TÜVNORDGROUP

security

Paving
the way to
security

Magazine 2025

TÜV®

At home in **50** countries

> 500 locations worldwide

> 15,500 employees worldwide

1,794.7 revenue in € million

A brief profile of the TÜV NORD GROUP

The TÜV NORD GROUP is a globally active technology service provider and the byword for the highest standards of safety, independence and quality. For more than 150 years, we have been making technological revolutions usable while ensuring the safety of those revolutions. With our six business units and almost 100 companies in Germany and abroad, we offer more than 1,500 services in the business areas of testing, inspection, certification, consulting, engineering and training. In personal dialogue with our customers, we create trust in technology for safe and sustainable solutions.

TÜVNORDGROUP · TÜVNORD · DMT · ALTER · TÜVIT

Contents

Digitalisation is changing the world of work. At the same time, it offers a great many new opportunities. But it is also creating dependencies between electronic systems, which are increasingly becoming the target of hacker attacks. It is to prevent these that we deploy our expertise, protecting systems and heightening awareness of these risks. In this way, we are playing our part in making business processes more secure and raising awareness of threats.

Technology is making ever faster leaps. What was unthinkable yesterday is already reality today. Despite all the progress that has been made, security and reliability remain decisive criteria. This is where our expertise comes into its own: We test technical equipment, certify systems and develop new standards and test procedures. Our work is crucial in keeping technology reliable and trustworthy.

Data streams know no boundaries on their journeys around the world and beyond. They are the backbone of the economy. Because even minor disruptions can have serious consequences, our expertise is widely appreciated: We help manufacturers set up secure systems. This results in robust infrastructures which protect data, neutralise threats and build trust worldwide.


esmo
talos

security

Paving the way to **security**

In the TÜV NORD GROUP, we are actively helping shape technological innovations by arming them against digital threats from the ground up. Here are six examples.

Thora Markert, Product Manager for AI at TÜV NORD CERT

Business Unit Certification

Using AI systematically

Artificial intelligence needs trust: Having been accredited in accordance with ISO/IEC 42001, TÜV UK and TÜV NORD Nederland are setting the standard for the secure and responsible use of AI.

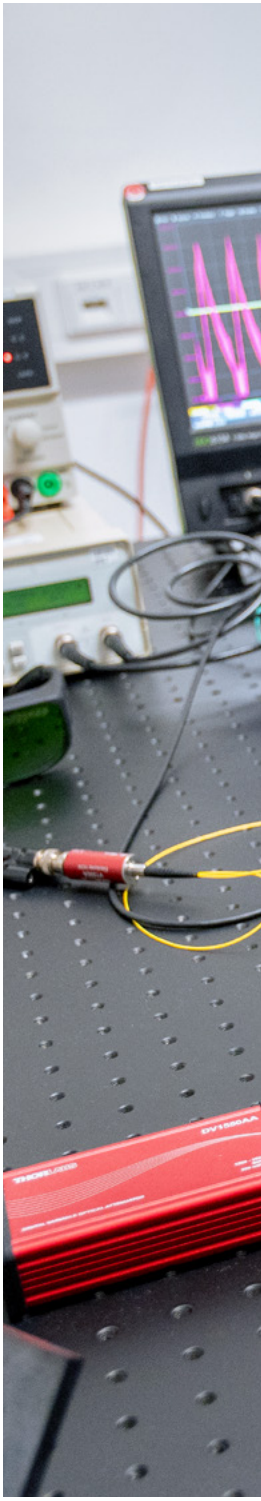
“Artificial intelligence is a technology that offers enormous opportunities but also comes with a lot of risks,” explains Thora Markert, Product Manager for AI at TÜV NORD CERT. The possible challenges range widely from technical malfunctions and manipulation risks to attacks on AI systems and ethical issues. “These are completely new questions that never used to be relevant with earlier technologies of this kind,” says Ms. Markert. This is precisely why companies are being called upon to use AI responsibly; after all, this is the only way to ensure the security and integrity of their systems.

And this is exactly where the ISO/IEC 42001 standard comes in. It is the world’s first international standard for management systems in the field of AI. “ISO/IEC 42001 offers a framework for implementing and deploying AI systems responsibly and effectively, and mitigating risks,” Ms. Markert explains. The standard places particular emphasis on the protection of people and society, the management of societal risks and compliance with ethical, data protection and security requirements.

