Knots secure us. Provide support. And create trust. But how exactly does trust come into being? What role does it play in everyday lives? And why is this feeling so important for economic success? Read about the world’s most fascinating resource.
Mutual trust is an essential mainstay of our co-existence. Whether in our personal lives, in politics, in the media or in business, without a basic level of trust in other people our society would cease to function. The sociologist and philosopher Niklas Luhmann once described trust as a “strategy of the broadest range”: only when we can rely on our counterpart to play fairly and abide by contracts, agreements and applicable laws are we able to expand our horizons. A person who can trust views the unknown first and foremost as an opportunity. A person who cannot trust will never be able to move beyond their very limited sphere because anything new always brings uncertainty. In this respect, trust is the indispensible basis for progress, innovation and further development.

This issue of our company magazine is consciously devoted to the key issue of trust. After all, the term is found in the title of the magazine: ABOUT TRUST. Trust is the central asset for TÜV SÜD, even more so than for most other companies. That is why we continue to make every effort to live up to the level of trust placed in us by our customers and by society. Find out more about this starting on page 28.

I hope you enjoy reading the magazine!

PROF. DR.-ING. AXEL STEPKEN
Chairman of the Board of Management of TÜV SÜD AG
Focus on

TRUST

ABOUTTRUST.TUV-SUD.COM

You can find even more exciting stories, interviews, videos and reports—on the content hub of ABOUT TRUST. For instance, find out which seven key technologies we should be able to better rely on in the future. Or join TÜV SÜD experts hot on the trail of brazen product counterfeiters all around the world.

tuv-sud.com/abouttrust/19_1/

PUBLICATION DETAILS

PUBLISHER TÜV SÜD AG, Westendstraße 199, 80686 Munich, Germany | Project Director and Editor-in-Chief: Jörg Riedle | Contact: +49 89 5791-0, info@tuev-sued.de | REALIZATION muhlhausmoers corporate communications gmbh, Invalidenstraße 112, 10115 Berlin, Germany, info@muhlhausmoers.com | Project Director: Stefanie Lysik | Editorial Director: Thomas Schmelzer | Creative Director: Anja Hamann | Art Director: Áine Gibbons | Image Editor: Jan Steinhauer, Charlotte Zeilerhoff | Editorial Staff: Felix Enzian, Angela Nguyen, Till Schröder, Lena Schulte | English Translation: Anthony B. Heric; English Editing: Penelope Krumm | PRINTING G. Peschke Druckerei GmbH, Taxisstraße 4, 85599 Parsdorf, Germany

The contents of the magazine are protected by copyright law. ABOUT TRUST is printed in a climate-neutral manner and on paper from responsibly managed forests.
FIRST WHALE WITH TÜV SÜD SEAL OF APPROVAL

Since the beginning of 2019, a very special test object has been hanging in a lecture hall at the Justus-Liebig-Universität in Gießen, Germany. The experts from TÜV SÜD have inspected the statics of a whole whale skeleton. The sperm whale, measuring 15 meters long, died off the coast of Helgoland in 2016. Employees of the Institute of Veterinary Anatomy brought the animal to the university, dissected it and then put the skeleton back together, which meant reassembling the skull, forty ribs and a lot of other bones. Even during the dissection, TÜV SÜD experts were hard at work performing a structural analysis of the skeleton. Now the whale is hanging safely over the heads of the students.
What does the transformation to industry 4.0 mean for companies? What do they have to prepare for? And: How can they plan safely? A new tool from the Smart Industry Readiness Index is now helping companies in Singapore to find answers to these questions. With the prioritization matrix presented for the first time at the Hanover Messe, companies can analyze which changes would have the greatest impact on their digital transformation. TÜV SÜD checks whether the solutions for Industry 4.0 are safe and reliable. The planning tool was developed in cooperation with TÜV SÜD, Singapore’s Economic Development Board, consulting firm McKinsey and technology groups SAP and Siemens. The goal of the cooperation is to develop tools that will help manufacturers in Singapore accelerate their digital transformation.

Cyber Security Experts worldwide wanted

According to a worldwide study by the non-profit organization (ISC)², the global economy needs at least three million additional cyber security experts. As a result, almost one of every four companies is suffering from a shortage of skilled workers. The study finds that North America needs around 500,000 such specialists, while there is a gap of about 142,000 IT experts in Europe, the Middle East and in Africa. Asia is suffering the most from this lack of expertise, with nearly 2.1 million skilled personnel needed.

of all Europeans place more trust in AI than they do in politicians. This is the result of a study by Spain’s IE University, which surveyed 2,500 European citizens. One in every four would be more likely to entrust important political decisions to an artificial intelligence than flesh-and-blood politicians. In the Netherlands, an incredible 43 percent of those surveyed would prefer to be governed by algorithms instead of people.
A QUESTION OF TRUST

A self-driving car turns a corner just as a pedestrian steps into the street—this scenario could soon be an everyday occurrence.
Self-driving cars and buses may soon take over the wheel from us. Yet many people have concerns about relying completely on technology while out in traffic. Whether we trust technology or not determines its fate.

