350+
- › Electricity customers: 320,000+

 glitrenett.no

ment to manage the ongoing paradigm shift. In the cybersecurity space, we require the unique functionalities that your systems offer. We want to maintain a strong connection and keep you involved. We want to continue using your equipment in the future," he concludes.

Our solution demonstrated its efficiency to the Glitre Nett team. Yet, as always, there is room for improvement. "We have ambitious plans for the future," says Ozan. "We aim to refine our signature base detection, enhance network visibility, and introduce new security features. Enhanced asset inventory collection is also on the agenda. Beyond that, we're continuing to innovate and adapt to emerging threats." ■

If you'd like to learn more about our StationGuard IDS and vulnerability management, please visit our website at

 omicroncybersecurity.com/en/solutions



LISTEN TO THE PODCAST

Interested in this topic?

In this episode, we will learn how an OMICRON team of cybersecurity experts goes about analyzing incoming alarms and how even the smallest indicators can reveal hidden dangers that threaten the safety and operations of an entire system. Scan the QR-code or visit:

 omicron.energy/episode79





Hello,
I am Casper

GENERATIVE ARTIFICIAL INTELLIGENCE IN THE POWER INDUSTRY

An exploration of generative artificial intelligence (GenAI) and how it can enhance our work and the power grid's efficiency

Challenges and transformation in the power industry

The power grid faces numerous challenges, from aging infrastructure and increasing demand to retiring professionals and integrating new technologies like virtualization. We are moving away from large, centralized power plants towards more renewables like solar and wind. All these factors combine to make power grid reliability a complex and evolving challenge:

- › **Aging infrastructure:** In some countries, the grid is outdated, prone to failures, and requires significant upgrades and maintenance investments.
- › **Increasing demand:** The challenges stemming from decarbonization efforts, such as reducing the use of SF6 and the rise in renewables, electronics, electric vehicles, heat pumps, and air conditioning, are straining the power grid significantly.
- › **Retiring professionals and knowledge gaps:** Many experienced professionals are retiring, leading to a loss of expertise and the challenge of training new workers.

Digital tools are no longer optional but essential for solving these challenges. Can GenAI be the solution to some of these problems? How can GenAI foster the creation of conversational models that can access vast, complex data sets and help close the knowledge gap?

Artificial intelligence: what, why, and how

To clarify some basic principles, let's start with a few definitions:

Artificial refers to something created by humans, for example, computer software. Intelligence is the ability to learn, understand, and apply knowledge to solve problems, adapt

to new situations, and comprehend complex concepts. It involves both cognitive functions, such as reasoning and memory, and emotional abilities, like empathy.

Artificial Intelligence (AI) combines these two ideas. AI is a branch of computer science focused on creating solutions that can perform tasks that typically require human intelligence. These tasks range from recognizing speech, making decisions, and translating languages to playing games or driving cars.

AI has evolved significantly from early rule-based systems like IBM's Deep Blue in 1997, a specialized chess software that analyzed millions of moves per second to defeat world champion Garry Kasparov. It advanced through Machine Learning in the 2000s with systems like Amazon's recommendations and then progressed to Deep Learning in the 2010s, exemplified by iOS Face ID.

AI holds tremendous potential in power grids. Although not yet widely used, it is starting to gain attention. AI can analyze massive amounts of data to predict and detect failures. For example, machine learning helps predict asset failures and optimize grid operations, aiding decision-making. However, it is important to emphasize that humans always make the final decisions.

GenAI, popularized by ChatGPT in 2022, can create conversational models that access vast data sources and provide human-readable answers to complex questions. These models can make critical knowledge easily accessible to (new) engineers, bridging the knowledge gap and enabling quicker problem-solving and more efficient grid management.