The point of ISO/IEC 42001 certification is to help companies meet growing regulatory requirements. Like many other regions around the world, the EU is currently establishing a legal framework for AI. In the summer of 2024, the bloc passed the EU AI Act, which will be gradually ramped up in the months leading up to August 2027. “With the gradual introduction of the AI Act, the demand for certification is going to increase significantly,” Ms. Markert predicts. Companies outside the EU which offer AI-based products in Europe must also meet the requirements of the EU AI Act. The certification arose out of close collaboration between TÜV UK and TÜV NORD Nederland, both accreditation pioneers within the TÜV NORD Group. TÜV NORD CERT supports the two foreign subsidiaries and is itself aiming for similar accreditation in the future. “Together we’ve developed an effective certification process that we’re also making available to other foreign companies,” Ms. Markert says. “This is enabling us to offer high-quality certifications for AI systems worldwide and offer companies optimal support in their various markets.”

Business Unit Digital & Semiconductor

Keys to the future



TÜVIT is building a state-of-the-art research laboratory for Quantum Key Distribution (QKD) systems in Essen. It is here that the foundations are being laid for the testing and certification of systems that enable secure data encryption using quantum technology.

Our digital world is home to more and more connected devices which are generating increasing volumes of data. And it is to protect these data that encryption systems are so very important. But quantum computers may well soon be in the position to crack classical encryption methods. This is because they offer a new type of data processing that is opening the door to previously unimagined computing power. “One common method of data encryption is what we call key exchange. In this process, two prime numbers are combined to create a very large number,” explains Sven Bettendorf, expert in quantum technology at TÜVIT. “A classical computer would need millions of years to get back to the original prime numbers. A quantum computer can do it in just a few minutes.”

This is why new approaches to secure data encryption are needed – such as QKD, with which key exchange is based on physical laws. “This is basically beating quantum technology at its own game,” explains Mr. Bettendorf. However, some hurdles still remain to be overcome for this method to see practical use.

The aim of TÜVIT’s new research laboratory in Essen is to create the technological basis for the testing, qualification and certification of QKD components and systems. This has been made possible thanks to funding from the “Blueprint of a Certification Eco-System for QKD Systems and Applications” project being run under the aegis of the German Federal Ministry of Research, Technology and Space.

“There’s probably no other laboratory in the world that is so well positioned professionally in this field,” says Mr. Bettendorf. One special feature is its open optical laser laboratory, in which researchers can deliberately and precisely manipulate key device components using lasers and simulate possible attack scenarios.

The laboratory was completed in 2025, and trials are now beginning. “Our goal is to be in the position to carry out our first tests and certifications in 2027,” Mr. Bettendorf explains. In this way, TÜVIT is not only supporting manufacturers of QKD systems but also strengthening the role of German industry in this forward-looking technological field.

Sven Bettendorf, expert in quantum technology at TÜVIT

Jan Struve, Head of Fire and Explosion Protection at TÜV NORD EnSys, and **Burkhard Rose-Mende,** Head of business field Cyber Security Projects and Critical Infrastructures at TÜV NORD IT Secure Communications

Business Unit Energy & Resources

Protecting what sustains us

Whether they be power plants, airports or water utilities, critical infrastructures are the backbone of our society. TÜV NORD EnSys and TÜV NORD IT Secure Communications are now combining their expertise to provide system-relevant facilities with holistic protection – an offer that is unique in Germany.

For operators of critical infrastructures, malfunctions can have grave consequences. The pressure on these companies is increasing as they are having to arm themselves against a range of fundamentally different dangers, including natural disasters and cyberattacks. This is exactly where the new collaboration comes in.

Jan Struve is Head of Fire and Explosion Protection at TÜV NORD EnSys. His team has many years of experience of assessing safety-related issues relating to nuclear power plants and is therefore familiar with high-risk technologies. Burkhard Rose-Mende is Head of the business field Cyber Security Projects & Critical Infrastructures at TÜV NORD IT Secure Communications. These two experts are all set to combine the expertise of their respective fields to create an offer without precedent in Germany: Business Continuity Management, which combines physical safety with IT security. Their shared task is to give companies the tools and wherewithal they need to quickly resume or restore operations in the event of power outages, hacker attacks or fires.