When Christian Müller wants to explain how artificial intelligence (AI) in autonomous vehicles can make life-or-death decisions, he plays a video. On his computer monitor, a white car appears. Traveling at about 50 kilometers an hour, it’s approaching an intersection and is making a left turn when a man suddenly steps into the crosswalk directly in the vehicle’s path. Instead of braking or swerving, the car remains on course. There’s a crash. Müller keeps a straight face. He already knows the tragic results. “Well, the artificial intelligence wasn’t so smart there,” he says.

The video scene is a simulation, the pedestrian, an avatar modeled on real movement data, and the auto, a projection from the underlying artificial intelligence. Only Müller, the scientist, is flesh and blood. He works at the German Research Center for Artificial Intelligence (DFKI) in Saarbrücken, Germany—nestled in the rolling hills between Luxembourg and Metz, France, on the Saar River—and is doing everything he can to ensure that such accidents happen only in simulations in the future. Müller is investigating how autonomous vehicles behave out on the roads in traffic with AI at the wheel. He is also working with TÜV SÜD and other partners to develop testing methodologies for these types of AI.

On his computer, Müller selects a different AI variant for the autonomous car and starts the scene again. The car again approaches the intersection and again begins to make a left turn. But this time the scene doesn’t end in tragedy. As the pedestrian enters the crosswalk into the vehicle’s path, the car easily swerves out of the way. “I’d be more likely to trust this sort of AI,” Müller says.

The simulation on Müller’s computer monitor is just one of countless situations that self-driving vehicles will have to cope with out in real-world traffic in the future. Yet it demonstrates what will be important no matter the circumstances: Will we trust the machine, its sensors and its enormously complex intelligence—or won’t we?

It’s the question that will determine whether autonomous vehicles will achieve a breakthrough in the coming years. Whether at some point in time there will be cars with sleeping passengers behind the wheel on the autorhans. Whether cars will be looking for their own parking spaces in the future. And whether driverless taxi fleets will be chauffeuring us through city centers any time soon. It is a question whose answer will also determine what the future of our mobility will look like.

FIGURES VS. FEELINGS

For answers to this question, statistics are a good place to start. Currently, about 80 to 94 percent of all traffic accidents around the world are caused by human error. Autonomous vehicles could reduce this high rate to a minimum, so the expectation—the consulting firm McKinsey, for example, predicts for the USA
STUCK ON YOU
Stickers are stuck most everywhere—including on stop signs. It’s a problem for AI in automated vehicles: it sometimes incorrectly categorizes the sign—and subsequently draws the wrong conclusions.

DRIVE ALREADY!
Human beings can communicate without language: through signs, facial expressions, a single glance. The sensors, cameras and software brains of automated vehicles have had great difficulty understanding such gestures up to now.
**MIXED TRAFFIC**

The transition from manually driven vehicles to autonomous ones isn’t happening overnight. In the transition phase, machines must take into account people and their unpredictable behavior.

**ZIGZAG**

Is that guy going to stagger out into the street or not? What can be difficult for people to anticipate is even more difficult for autonomous vehicles. Since the vehicles lack any type of intuition, they first have to wait and observe for a long time.

**GAME OF THORNS**

Trees and shrubs appear differently depending on the season. Leaves grow and then fall off, bark peels, buds sprout. This can confuse the sensors and AI—leading them to perceive obstacles where there are none at all.

**HOMEWORK**

Automated vehicles can already safely deal with a wide array of extreme situations. At the same time, there is still quite a lot to be accomplished along the path to completely autonomous vehicles—as these examples show.
that the market penetration of highly automated vehicles could enormously reduce fatal accidents by the middle of the century.

On the other hand, many people are deeply skeptical about driverless vehicles. According to a study conducted by the Baden-Württemberg Cooperative State University, two of three respondents believe that a lack of trust in autonomous vehicle technology could complicate its acceptance. Almost as many study participants also expressed fear that hackers could target the extensive software in the vehicles. The German online portal for statistics, Statista, found that the idea of fully automated driving systems generated negative associations in almost half of those surveyed.

On top of all this is people’s overestimation of their abilities. “Almost everyone believes they drive much better than they actually can,” says Andreas Herrmann from the University of St. Gallen. For his book Autonomes Fahren: Wie die Autonome Revolution unser Leben verändern wird, he set man against machine in a simulator. The results: in the majority of situations, the machine was better. “However, we also saw that the machine reaches its limits in more complicated traffic situations,” Herrmann adds.

These critical situations are the crux of the matter for the future. “If we are to hand over control when driving, we must have enormous trust in the system’s safety and security,” says Global Head Autonomous Driving Dr. Houssem Abdellatif at TÜV SÜD. “That’s why we must work with manufacturers to prove that the technology can guarantee this safety and security.”

This is exactly what scientists, entrepreneurs and inventors have been working on for years. TÜV SÜD is also working on creating solutions in a variety of projects around the world. Together they’ve managed to make the technology safer, more transparent and more verifiable. And, together, they are tackling the next major challenges.