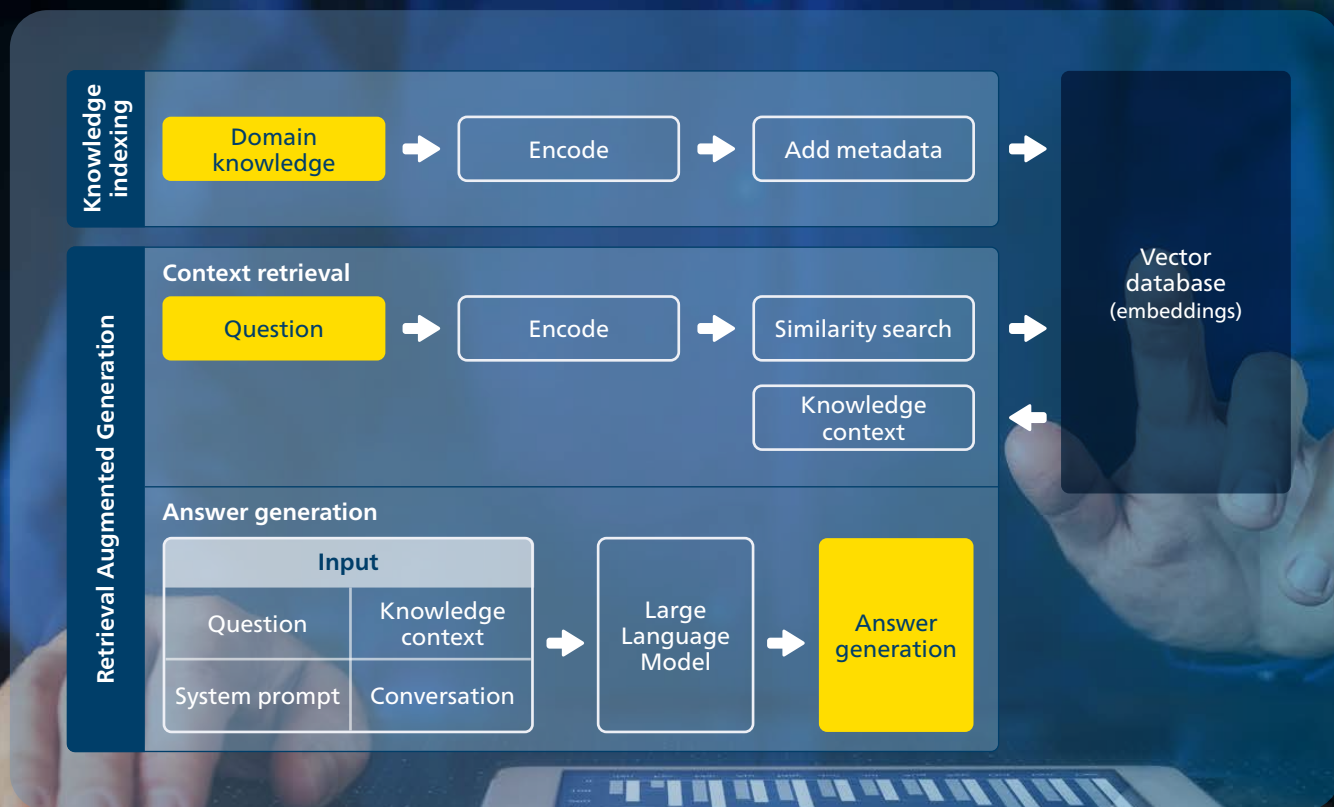
GenAI is advancing very quickly. This rapid change creates significant gaps between what is possible with new technologies, what we can understand, and, most importantly, how we can integrate them into our daily work. At OMICRON, company culture will help us close these gaps with continuous learning, sharing knowledge, and exploring new ideas. Failure isn't something to avoid; small, manageable failures are the best way to learn and grow, both individually and as a company

Retrieval-Augmented Generation

Large Language Models (LLMs) are a specific type of GenAI focused on understanding and generating human-like text. LLMs like GPT-4 are incredibly powerful but have significant limitations, particularly from a training perspective. Training these models is extremely expensive due to the massive computational resources and energy required. Additionally, LLMs need vast amounts of diverse and high-quality data, making data collection and curation challenging. Once trained, updating these models with new information is also complex and time-consuming, often requiring costly retraining or fine-tuning.

Luckily, retrieval-augmented generation (RAG) offers a solution to these limitations. RAG needs to be used with models that have already been trained, such as GPT-4 (OpenAI), Gemini (Google), LLaMA (Meta), or Claude (Anthropic). It combines their power with a real-time retrieval system that accesses relevant information.

This approach reduces the need for constant retraining, making it more cost-effective. Furthermore, RAG can give models access to specific knowledge stored in internal documents and ▶



Retrieval Augmented Generation schema

collaboration platforms. This ensures accurate and up-to-date responses to internal queries. RAG also has an important advantage: the information it retrieves is not used to train the models, which is crucial for maintaining data confidentiality.

Another advantage of RAG is its independence from the specific LLM it uses. This independence makes it easy to switch between different versions or LLMs as needed, ensuring the system can adapt quickly to new advancements or specific requirements without significant reconfiguration.

Challenges of implementing AI

Implementing AI in any field has several challenges. We had to give careful consideration to the following factors before implementing AI:

- › **Data preparation:** AI solutions can only be as good as the data they

use. Ensuring clean, reliable, and well-organized data helps AI systems learn effectively, achieving more accurate results.

› **Integration with existing systems:**

Integrating AI with existing systems is challenging due to data silos and outdated legacy material. In some cases, these systems store data in unconnected and inconsistent formats. Established processes tied to these legacy systems often lack the flexibility to support AI, making it difficult for AI to access and process data efficiently. Departments need to collaborate and adapt established processes to ensure seamless data flow and maximize the potential of AI tools.

- › **Acceptance:** Resistance to change, a lack of understanding, and trust in AI's capabilities make accepting AI solutions challenging. Overcoming this reluctance requires training, clear communication, and demonstrating the value of AI. Encouraging

a culture that embraces innovation with ongoing support helps smooth the transition and enhance the overall effectiveness of AI initiatives.

Casper: Our experiments with GenAI and LLMs

Casper is our first GenAI-powered assistant. It was developed in 2023 as part of an innovation project aimed at helping colleagues find and draft answers related to OMICRON products. It can retrieve information contained in files and other knowledge resources. Along with the answer, it references related documents, allowing the user to obtain more information that helps validate it.