“Many of our existing customers work with unconnected solutions, with fire protection in one silo and IT security in another. We’re now systematically bringing all of these into relationship with one another, and our work is being welcomed by clients,” explains Mr. Struve. In collaboration with the customer, his starting point is a systematic analysis of the risks, after which he arranges them in order of priority and works out suitable measures to counter them. The coronavirus pandemic and the war in Ukraine have shown that companies often do not know where they are vulnerable – until critical processes fail.

The implementation of the Network and Information Security Directive is prompting companies to act, Mr. Rose-Mende says: “The scope of application will be expanded and the requirements tightened.” The number of affected companies is expected to increase from its current level of about 4,500 to 29,500.

The idea for the cooperation arose out of practical experience: Data centres served as a blueprint and showed how valuable the combination of both disciplines is. The municipal utility market, in which both business units already have established customer relationships, looks particularly promising. With the integrated approach, customers benefit from the pooling of expertise, and TÜV NORD is optimally positioned in this growing market.

Business Unit Industry

Security through smart testing

For the first time, the Korean electronics manufacturer Samsung has commissioned TÜV NORD with the testing and certification of its smart home products – a sign of its commitment to cyber and data protection in connected environments.

Smart home products, ranging from intelligent refrigerators that that keep track of their own contents to generate shopping lists to robot vacuum cleaners that that improve their own navigation skills by recognising certain objects, can make everyday life easier. “A device becomes a smart home product when it gets connected to a network and interacts with its environment,” explains Matthias Springer, Senior Vice President for Functional Safety & Security at TÜV NORD. However, connecting more and more devices brings with it a weight of responsibility: To prevent devices from becoming gateways for hackers, manufacturers must secure their products against cyberattacks.

The Cyber Resilience Act (CRA) has set minimum requirements for IT security in the EU since 2024. TÜV NORD tests and certifies connected products for the Internet of Things (IoT) taking its cue from the ETSI with the ETSI EN 303 645 standard, which provides guidelines for compliance with the CRA.

During the audit, manufacturers must, on the one hand, produce documentation to prove that their products meet certain safety criteria; on the other, the devices themselves are subjected to verification and validation tests. “Password protection, authentication and user documentation are the key points,” says Kim Youngcheon, engineer at TÜV NORD Korea.

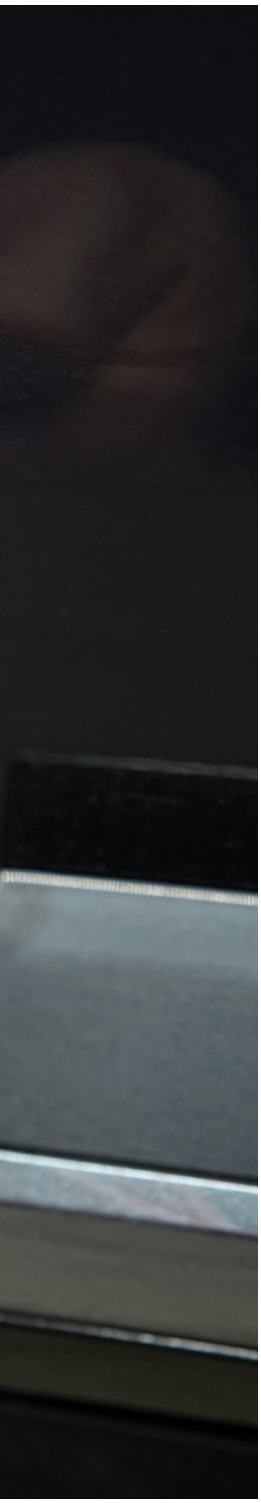
For the first time, Samsung has had two ranges of robot vacuum cleaners, the Bespoke AI Jet Bot Stream and the Bespoke Jet Bot Combo tested along with a range of bespoke AI refrigerators – with success. The manufacturer-independent TÜV NORD “Certified Cybersecurity” test mark is intended to offer consumers better protection, provide guidance for purchase decisions and reduce security concerns.