On the task are people like Marius Zöllner, who is working with TÜV SÜD testing self-driving vehicles in real traffic at the Research Center for Informatics (FZI) in Karlsruhe, Germany. Inspectors like Peter Salzberger, who is working for TÜV SÜD in the PEGASUS project to ensure that autonomous vehicles don’t make any driving errors on highways. And Christian Müller, who is unlocking the secrets of artificial intelligence in Saarbrücken.

DEMYSTIFYING AI

Müller’s computer screen is now displaying tables, graphics and schematics. As he clicks from slide to slide, words and abbreviations flash across the monitor, including Grey Box Testing, Deep Reinforcement Learning and APPL. Müller is working with his team, plus the colleagues from cooperation partner TÜV SÜD in Munich. “Basically we’re all working on demystifying artificial intelligence,” he says.

In the project openGENESIS, Müller is working towards this goal with TÜV SÜD and additional project partners to enable vehicles to make independent decisions. It was this project that made the rapid rise of autonomous driving in recent years possible in the first place.

OPENING THE BLACK BOX

The breakthrough for driverless driving is mainly due to the rapid increase in computing power on microprocessors, as well as new and improved sensor technology. Only this combination has allowed artificial intelligence to finally develop its full potential. It is now unbeatable in finding patterns in vast amounts of data and drawing its own conclusions. There are many areas in which it has long since surpassed human brainpower.

Yet this technology still has one big catch: hardly anyone completely understands exactly how it works, what precisely is going on inside AI’s black box. Why an AI can recognize millions of pictures of dogs and then suddenly identifies a hamster as one; why it can drive for thousands of kilometers along country roads and through intersections without a mistake and then suddenly stops in the middle of an intersection. It’s still something of a mystery.

To solve this mystery, Müller, his team and the project partners are, to put it in simple terms, proceeding as follows: first, he combs the huge datasets to find situations in which AI has previously been pushed to its absolute limits. In a second step, he recreates the situations virtually. To do this, he uses datasets that his team has gleaned from actual movement profiles from road users. Next, various AI systems compete against one another in the virtual situations. This is where Müller looks into the black box. Finally, he checks to see if the virtual situation can be transferred back into the real world.

For openGENESIS Project Manager Matthias Eicher at TÜV SÜD in Munich, each of these results is a new building block on the road to consistent and reliable testing of artificial intelligence in self-driving vehicles. “We want to build a community with openGENESIS in which each partner utilizes their various strengths to investigate and shine a light on the subsections of AI,” he explains. Gradually, the big overall picture will grow. “Our ultimate goal is to completely understand the tech-
From the computer to the streets

To ensure approval, autonomous vehicles must demonstrate that they can drive safely under real-world conditions, in everyday traffic, not just in a simulation. This is the specialty area of Professor J. Marius Zöllner, who holds a doctorate of engineering. At the FZI in Karlsruhe, where he is also a member of the board of directors, the computer scientist heads to the tools he uses for these tasks. There are two test vehicles parked in a garage, the trunks jam-packed with processors, cables, circuitry. The car bodies are equipped with more than two dozen cameras and sensors. Where the air conditioning is normally located on the dashboard are three selector buttons: normal, assisted, autonomous.

In field tests, the cars drive themselves through intersections, stop at signals and navigate through the city’s streets. “In the middle of Karlsruhe,” Zöllner clarifies. Researchers in the cars only intervene in problematic situations during such test drives. Zöllner oversees Germany’s first testing grounds where self-driving vehicles are already being tested in urban street traffic. In order to ensure safety and collect as much data as possible, the researchers have also installed sensors and cameras at intersections, in the asphalt and on bridges.

On a touchscreen as big as a kitchen table, Zöllner shows what can be done with this data: a virtual, four-lane intersection, traffic lights, stop lines, a tramway bridge, a whole lot of colorful cars. “This isn’t a simulation, but is actually a real intersection in Karlsruhe,” Zöllner explains. The cars are moving as they do in real life. The bicyclists and pedestrians behave as they do in real life.

Invisible obstacles

Observing this intersection, Zöllner and his team have learned that about one driver an hour makes an illegal U-turn. That bicyclists sometimes cross the intersection against the red light. And that pedestrians in a hurry sometimes scurry through the crosswalk at the last second. Fortunately, they can use this data to test real everyday situations. For instance, how their test vehicles would behave on a spring morning with some light fog when they are entering an intersection at exactly 34 kilometers per hour behind another vehicle that suddenly slams on the brakes. “It allows us to collect extremely valuable data,” Zöllner says. So far, however, there is no uniform worldwide system to catalog and store this data.

Another challenge is the quirks of some of the sensors. Every technology has strengths and weaknesses. Cameras have trouble when there is backlighting but can recognize colors. Radar waves fail in tunnels but are good at measuring distances. Laser sensors are very precise but cannot identify color. Together, the sensors and cameras cover all possible situations. Yet sometimes glitches crop up. On the test course in Karlsruhe, an invisible obstacle suddenly appeared in an intersection during winter. The test vehicle abruptly stopped every single time. “The technology saw a monster where there was none,” Zöllner explains. At some point his team realized that the sensor and to develop the requirements for testing and certifying AI in vehicles.”