Casper is intended for internal use only. Currently, there are no plans to turn it into an OMICRON product. Experimenting with a GenAI-powered bot enhances our innovative capabilities and lets us explore new ways to

improve our solutions. During 2024 and 2025, we will present the tool to some of our customers to collect feedback about the technology and its potential in our industry. While we don't have plans to commercialize Casper, the feedback we receive will help us identify new opportunities for improving our solutions.

Is OMICRON's GenAI experiment simply a custom version of ChatGPT or Copilot 365?

No, Casper, ChatGPT, and Copilot have different purposes and access to other data. Our bot understands the relationships between our products, such as software and accessories compatible with main devices, and differentiates it from ChatGPT. Casper also takes into account documents that may be less relevant, such as those related to phased-out products or obsolete accessories.

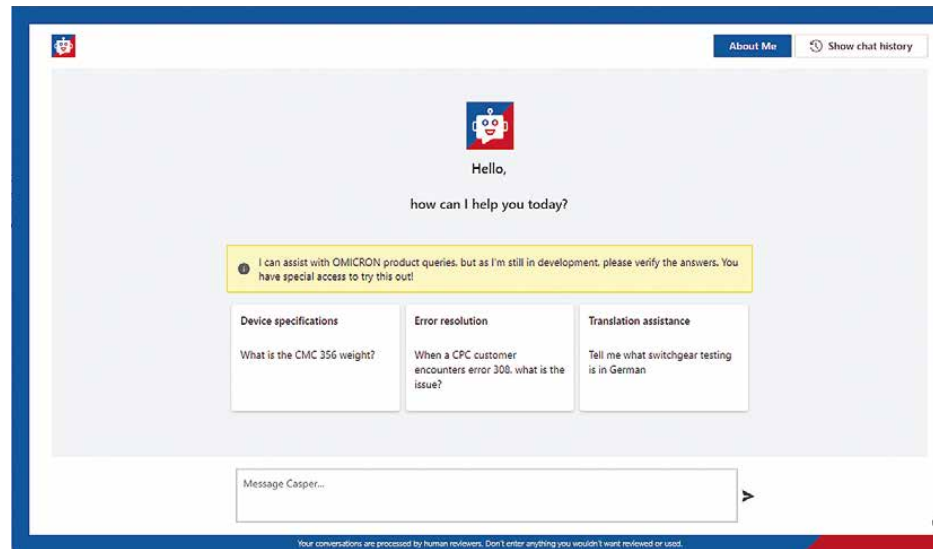
Copilot 365 is an AI-powered assistant integrated into Microsoft 365 applications. It is designed to enhance productivity by providing contextual suggestions and automating tasks. It can access your data, such as emails, meeting notes, and documents, during

retrieval. Copilot offers personalized insights and support directly within Microsoft Office apps like Word, Excel, and Outlook. This makes it a personal assistant integrated with Microsoft Office and tailored to your needs.

On the other hand, Casper can use data about OMICRON products. It is meant to be a virtual intern, able to quickly answer OMICRON product-related questions, draft responses, grant access, and provide references to related documents or knowledge sources.

While still in the experimental stage, GenAI shows great promise in enhancing the value we deliver to customers. We are exploring this technology to boost efficiency and improve internal knowledge management.

If you want to know which parts of this text were AI-generated and which parts we wrote ourselves, please contact us! ■



Casper, our first GenAI-powered assistant

LISTEN TO THE PODCAST

Interested in this topic?



In this episode, OMICRON digital transformation experts Florian Fink and Juan-Carlos Sánchez discuss how implementing digital tools, such as artificial intelligence (AI), helps optimize power grid reliability. They describe the advantages AI presents to the power industry in removing knowledge barriers and improving the efficiency and accuracy of daily tasks, such as analyzing data to predict and detect failures or to optimize energy distribution. Scan the QR-Code or visit:

omicron.energy/episode80



SAY FAREWELL TO THE TIME-CONSUMING SEARCH FOR CIRCUIT BREAKER REFERENCE DATA

Welcome to the Circuit Breaker Testing Library (CBTL)! Our field-proven circuit breaker testing library provides you with reference values at the touch of a button



We're all familiar with situations where numerous circuit breakers and drive units require a multitude of tests and analyses. The test results also require vast amounts of reference data, which involves even more time leafing through reference manuals. Sometimes, the data may not even be available. All this makes data management slow, laborious, and prone to errors. However, CBTL allows you to access an extensive collection of reference values instantly – simplifying your work as a circuit breaker test engineer.

Making use of breaker data from the OMICRON community

The popular Primary Test Manager™ (PTM) software offers the CBTL as an add-on database compatible with the CIBANO 500. You'll have over 400 data records at your fingertips in no time.

Additionally, accessing the library via our new OMICRON customer portal ensures that more and more data will become available over time.