“We’re very proud to have carried out the first IoT certification according to ETSI EN 303 645 for Samsung in collaboration with the team in Germany,” says Kim Soyeon, Assistant Engineering Manager at TÜV NORD Korea. “This project and the certification are a milestone in IoT cybersecurity and will set new standards for the market.”

The transitional phase of the CRA will finish at the end of 2027 – until then, the requirements will be gradually tightened. “We will keep pace with the regulations and continue to use our expertise to support our customers,” says Mr. Springer. The most important thing now is to tell the customers and raise awareness of the upcoming regulations, he adds.

Matthias Springer, Senior Vice President Functional Safety & Security at TÜV NORD, and **Kim Youngcheon,** an engineer at TÜV NORD Korea, alongside **Kim Soyeon,** Assistant Engineering Manager at TÜV NORD Korea

Gero Eggers, Product Developer and Product Manager at TÜV NORD Mobilität



Business Unit Mobility

Data diagnostics with a clear view

TÜV NORD Onboard Car Diagnosis represents an innovative solution for modern vehicles which makes digital inspections safer, more efficient and more transparent – and offers potential for other fields of application.

Modern cars have long been more than just a means of transport – they are now data storage devices on wheels. From navigation destinations to call logs and payment data, they collect enormous amounts of sensitive data over time, especially via smartphone connections. This means that vehicles are not exempt from the increasing regulatory requirements for digital information security.

A particularly risky juncture is the point when a car changes hands. “There are many scenarios in which it’s critically important to establish if particular information is still stored in the vehicle,” says Gero Eggers, Product Developer and Product Manager at TÜV NORD Mobilität.

The concerns extend beyond mere unprotected data to include manipulated mileage and concealed faults. This is exactly where the TÜV NORD Onboard Car Diagnosis comes in. The system uses the on-board diagnostic interface to connect to the vehicle and delivers a comprehensive analysis within minutes. As a one-dongle solution, it combines several services: Personal information is cleaned up (using an app) in compliance with GDPR, technical problems are brought to light by an error memory analysis, and the mileage and vehicle identification number are checked for plausibility. For this innovative solution, the system was recognised as one of the top-3 innovations in the “Electrical/electronical systems & software” category of the Best of Industry Award 2025, Mr. Eggers reports. “It’s amazing how many vehicles do actually get manipulated,” Mr. Eggers reports. The TÜV NORD Onboard Car Diagnosis detects which control units have been used to store mileage and identification numbers and reliably detects discrepancies. Installed spare parts can also be checked for “false identity” by the same means.

The solution is also opening up further perspectives. “We have lots of ideas for additional applications – for different services, customer groups and vehicle types,” Mr. Eggers explains. The latest addition to the portfolio is a battery check for electric vehicles, which can be used to reliably assess the condition of the traction battery in an EV. All collected data are anonymised and stored on secure servers. As well as meeting current data protection requirements, the TÜV NORD Onboard Car Diagnosis is thus also laying the foundations for further analyses. “In the long term it will be possible to evaluate this data pool and use it to improve road safety,” says Mr. Eggers.

Business Unit People & Empowerment

Fit for cyber protection

Cybersecurity no longer only affects large corporations – SMEs are also increasingly being targeted by hackers. With the TÜV NORD Akademie's NIS-2 expert training course, companies can precisely target the measures they need to become resilient and meet the new legal requirements.

The threat posed by cyberattacks is growing as digitalisation continues to spread. It is for this reason that the European Union has fundamentally revised its Directive for Network and Information Security. "The requirements have been dramatically tightened," explains Melanie Braunschweig, Product Manager at the TÜV NORD Akademie. The new NIS 2 Directive (EU) 2022/2555 will oblige not only operators of critical infrastructures but also numerous medium-sized and large companies from other sectors to implement stricter standards in cyber resilience. The TÜV NORD Akademie responded very early to these changes. "Close market observation and open communication enabled us to pioneer a tailor-made training programme," says Ms. Braunschweig.

Depending on size and annual turnover, some 30,000 companies in Germany from 18 sectors are affected, including digital services, public administration and food production. What is new is the insistence on the personal responsibility of management: Directors and senior executives must ensure that risk management measures are implemented and monitored. They are obliged to complete appropriate training – and, in the event of violations, they will be personally liable. But motivation to act should not come solely from the legal requirements. "It's important to communicate the importance of security to employees and to be well prepared for emergencies," emphasises Diana Kühn, Account Manager at the TÜV NORD Akademie.