LEVEL 4
The vehicle takes over all driving functions in predefined situations. The driver becomes a passenger for this time and can even take a nap.

LEVEL 5
The vehicle is fully autonomous. Passengers must no longer intervene. This is still a long way off, however.

Strong together

Autonomous vehicles are equipped with dozens of sensors and cameras that mutually complement one another. Together they cover all the areas around the vehicle.

- Surround View
- Park Assist
- Traffic Sign Recognition
- Lane Departure Warning
- Cross Traffic Alert
- Emergency Braking
- Pedestrian Detection
- Collision Avoidance

- Ultrasound
- Lidar
- Long Range Radar
- Camera
- Medium Range Radar
- GNSS
sors were incorrectly interpreting reflections from bushes along the roadside.

Despite all the challenges, Zöllner thinks that vehicle automation will continue to accelerate. Scenarios with multistory parking structures and company premises where cars look for empty spots and park themselves—or even semi-autonomous driving on the autobahn—is something he considers realistic in the next ten to fifteen years. But he also believes that it will still take some time before vehicles will be able to manage every situation without a human driver. There are still too many uncertainties, risks that are too great, costs that are too high.

**RESOURCE: TRUST**

For many people, there is also still too much skepticism. Armin Grunwald, Professor of Philosophy of Technology at Karlsruhe Institute of Technology, has been studying the societal consequences of technological advancement for years. He’s learned that the majority of people generally view technical progress in a positive light. At the same time, he also knows that for every technological innovation, there’s one resource that is more important than all the others: “Nothing works without trust,” he says.

For autonomous driving, that’s why it’s a matter of appropriate diligence and a measured marketing launch. It’s about shifting down a gear and not just banking on speed. This is the only way to learn from the mistakes that will inevitably happen at some point and to improve the technology accordingly. “I recommend that they take time and that not everyone bends to economic pressures,” Grunwald says. This will also allow customers to get a better feel for the new technology.

Author Andreas Herrmann has also observed in his research that it may indeed need some time. When he sent his subjects on a test drive in a driving simulator, at a certain point during the test he gave them the instruction to turn the driver’s seat to face backwards and let the computer keep driving. Herrmann was surprised at how great the inhibitions were to handing over control, even in a simulator. “An independent testing and certification process for autonomous vehicle technology is undoubtedly an important step in building trust,” he says.

This next step for highly automated driving on the autobahn is currently being developed in PEGASUS. In this joint project, sponsored by the German Federal Ministry for Economic Affairs and Energy, car manufacturers, suppliers, research institutes and TÜV SÜD—as the sole testing organization—are drafting standards and regulations for the uniform testing and approval of highly automated driving functions. “First it’s all about developing the guidelines for uniform testing,” says Peter Salzberger, who is heading the project for TÜV SÜD. It may sound trivial, but in practice it’s an extremely complex undertaking. Which driving scenarios must be tested for approval? Which of these should be real-world tests, and which simulated? How often must the highly automated vehicles run through a particular situation? How specific do the requirements have to be? Where do the risks of automation lie? And how high does the level of human and technological performance need to be for highly automated driving?

“We had to develop standards for the virtual simulations, standards for the software and testing systems that are used, standards for how we plan to design the scenarios for real-world testing sites,” Salzberger notes. Shortly before the end of the project, he’s satisfied with its results. “We’re pretty far along for highly automated driving on the autobahn,” he says. TÜV SÜD provides its own testing environment for safeguarding the highly automated driving functions on its test site, and its industrial partners’ test vehicles are already driving autonomously on the A9 Autobahn between Munich and Ingolstadt.

**THE FUTURE IS ALREADY HERE**

If you want a glimpse even further into the future, you’ll have to travel to Singapore and go to the one-north business park. A pilot project has autonomous taxis gliding along the asphalt between palm trees and high rises. The taxis currently have minders behind the wheel during this testing phase, just in case, but should soon be driving through the city fully on their own. Nanyang Technological University in the western part of the city has a built a small mini-city on a two-hectare site to test autonomous vehicles as realistically as possible. TÜV SÜD is assisting here as a strategic partner in the CETRAN project, which is working on making highly automated buses and cars as safe as possible. The city plans to have a fleet of such buses on the streets by 2022.

So Singapore is potentially becoming a place where highly automated driving may have its first real breakthrough on a larger scale. Yet here, too, consumers will ultimately have the final say about the technology’s fate. “We want to ensure throughout the world that a vehicle has been tested to the highest possible standards of technology and rigor,” Global Head Autonomous Driving Abdellatif says. “This vision will only become a reality when people trust the technology.”
This is what the future could look like: autonomous taxi fleets snake through the urban canyons, driverless buses shuttle us through the city. In Singapore, parts of this vision are already reality.
Mr. Matouschek, as an economist you deal with optimal decisions every day. How do you yourself decide whether to trust someone? In the best case, I already know the person. Then I know how they think and can assess whether they will actually keep their promise. For instance, one of my colleagues never goes back on his word because that would literally give him a guilty conscience. It’s easy to trust someone like that.