Two ways to expand your data pool

First, use the existing circuit breaker data records in the OMICRON CBTL database, which is supplied with the PTM add-on. Second, download specific circuit breaker data as needed directly from the OMICRON customer portal:

 my.omicronenergy.com/cbtl

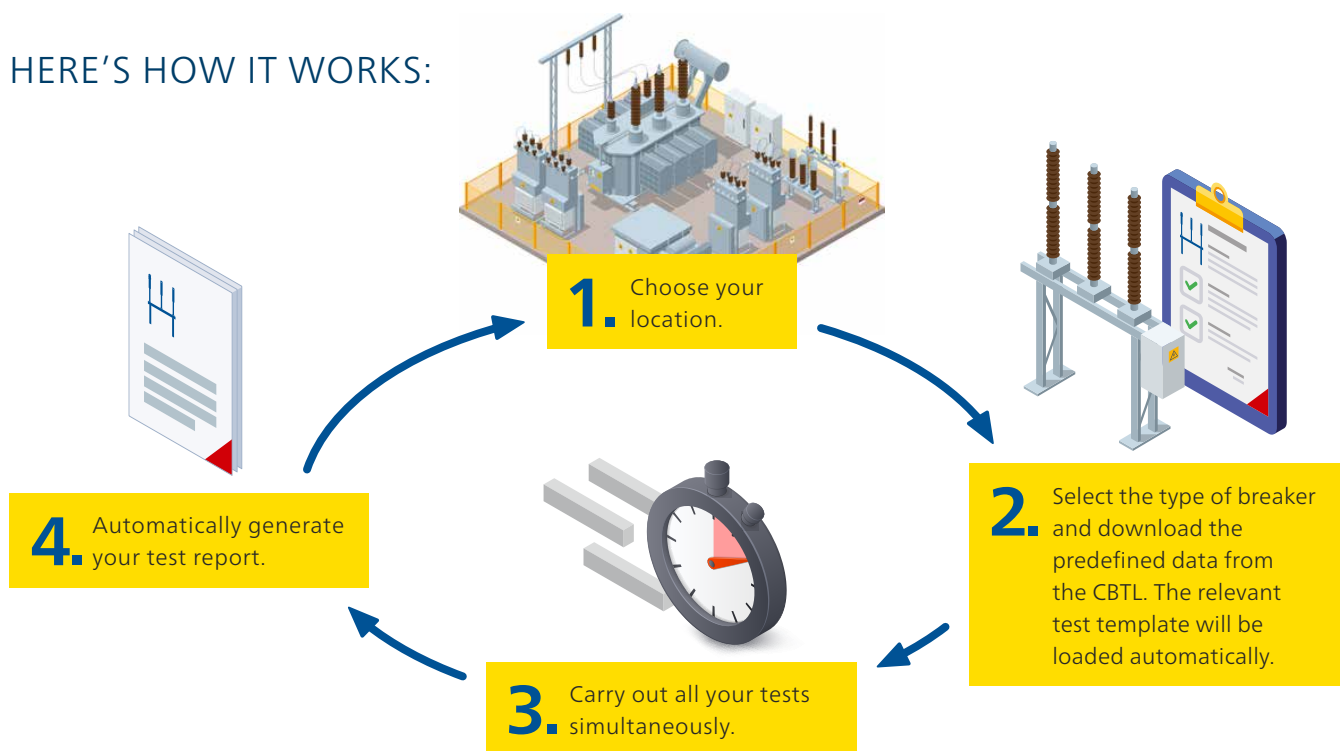
We've introduced this new access method to provide the CBTL user community with faster and more targeted access to the data required. Additionally, CBTL users can upload their anonymized data records to the OMICRON customer portal via email

at cbtl@omicronenergy.com, allowing other interested parties to access them. This will ensure that more and more data records will become available over time, benefiting everyone.

Accelerated testing process and simplified equipment specification

Having all the equipment-specific standard data available almost immediately results in drastically reduced test procedures and less preparatory work. Simply search for the breaker type designation, make any changes to the standard data, and start the test. A CBTL data record often contains valuable additional information for motion transducers, manufacturers' evaluation limits, and conversion data for motion measurements. ■

HERE'S HOW IT WORKS:



LIFE VESTS FOR TEST SETS?