To support managers and directors in their duties, the TÜV NORD Akademie offers three training courses with different focuses. Another component of the comprehensive training programme for cyber and information security is the four-day certificate course entitled "NIS-2 Expert (TÜV)", which is aimed at security and IT managers. "Participants leave the seminar with an understanding of the legal requirements and the ability to apply them to their company," Ms. Braunschweig says.

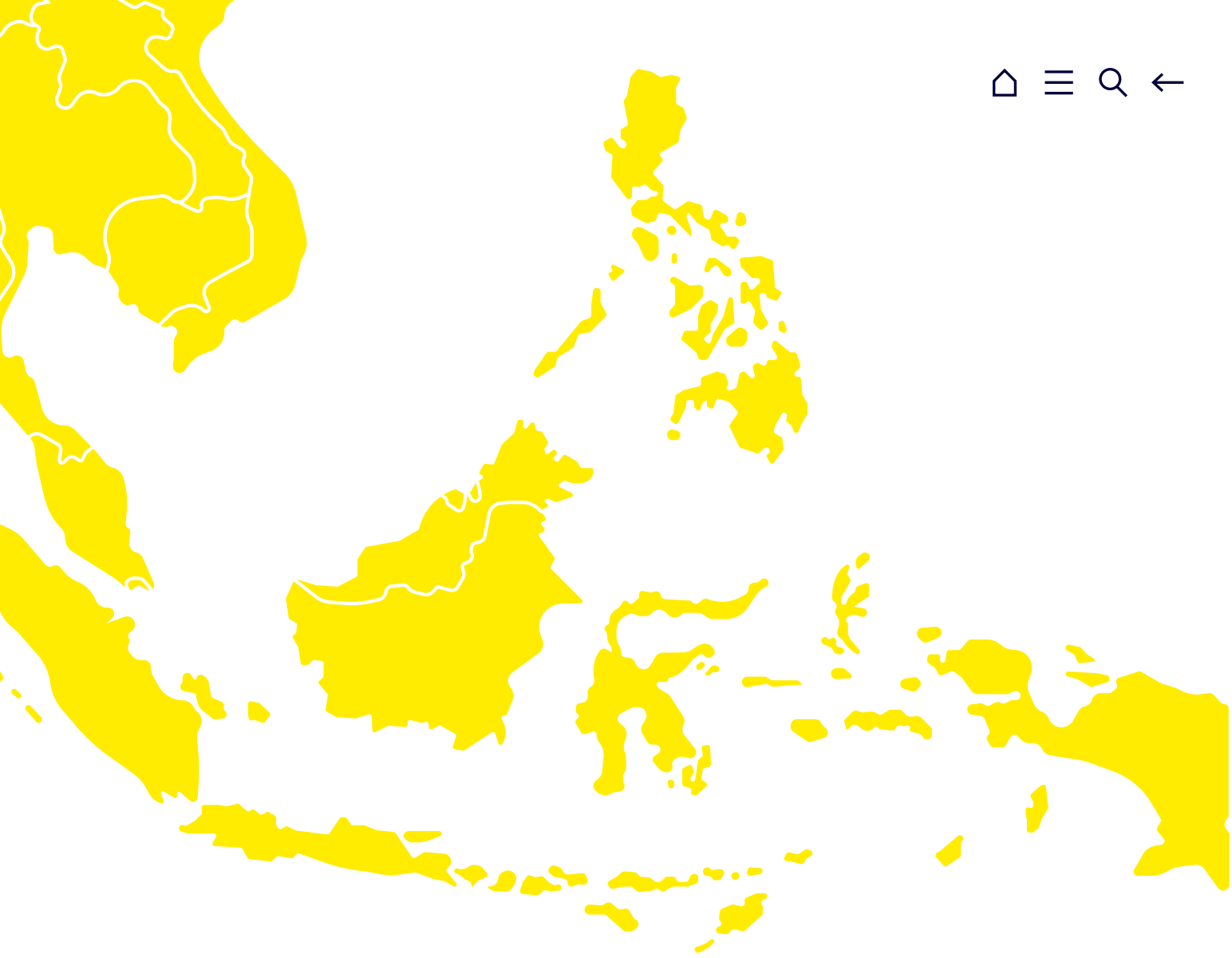
The course has been successfully held eleven times since September 2024, and at least 18 more training dates are planned for 2026. "The increase in demand has vindicated our early strategic orientation and confirms our expertise in practical communication," Ms. Kühn says.