But we often deal with people we’ve never met before. That makes everything more difficult. Particularly when a stranger is also pursuing their own business interests or is working for a company that by definition is trying to maximize its own profits.

So you can trust someone like that? In most cases, yes. Otherwise our everyday lives would never work at all. But I always ask myself two questions beforehand. First: Does my counterpart have a long-term interest in keeping a promise although it might be more advantageous to break it over the short term? And second: Would other people find out if this person cheated me? The higher the long-term interest of my counterpart and the more transparency there is, the more likely I am to trust the person.

How often have you been correct using this method? It usually works pretty well. But sometimes it doesn’t, of course. When I moved into a new house with my family a few years ago, my wife and I hired an interior decorator and paid in advance. That was admittedly somewhat naive. The decorator did a good job for a while, but then he was suddenly gone. Just vanished off the face of the earth.

Did you research the decorator beforehand? Friends recommended him to us. And we were certain that he would be interested in our recommending him later as well. But apparently we were wrong about that. There were also no online reviews of him. To that extent, there was a certain lack of transparency.

You research trust as an economist. Have your findings helped you? Yes, there is always overlap. In the
specific case of the interior decorator, for instance, it was interesting because he should have had a strong theoretical interest in our recommending him to others. So much business in his branch comes from personal references. But sometimes things in real life work differently than they do in theory. As an economist and game theorist, I also look at trust through a very special set of glasses.

But they might also gamble that you’ll never come back to that city anyhow and other guests won’t find out about your dissatisfaction. That’s exactly the trade-off the hotel has to consider. How they decide depends strongly on the circumstances. Taking a game theory approach, we’d argue that it depends on how often the game—in this case my choice of a hotel—will be repeated and how high the level of transparency for this decision is. Online rating portals, for example, increase the chance that other guests would find out about my experience. The transparency increases. And with it, the incentives for the hotel to keep its promise.

So you’re saying whether we can trust someone simply depends on whether they expect long-term benefits from it? It’s not quite that simple. For instance there is an experiment in which two people who have never met before play a unique game. The rules are that person A receives 10 euros. This person may then decide whether they give person B some of the money. If person A shares the money, the money person B receives gets tripled. Afterwards, person B can decide whether or not and how much of the tripled amount goes back to person A. And after that, they never see each other again.

Theoretically, person A would keep all the money and the game would be over. And that’s exactly what doesn’t happen in practice. Instead what we see is that people trust one another. On average, person A gives about half of the money away, and person B returns about the same amount. People

And what do you see? Incentive systems above all else. I’m interested in whether a person keeps their word and what types of incentives support that even though there’s no benefit over the short term. Incentives are everything.

Can you provide an example? Let’s say that I am taking a business trip and pick a hotel because it advertises an absolutely gourmet breakfast. It is interesting to see whether the hotelier actually serves me breakfast of the promised quality after I’ve checked into the hotel. Once I’ve paid, the hotel is faced with the increasing temptation to serve me a more mediocre breakfast to save on costs. In my definition, the hotel would be trustworthy when it has the will to prepare me the promised breakfast despite this temptation.

Why would they do that? Because alongside the short-term temptation to maximize profits is the long-term incentive. As long as the hotel isn’t planning to close anytime soon, it’s also dependent on paying guests in the future. For instance on me, the next time I’m in that city. Or on other guests who decide to book the hotel on my recommendation.

So why does it happen? I personally believe that we simply all have a certain basic level of trust within ourselves. Some researchers explain this basic trust as providing an evolutionary advantage. It would be very difficult to imagine us living together in large societies with divisions of labor without us mutually trusting one another in advance.

On the other hand, there’s all sorts of fibbing going on in real life. This is also reflected in the experiment. As soon as the stakes are increased, the shared contribution decreases. So there are limits to our basic trust.

And that brings us back to incentive systems? Exactly. If for instance you modify the rules so that there are more rounds of game play, you see that the mutual trust increases or decreases.
So we don’t actually need trust if there are watertight contracts? As long as I clearly define the quality of a service or a product in a contract, fully verify it afterwards and, when in doubt, can sue, then I don’t really need trust. However, the point is that the exact definition and immediate testing of a service ends up being difficult and is often quite expensive in huge sections of the economy. What exactly does a gourmet breakfast entail? And what are the precise details of what you expect from an interior decorator?

Why is that? Because markets without trust wouldn’t work nearly as well as they actually could. If you as a customer don’t trust me, then you’ll stop buying from me even if we both profit from the business. And if you’re an investor and don’t trust that I’ll pay back the money, then you won’t loan me any even if I have an extremely good business idea. Many deals wouldn’t take place without trust. There would be less value creation. The market economy would wither on the vine.