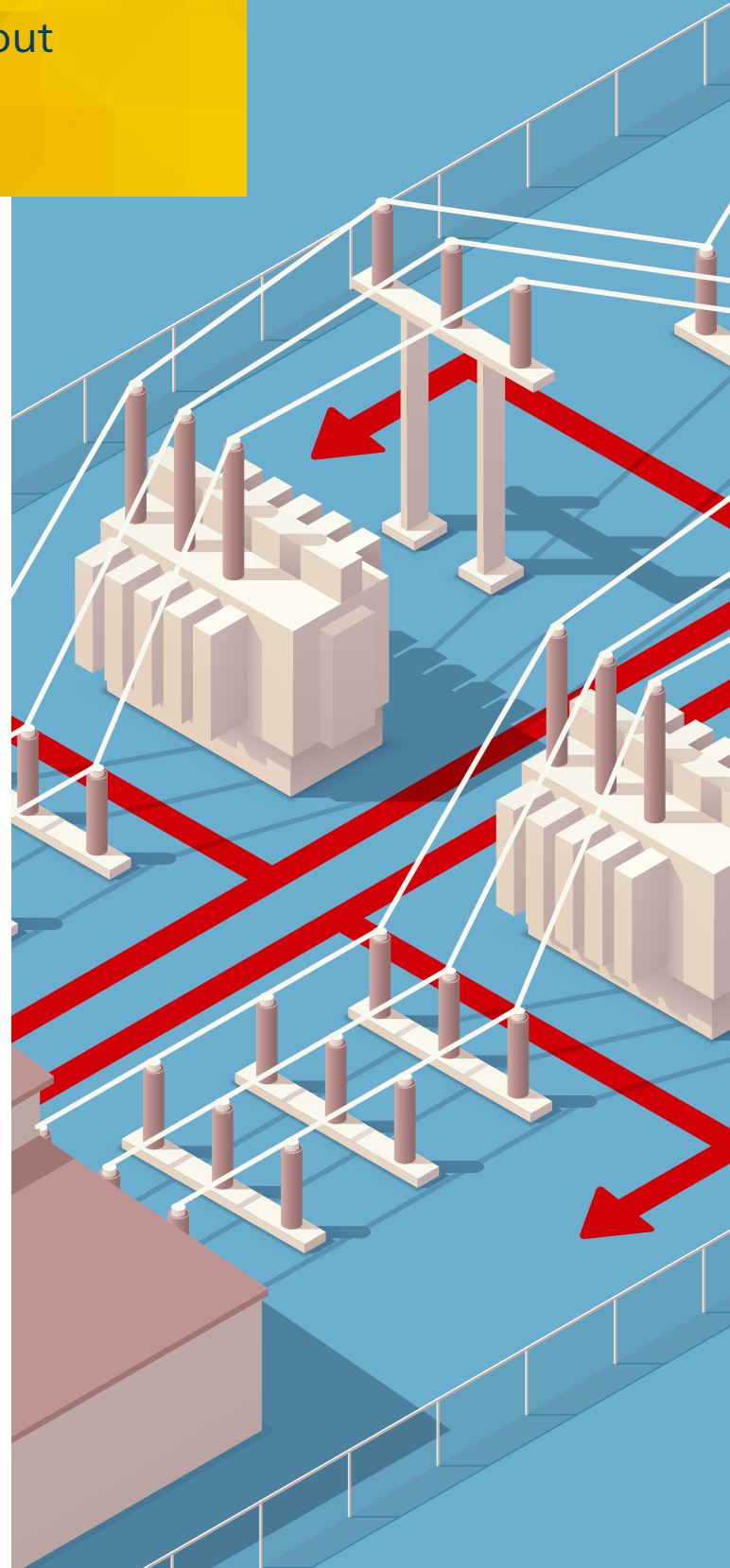
Why we're constantly thinking about improving safety measures

«Hello, everyone, and welcome to today's partial discharge test. We'd like to start with some important safety information to ensure your test is as safe and comfortable as possible. Please keep your safety belt fastened for the duration of the test and place your test set in an upright position. In the unlikely event of an evacuation, please remain calm and follow the illuminated path along the floor to the nearest emergency exit. If the substation floods, you can find a life vest underneath your test set. Pull the life vest over your head, fasten the belt around your waist, and pull on the red tag to inflate it.»

Fortunately, the safety instructions in a real substation are far more reasonable and professional than those described above. However, after training, electrical engineers must rely on their own vigilance and strict adherence to the five safety rules of electrical engineering to ensure their safety.

Developed with safety in mind

Working with electricity is always dangerous, especially when dealing with high-voltage electrical equipment where every task can be a matter of life or death. At OMICRON, we prioritize creating products that are efficient, user friendly, and, above all, as safe as possible. This is why a Product Safety Risk Assessment (PSRA) is integral to our product development process. Many safety features, such as automatic wiring tests, device self-tests, and detailed circuit diagrams in our software interfaces, stem from the PSRA.





LISTEN TO THE PODCAST

Interested in this topic?



Be sure to listen to our Energy Talks Podcast series episode number 87 about how to save lives in high-voltage environments. Scan the QR-Code or visit:



micromenergy.com/episode87

Software updates that can save lives

Even after launching a product, we continue developing new protection functions. While it's well known that software updates can enhance device safety, they typically don't address user safety. Last year, we released a software update for Primary Test Manager™ 5.0 (PTM) that changes this. New CPC 100 features, such as "2kV-Timeout in Quick" and "Rapid Fault Sense" (RFS) technology, provide additional safety measures. These can limit users' exposure to hazardous voltage in the event of an accident.

The 2kV-Timeout in Quick stops the high voltage supply after a defined period. At the same time, RFS monitors the output variable in real time and shuts off the device in less than a millisecond if it detects an anomaly. These features are a valuable addition to existing safety measures and rules. The benefits of the software update even apply to your first CPC purchase, as both functions are fully backward compatible.