Melanie Braunschweig, Product Manager at the TÜV NORD Akademie, and **Diana Kühn,** Account Manager at the TÜV NORD Akademie

Digital transformation launched in Indonesia

The Digital Hub SEA is the launchpad for a cloud-first platform that will connect international units and enable a new digital way of working. According to Dr. Jörg Aign, Managing Director of TÜV NORD International, Southeast Asia is serving as a pilot region for the development of a resilient blueprint for global transformation in a dynamic environment, with a focus on AI-supported productivity and security.

Dr. Jörg Aign, Managing Director of TÜV NORD International



What's the idea behind the Digital Hub SEA?

The Digital Hub SEA is the launchpad for our cloud-first platform, which will one day connect all our international units and create the basis for a new, digital way of working. You could say that we're laying a secure foundation on which to build an entire digital house. We're developing the platform in a protected environment with the aim of optimising it and then rolling it out globally. In this way, we're creating the basis for AI-supported productivity, globally standardised processes and new digital services.

Why was Southeast Asia, especially Indonesia, chosen as a pilot region?

Southeast Asia is one of the world's most dynamic economic regions: More than 680 million people live here; the digital economy has surged to a gross merchandise value of more than 300 billion US dollars and growth rates of around 4.5 percent. We've selected Indonesia for the development and secure trialling of the new platform. Indonesia offers us ideal conditions to quickly gain experience and develop a resilient blueprint for global transformation. We aim to roll out the platform globally as soon as possible for the use of Microsoft's Copilot. By relieving our employees of routine tasks and helping them with multi-layered evaluations and analyses, we will increase their personal productivity.

So the goal is to increase productivity, standardise and automate processes, and merge data?

That's right, but it's only the beginning. We're talking about a multidimensional transformation. Alongside the increase in productivity I mentioned earlier, we're automating complex business processes using power apps, Copilot Studio, and Foundry IQ. These tools are helping us develop digital solutions and optimise business processes. The idea is to quickly and reliably merge data from multiple storage locations for ease of use. We want to digitalise business processes quickly without having to bring in IT specialists. And we aim to develop new digital products. This isn't just about efficiency; it's also about realigning the way we work and developing new opportunities for the Group.

How will that work in concrete terms?

Summarising e-mails, drafting texts and analysing data are all tasks that Microsoft Copilot can perform well. At a later date we aim to use AI-supported software, or agents, to automatically develop specific tasks. These agents will then support us in complex tasks. But always under human control. AI is a helping "hand" that will relieve of us of donkey work: Copilot can automatically create multilingual notes during a meeting and summarise the most important decisions live. This means that all the participants are immediately on the same page – without having to redo the notes or overcome language barriers. This is an example of what we're testing in Southeast Asia, with the aim of making it available to everyone in the Group as soon as possible.

Can you trust AI, especially when it comes to solving complex tasks?

If anything, it's in the area of complex tasks that AI is likely to come into its own in the future. The necessary trust will be built up through transparency and experience. We're relying on the "human in the loop" principle here. AI, as I said, is just the helping hand. Modern data platforms like Microsoft Fabric IQ go way beyond simply collecting and storing information. They connect data from many sources, preparing them intelligently and rendering them usable for analytics, AI models and automation. The result is a true "intelligence platform" that transforms data into knowledge, forecasts and concrete recommendations. Foundry IQ then builds on this as a knowledge and context layer for AI agents, enabling the development, training and secure operation of AI solutions that can be integrated directly into business processes, such as predictive analytics, automated workflows or intelligent decision support in areas like finance, operations or strategy. This means that information is always up-to-date, secure and scalable. AI can recognise complex relationships and make concrete recommendations, but it will always be down to humans to evaluate them. All the processes are transparent at all times.