At the same time, this trust can always be taken advantage of. That’s true. Fortunately, our experiments show that taking advantage of someone’s trust doesn’t pay off over the long term. Instead what is rewarded is a good reputation. Acting in a trustworthy manner in modern market economies is good for the soul and also good for the bottom line.
RADIM MATUŠŮ TESTING ENGINEER IN PRAGUE “Emissions regulations are constantly changing. To ensure that the legal requirements are met, I regularly inspect cars’ pollutant emissions using special tests. My customers come to me for a wide variety of reasons. I test whether the mass production of new car models complies with the regulations. I conduct quality assurance tests for previously approved vehicles that are already out on the streets. Or I test new types of vehicles.

What I like most about my work is that I have so many different things to do as a TÜV SÜD testing engineer. I’m in the lab every day and conduct inspections and tests with my team. I also work in the office, communicating with our customers.

To test a vehicle, I first have to determine what type of vehicle it is. I check the vehicle identification number, the model type and tire pressure. Next, I fill up the vehicle with the appropriate fuel and fully charge the battery. Then the vehicle is ready for testing. It goes through several phases of tests and situations. I measure the emissions of pollutants and, at the end, calculate a final value. Depending on the result and what the regulations require, I then decide whether further tests are necessary.

It’s very important that I always work carefully and focus on the details. After all, our customers trust that the testing results are correct. That’s why I place great importance on their accuracy. If something is off, then I’ve obviously not done a very good job.”

FOCUSING ON DETAILS
Radim Matušů pays attention to every detail at work. It’s the only way he can ensure that his measurements are absolutely correct.
Three safety airlocks, a separate power supply, walls of steel: in the middle of Hamburg, laboratory technicians research some of the world’s most dangerous pathogens under the strictest safety precautions. About working between Ebola and peracetic acid.
To work in the laboratory you have to wear three pairs of gloves (left) and a special suit made of completely tear-resistant material (right).
There's a very special dream that every employee in the high-security laboratory eventually has at some point. Elly says that once you've dreamed this one particular scenario, that's when you know you're really part of the team. The dream is actually a nightmare and it goes like this: it's a workday like any other. You go through the three safety airlocks into the high-security laboratory. You do your research on the most dangerous pathogens on the planet. And, as always, you want to leave the lab after three hours because that's the maximum limit you're allowed to work at a time. So you head over to the airlocks, and as you are about to press the button for the shower of peracetic acid to disinfect yourself, you finally notice that you aren't wearing the protective suit. You begin to panic.

"And the point is that you're not panicking because you've been working with the Ebola virus without a protective suit," Elly explains. "The problem is that you aren't wearing the suit and you have to walk through the peracetic acid shower. And it's caustic." She laughs. "When your fear of everything else is greater than your fear of the virus, that's when you've really 'arrived' at the lab."

Lilly is 32 years old and has been working for five years as a biology lab technician in the high-security laboratory at the Bernhard Nocht Institute...
for Tropical Medicine in Hamburg. For security reasons, her full name cannot be used here. The high-security laboratory in Hamburg is one of just four such labs in Germany that fulfill all the requirements for the highest security level, S4. It’s a lab that its employees affectionately call “The Submarine” because it’s a unit unto itself, a self-sufficient building within a building, completely separated from the rooms surrounding it, with its own supplies of power and fresh air—as required by international standards. A laboratory, about half the size of a tennis court, all of shining metal. Walls, tables, shelves, everything is made of stainless steel. The silver doors have round windows, like portholes. There are bright blue hoses dangling from the ceilings everywhere, delivering compressed air.

Highly infectious pathogens such as the Ebola, Lassa and Marburg viruses may be studied only in these types of laboratories. An infection with any of them can lead to life-threatening bleeding and organ failure in just days. These are some of the world’s most deadly viruses. The employees inside must trust that every protective measure works. And the population outside that no viruses escape. That the airlocks remain sealed and that everything is working properly.

Two of the laboratory’s three rooms form traditional lab bays. These contain white incubators that keep the temperature for the dangerous viruses at a constant 37 degrees Celsius. The scientists carry out their experiments in the next room. They work on sterile workbenches, separated from the viruses by a glass pane and a flow of sterile air. There are monitors and microscopes on the tables. The researchers still use fax machines to send their notes to the office. They’re only allowed to take the papers out of the lab once a year when the entire facility is sterilized and serviced. Even normal waste must be decontaminated before it can be disposed of outside as laboratory waste. To keep the laboratory clean, its employees take turns as janitors because no cleaning staff are allowed to enter the lab.

Lab animals await their fate in the third room. Mostly regular laboratory mice, but also the Natal multimammate rat: a common African rodent that is known to harbor the Lassa virus. Elly checks in on the animals every morning. She also carries out experiments on them.