Upcoming safety features

It's unlikely that our test sets will come with life vests anytime soon. The same goes for airbags, safety belts, and anti-roll bars. However, you can be sure that we're constantly developing new, practical safety features that aim to make your tests as simple, efficient, and safe as possible. ■

THE FIVE SAFETY RULES

1. Disconnect completely.
2. Secure against re-connection.
3. Verify that the installation is dead.
4. Carry out grounding and short-circuiting.
5. Provide protection against adjacent live parts.

NO PROTECTION TESTING, NO KICK-OFF

The importance of testing interconnection relays

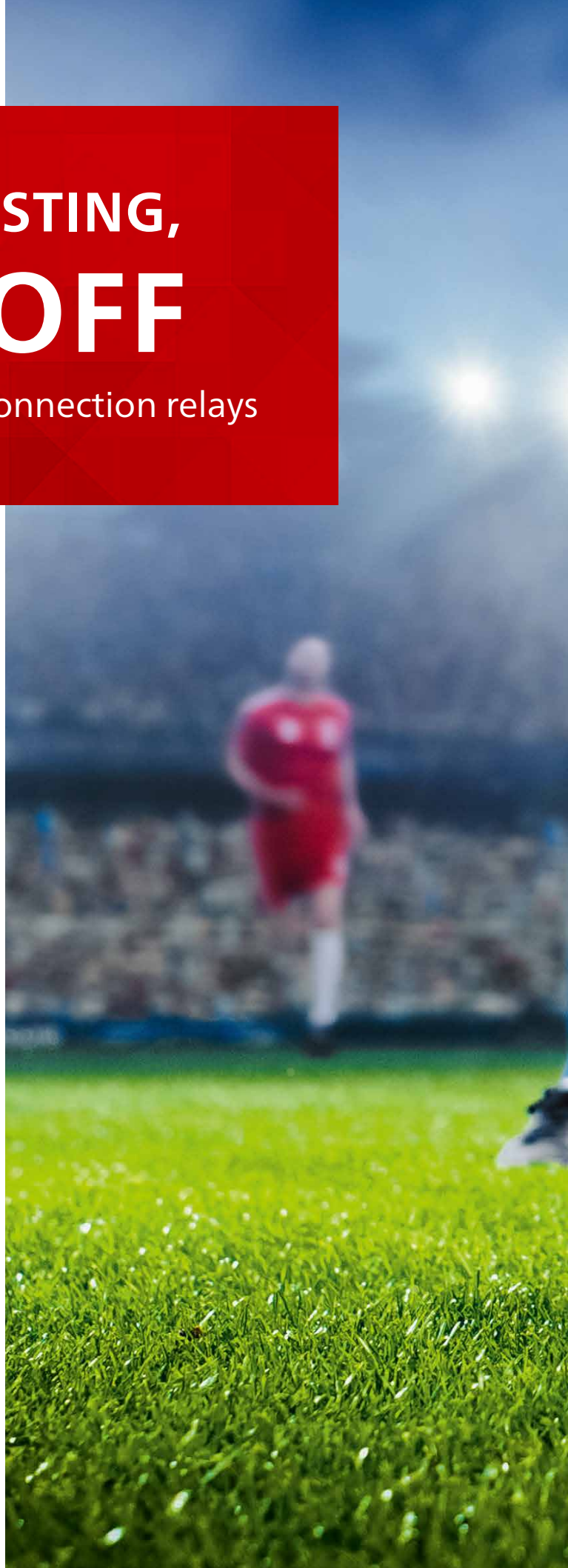
As with any other major sporting event, soccer fans eagerly awaited the opening match of the EURO 2024 competition. In the course of one month, the best European men's national teams faced off in ten stadiums across Germany, with Spain emerging as the champions. Simultaneously, the Copa América 2024 took place in the USA, which Argentina won. During this period, the focus was on the thrilling performances and joyous evenings spent with friends in front of screens, TVs or in the stadiums themselves. However, few people know that protection testing is crucial before such a major event.

Organizing a major event involves an enormous amount of planning and preparation. Beyond logistics and catering, ensuring the safety of everyone inside the stadium is of utmost importance.

Sebastian Geiling, an Application Engineer at OMICRON, explains the critical role of the interconnection relay in this context and outlines the process of testing these relays. Well before EURO 2024, he and his team conducted protection tests in several sports arenas to ensure correct operation ahead of major events.

What role does the interconnection relay play in ensuring the safety of those inside a soccer stadium?

Sebastian: Selected stadiums must satisfy specific conditions to be considered a venue for the competition. At a communal level, the relevant authorities must develop and verify safety concepts for plausibility and coherence. Organizers must demonstrate that the stadium grid is





«Normally, the interconnection relay protects the distribution grid. In the event of a grid fault, generating systems are isolated from the grid to prevent unintended infeeds and resulting voltage and frequency fluctuations. **However, in a soccer stadium, the situation is reversed.**»



Sebastian Geiling,
Application Engineer,
OMICRON

resilient enough to supply energy in an emergency. If the stadium suddenly goes dark at night, dangerous situations can quickly develop. Emergency generators are used to prevent this. These generators start up before the game and run in parallel until the event is over. If there are faults in the transmission network, these generators ensure that power continues to be supplied to the critical infrastructure, such as floodlights, emergency lighting, and the fire alarm system. Additionally, UEFA requires that both the match and its transmission can continue uninterrupted. The stadium grid can achieve this by being isolated from the transmission network. This is the role of the interconnection relay. Once isolated, the stadium grid can switch to emergency islanding operation. Ideally, if a fault occurs, neither the power supply nor the match will be interrupted.