The Indonesian team is working single-mindedly on forward-looking digitalisation projects.

Building an infrastructure for data integration – merging data from different sources.

Increasing business productivity by automating complex business processes using AI and power apps.

Increasing personal productivity through the use of AI in routine activities.

AI doesn't necessarily run on individual laptops, but tends to be server-based, right?

That's correct. We've adopted a hybrid IT architecture that combines cloud and on-premises infrastructure. The intelligence lies in the cloud, where we can guarantee scale, security and performance. Sensitive data and confidential work are specifically protected and, where necessary, processed in specially secured cloud environments or locally.

Do you intend to use the knowledge acquired in Southeast Asia in other regions too?

Learning, scaling and reusing are what the project is all about. What we're developing in Southeast Asia will be the blueprint for all other regions. And we're going to go even further. Good solutions that emerge anywhere in the world will be shared globally. In this way, we'll avoid duplication of effort, increase our efficiency and accelerate the introduction of new technologies worldwide.

After the kick-off event for the Power platform, the committed and motivated Indonesian team is getting to grips with the tasks that await them.

The Digital Hub SEA is the launchpad for our cloud-first platform, which will one day connect all our international units and create the basis for a new, digital way of working.

Good solutions that emerge anywhere in the world will be shared globally. In this way, we'll avoid duplication of effort, increase our efficiency and accelerate the introduction of new technologies worldwide.

“Our Digital Hub SEA will make us faster, more efficient and more secure. It will also open up new business fields for us.”

Dr. Jörg Aign, Managing Director of TÜV NORD International

This will have an impact on the entire Group, won’t it?

That’s the vision in a nutshell. Southeast Asia is the launchpad for our fundamental global IT transformation. In the end, we’re all going to be working on a secure, cloud-first and AI-enabled platform. This will make the TÜV NORD GROUP an agile, data-driven and trustworthy partner – with security as its immovable foundation.

Digital security is an important issue: Have you factored it into your calculations?

Our platform is founded on security. We’re placing our reliance on a modern security architecture with “Zero Trust” as its basic principle. This means that no user, device or application is ever automatically trusted, whether it’s inside or outside the corporate network. Every access is consistently checked, every authorisation restricted to what is absolutely necessary and also time-limited. This prevents attackers from spreading throughout the system, even if they should manage to compromise one access point.

Could a platform like this contribute to the development of the company?

Yes, enormously. It will make us faster, more efficient and more secure. But above all, it will open up new business fields: Data-based services, digital test models, AI-supported analyses, to name just a few. It will transform us into a data-driven company, integrating AI into our processes and enabling us to develop new business models. In other words, the platform is going to be the foundation for sustainable success and the future of our business. We’re learning, trying things out, discovering new ways of working together and developing step by step. The key thing for us will be to go down this path as a team. AI will support us, expand our range of opportunities and give us humans, with all our knowledge, the freedom to be and stay unbeatable. Together, we’re going to shape the future of our company, and that’s exactly where our success will lie.

Legal notice

Publisher
TÜV NORD AG
Am TÜV 1
30519 Hanover, Germany
tuev-nord-group.com
info@tuev-nord-group.com

Editorial staff
3st kommunikation, Mainz, Germany

Concept and design
3st kommunikation, Mainz, Germany

Translation, English edition
Jonathan Bruton, Shrewsbury, UK

Photography
Adobe Stock [pp. 12, 16]
Moritz Frankenberg [p. 20 below]
Felix Matthies [pp. 16 top left, 23 – 24]
Christian Nielinger [p. 12 top]
Samsung Electronics [p. 19]
Jeff Schad [pp. 8 – 9]
Henning Scheffen [pp. 4 – 5]
Frauke Schumann [pp. 11, 15, 19 top left, 23 top]
Eric Shambroom [pp. 6 – 7]
Dieter Sieg [p. 20]
TÜV NORD GROUP [pp. 19 top centre + top right, 27 – 28]
Peter Venus, Capital Headshots Berlin [S. 16 top right]

We would like to thank Samsung Electronics Co., Ltd. for the kind support and for providing an image.

TÜV NORD AG
Am TÜV 1
30519 Hanover, Germany
Telephone +49 511 998-0
tuev-nord-group.com
info@tuev-nord-group.com