Before Lilly can enter the lab, she must put on her protective suit and pass through the three airlocks. The pressure drops behind each of the doors to prevent any contaminated air from escaping in the event of an emergency. Only
twenty people have access to the laboratory. Just five at a time are allowed inside. The only way out is through a four-minute decontamination shower of peracetic acid and water, after which the protective suit is pathogen-free. Lilly is part of a team researching the Lassa virus. Lassa is widespread in West Africa and probably triggers an overreaction in the immune system. After flu-like symptoms, a continuous fever sets in. The liver and kidneys become enlarged, the skin breaks out in a rash. Because no effective therapy has yet been found, about one of every seven patients dies from the disease. The researchers are trying to find a treatment and also to understand exactly how the virus works.

The viruses being researched in the lab may sound exotic, yet it’s not impossible for them to crop up in Germany. The Marburg virus, for example, first appeared in 1967 in a lab technician in Marburg. When a number of people came down with high fevers and gastrointestinal problems and then died as a result, a state of emergency was declared for the entire town. The Lassa virus has also been repeatedly brought in to Germany. And August 2014 marked the date of the first patient to be treated for Ebola in Germany.

The high-security laboratory is located in the St. Pauli neighborhood in Hamburg, not far from the Reeperbahn red-light district. Where exactly the lab is located within the institute is a secret. Anyone who enters it is first reviewed by the secret service. That’s why we cannot print Elly’s full name nor photograph her. The risk is too high that someone might threaten her or infiltrate the laboratory to steal the viruses that she and her colleagues are researching.

To put on her protective suit, Elly first takes off her gray skirt and white sweater and puts on white trousers and a blue shirt. “It gets warm in the suit,” she says, “and if I’m going to sweat, then at least not in my own clothes.” Next, she clips a walkie-talkie onto the waistband of her trousers. The walkie-talkie has a fail-safe mechanism, similar to a dead man’s switch, that sounds an alarm if the device has been lying horizontally on the ground for some time. This gives the employees the assurance that they will receive immediate help if they should collapse or faint. The two supervisors who continuously observe their coworkers in the safety lab and maintain radio contact with them would be notified immediately. If necessary, they would begin an evacuation.

Lilly pulls orange gloves over her fingers, the first of three pairs that all employees must wear, one on top of the other. Then she secures her headset with a bandana. Now comes the suit. “It’s made of absolutely tear-resistant material,” she notes—made entirely of white PVC. “You could even walk through contaminated water in Chernobyl wearing this.” The protective suit is the life insurance for employees at the high-security lab. Elly trusts it to keep her safe. Filtered air flows into it through blue tubing. The air in the suits is at a higher pressure than the air in the lab, so that any escaped viruses would be pushed away. Once Elly has inflated her suit, she looks like an astronaut.

She slowly paces back and forth a few steps. Her gait is sluggish. In one hand she holds the blue tubing that supplies her with filtered air. As soon as she detaches it, her transparent face shield begins to fog up after a few minutes. Then her cheeks turn red as it gets warm. In the lab, the employees have established the rule that everyone must take a break after three hours. They can’t concentrate longer than that anyhow under such conditions.

Lilly can find some appeal in a few of the things that others might consider a burden. “Everything is different in the suit, particularly your senses,” she says. “Your sense of touch is different through the three pairs of gloves. You hear differently, with the constant hissing of the air supply, and there’s beeping now and then.” Elly must communicate in a different way, mostly through sign language. But most of all, she must be absolutely focused and alert at
**POSITIVE PRESSURE** Filtered air flows into the suit through blue tubing. The higher pressure of the suit’s air compared to the air in the room means that any potential escaped viruses would be pushed away.
all times. The physical component of the lab work is often underestimated, she says. After her first times on the job, when she was much more tense, Elly would feel completely exhausted. It took a while before reality outside the lab felt normal again. She initially couldn’t listen to music for hours, but now she listens to all sorts of music even while inside the suit.

Because of all this, new employees must undergo a strict, multistage training program. Before anyone is allowed to work alone with a virus, they must have been inside the lab at least twenty times with a co-worker. “Everyone gets a very slow introduction,” Elly explains. “I always try to teach the new ones as much as possible outside the lab.” With the student she most recently trained, she had him put on the three sets of gloves in his regular office. That allowed him to experience the way that completely familiar items, like pipettes and syringes, felt through the layers of rubber. Elly finds it especially important to familiarize the newcomers with hazardous incidents. “There’s always a chance that all of a sudden an alarm goes off in the lab because the air pressure deviates too far from the target value because of a door that is closing too slowly,” she adds. “Or the tech department calls and says there’s a small problem with one of the decontamination showers and you should use the other one. That can be scary for someone who’s never experienced it.”

The innumerable repetitions, the slow internalization of movement sequences and the precise technical knowledge about the safety precautions gradually give the employees a feeling of control of their own day-to-day work. They develop trust in the protective measures and in their own abilities. Despite all of this, there’s always a residual risk. In 2009, a scientist at the Bernhard Nocht Institute in the high-security laboratory accidentally pricked herself with a needle through her protective gloves while working with the Ebola virus. She had just used the needle to infect mice with the virus. Residues of the deadly pathogen could have made their way into her bloodstream. She was immediately placed in an isolation ward and it would have been Germany’s first case of Ebola. It took days before she was declared virus-free and was able to leave the hospital.