What makes soccer stadiums unique?

Normally, the interconnection relay protects the distribution grid. In the event of a grid fault, generating ►

systems are isolated from the grid to prevent unintended infeeds and resulting voltage and frequency fluctuations. However, in a soccer stadium, the situation is reversed. The relay must trip whenever the distribution grid fails so that the emergency power generators can activate and enable the stadium grid to switch to islanding operation.

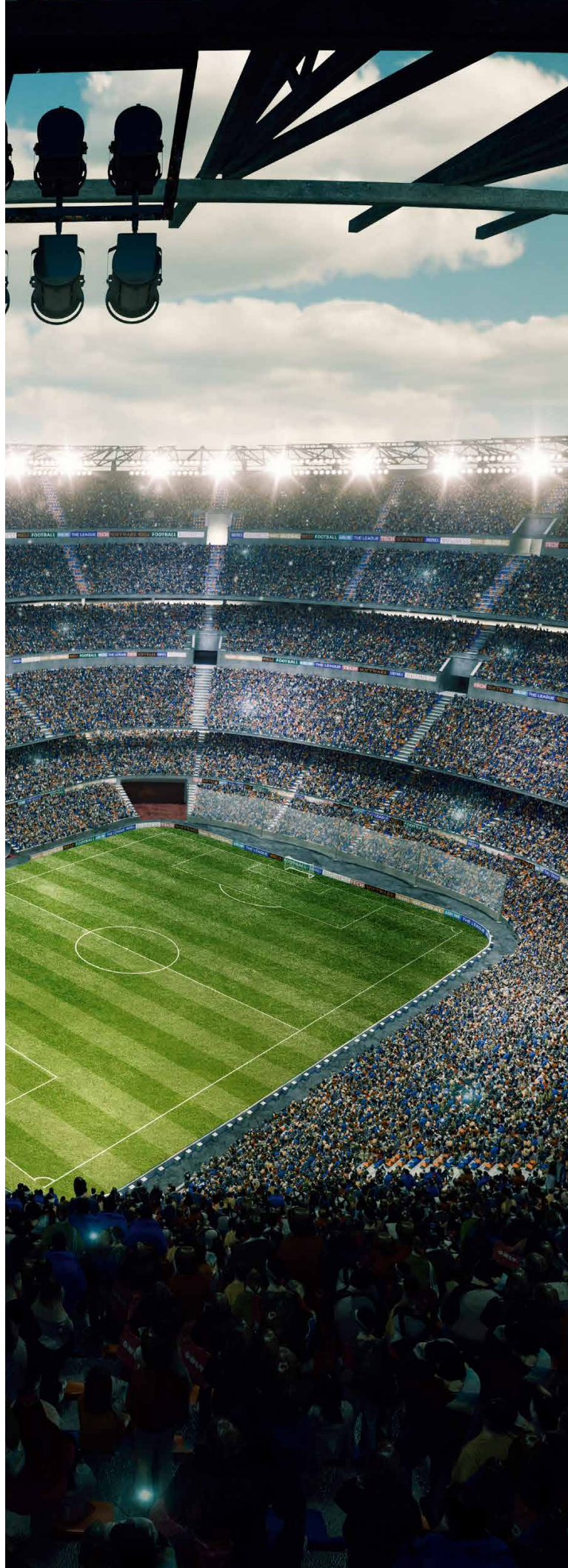


What does the test consist of?

Testing the interconnection relay is a standard test that can be performed quickly and easily using our CMC 310. Simulating a power outage after the relay test and recording it with the CMC 430 and EnerLyzer Live is the interesting part of the procedure. The grid voltage and generator busbar voltage must be measured and recorded for analysis. The circuit breaker is also considered during the measurement. The outage simulation can be performed by isolating a single phase. The interconnection relay then trips the circuit breaker and isolates the emergency power generator from the grid. If the generator functions correctly, the generator busbar's voltage should stabilize shortly, and then the test can be successfully terminated. This confirms that the decoupling from the transmission network is working correctly, and the emergency power generator's response can be measured and analyzed to determine its suitability.

The requirements are met if a stable, basic electrical supply is guaranteed following a brief power loss. Once the test results are available, there's nothing to stand in the way of an exciting evening watching soccer.

Thank you for the interview and for giving us a fascinating glimpse behind the scenes. ■





STATIONSCOUT NAVIGATES NEW WATERS

Support for IEC 104 RTU / Gateway testing

Ensuring accurate data transmission between substations and control centers can be challenging, especially with inefficient testing processes. These inefficiencies can lead to:

- › Longer engineering times
- › Higher operational costs
- › Potential system weaknesses

Traditional manual methods are time-consuming and can compromise the efficiency, security, and safety of power grid operations. Consistently maintaining the system after firmware updates to IEDs is also crucial and challenging.

StationScout automates testing for IEC 61850 and IEC 60870-5-104 protocols. It simultaneously connects the station bus, process bus, and RTU/ Gateways, running thousands of tests in minutes with pre-made test cases and generating automated reports for follow-up actions.

Save engineering time with StationScout

A typical manual test run for the substation automation system (SAS) involves multiple steps and tools:

1. Finalize configuration files, including SCL and gateway mappings.
2. Ensure all SAS elements are present.

3. Wire and label SAS panels.
4. Check wiring against schematics and send configurations to devices.
5. Validate SCL files.
6. Verify communication between devices.
7. Test digital-wiring and communication services.
8. Control process simulators and check binary inputs/outputs.
9. Test communication to control center HMIs.
10. Repeat steps 5–9 for all other bays.
11. Repeat steps 5–10 during FAT and SAT.
12. Repeat steps 5–10 during maintenance or firmware updates.
13. Repeat steps 5–10 for the next project, even if it's identical.

Using StationScout simplifies this process significantly:

1. Finalize all IED configurations.
2. Simulate the rest of the SAS, only making the Device Under Test (DUT) available.
3. Connect to multiple subnetworks simultaneously.
4. Run pre-prepared test cases automatically.
5. Duplicate and re-execute tests for typical bays.
6. Save and reuse test cases for FAT and SAT.
7. Export for use in the next project with minimal adaptation. ■



CELEBRATING 40 YEARS OF OMICRON

Four decades of innovation
and customer loyalty

This year, we're celebrating OMICRON's 40th anniversary. The past four decades have been marked by achievements and highlights, such as product innovations and new solutions that have expanded our global team. We've also gained many loyal customers who've helped us develop our presence and network.

It all began in 1984 when Rainer Aberer founded our company in his parents' basement in a small town in Western Austria. Rainer had a vision of developing software for the electronics and communication industry. In the early years, Rainer and his small team developed QuickFil and AFIL software tools for passive and active filters. They appeared at their first big trade show in Vienna in 1987 with a makeshift wooden booth built in Rainer's parents' backyard.

At the request of an Austrian electric utility, the team began working on their first hardware project: a test set for measurement transducers. Spurred on by their customer's request, a small, dedicated team, including some of Rainer's fellow students, began



developing what became the first CMC, delivered in October 1990. What followed was a challenging period of high development costs and securing the loans needed to cover them.

The turning point came when the team realized that protection testing would be the key to the CMC's future success – an area they were unfamiliar with. So, they began researching protection testing and adapted their software accordingly, leading to OMICRON's first relay test set: the CMC 56. In 1992, this proved to be a wise decision. The high precision, lightweight device was ideal for new digital protection relays. In addition, positive customer feedback strengthened OMICRON's reputation in the market, leading to the device's success.

In those early days, celebrating each CMC order with a cake became a tradition. The small team soon found themselves overwhelmed by numerous cakes. So, when the 100th device was sold in 1993, Rainer expressed his appreciation for the team by taking them on a short weekend trip.

Our product portfolio has continued evolving to meet our customers' needs and requirements. What began with protection testing has diversified into innovative and groundbreaking solutions and services for testing, diagnostics, and monitoring of the world's electrical power industry assets, including products such as the CPC 100 or the CT Analyzer.

Sharing knowledge has been one of our top priorities right from the start. In 1993, we held our first OMICRON User Meeting in Frankfurt, Germany. The event's concept spread around the world and remains popular with our customers today. A year later, we launched training programs through our OMICRON Academy. Today, more than 200 training courses are held annually in 19 training centers worldwide.

In four decades, our success has spread across the globe, serving customers in more than 170 countries. What began as a solo-act in a basement in 1984 has grown into a team of 1,250 employees in 24 locations worldwide, with about 150 dedicated sales partners situated

in many more. Our global network helps us make generating, transmitting and distributing electricity safe and reliable.

We can't wait to see what the next 40 years have in store for us. We want to thank everyone who's shared this journey with us. Thank you for your trust. ■

- 1 Our first booth design, built in Rainer's parent's backyard.
- 2 The makeshift booth design was used for the first time at a trade show in Vienna, where Herwig Ferstl (left) and Rainer Aberer (right) participated.
- 3 Our first User Conference took place in 1993 in a hotel in Frankfurt, Germany with about 65 participants.
- 4 Early CMC 56 advertisements.
- 5 Juan Parra and Marc A. Vogt working together in the former office in Althach, Austria, in 1997.



WHAT'S GOING ON

We are continuing to share our knowledge. We are going to reach out to you physically or digitally with our events, trade shows, conferences, webinars and training courses. Keep yourself up to date by checking out our events and training courses.

Scan QR-Code to get fast access to all links:



OMICRON ACADEMY COURSES & WEBINARS

omicronenergy.com/training
omicronenergy.com/recordings



OMICRON EVENTS

omicronenergy.com/events



OMICRON ENERGY TALKS

omicronenergy.com/podcast

WE ARE LOOKING FORWARD TO SEEING YOU.