You might think that safety standards like the ones here would be the rule and not the exception. Unfortunately, Elly experiences the exceptions once or twice a year. She and her team fly to Nigeria, usually between December and March, during the dry season, when the rats that carry the Lassa virus scurry back into human-made structures. There are frequent outbreaks of the virus around this time. It’s a rough four weeks. Lilly works twelve hours a day, seven days a week. In a hospital near the border with Benin, she helps diagnose cases of the Lassa virus with a portable minilab. Sometimes when she receives a sample she sees that the patient is a three-month-old newborn, sometimes she learns that the virus has wiped out an entire family. Lilly becomes thoughtful talking about it. “When you’re in Nigeria and you see patients, and you also see relatives and you hear their stories, that’s when it suddenly becomes clear what this disease actually is.” Lilly believes that everyone who works with these types of viruses should travel now and then to the areas where there are outbreaks so as not to forget the human cost. When there is an outbreak, the team from Hamburg needs 72 hours to get to the location with their mobile lab and start doing diagnostics. They travel without the lab if they’re conducting research projects: just this morning, a four-member team set off for Congo. Since the start of the Ebola epidemic there last summer, more than five hundred people have died.

Lilly says her work out in the field refreshes her respect for the virus. The familiar working methods of a controlled environment like the one in Hamburg don’t exist in Nigeria or in Congo. She naturally wears protective clothing when she’s working there and is meticulous about cleanliness, but the viruses are everywhere. Elly has come down with a cold twice on the plane back to Germany—the symptoms are similar to those of an infection with the Lassa virus. If she had also come down with a fever, she would have needed to get herself tested for the virus. Fortunately, that hasn’t been the case so far.
The situation after an earthquake is chaotic, with people trapped, buried under rubble. Even without the aftershocks, more buildings are in danger of collapsing. It’s not an easy situation for rescue teams; they dig for buried victims and tend to the injured but are always in danger of being buried alive themselves. At this point it would be wonderful if robots could take over the most dangerous work. Which they can. Such high-tech devices are already being used—and they’re getting smarter.

The first use of such rescue robots dates back eighteen years. After the terrorist attack on September 11, 2001, they were scrabbling through the rubble in large-scale operations. Dr. Robin Murphy and her team from the Center for Robot-Assisted Search and Rescue (CRASAR) were also there. They guided the mechanical assistants through the ruins and transmitted live images from the robots to the rescue teams, providing the precise information necessary for making correct decisions from a safe distance.

Murphy has been researching robots for more than twenty years. She is one of the pioneers in this field. The first time she started thinking about rescuers made of plastic and steel was in 1995. A truck bomb terrorist attack on the Murrah Federal Building in Oklahoma City, Oklahoma, had shaken the United States. One of Murphy’s students helped with the rescue there and told Murphy about how helpful it would have been to have had small, maneuverable robots to perform certain tasks.

This gave Murphy the initial inspiration. Together with Satoshi Tadokoro, she got the ball rolling in a new field of research into rescue robots in the years that followed. Since then she’s helped with more than 25 rescue operations all around the world. “The robots themselves aren’t anything special,” she says. “But using them is.” Since the surroundings have usually been completely destroyed by a catastrophe, the experts must redefine the robot’s tasks on location for every new mission. Murphy now has three types of robot in her repertoire: helpers in the air, in the water and on the ground.

The most important component for a robot is its software: the artificial intelligence. Because hundreds of hours of video material are easily recorded during disaster operations, intelligent and learning algorithms search through this data and send it to the rescue teams pre-sorted. This allows the teams to more quickly evaluate the images and make better decisions.

The robots have yet to be able to work without human assistance. They are remotely controlled and deliver their sensors’ data to the rescue teams. The situations during catastrophes are simply too chaotic for robots to operate autonomously. The robots are also quite small due to the special circumstances of their use. “They have to fit inside the back of an all-terrain vehicle,” Murphy explains. “Everything has often been destroyed in disaster areas. Transporting anything large and heavy isn’t practical.”

Murphy has ambitious goals for the continued development of her robot rescuers. She plans to utilize the enormous progress made in sensors, microprocessors and artificial intelligence to support rescue teams even more effectively. It’s about getting the right information to the right people at the right time so they can make the right decisions. “My goal is for the robots to be routinely used in rescue missions by 2030,” she says.
Mr. Stepken, trust has been the focus of the company’s philosophy for years, not just since TÜV SÜD celebrated its 150th anniversary in 2016 with the motto “150 Years of Inspiring Trust.” Why is trust so important? Because trust is the glue that holds our society and economic system together. No relationship can survive without trust—it’s no different in our personal lives than it is in the business world. As a customer, I must be able to rely on the fact that a product will deliver what the manufacturer or retailer promises—regarding quality and safety, for example. Likewise, every company that does business with other firms must be able to rely on agreements being honored. And for all technical equipment it must be ensured that it is safe and can actually do what it was purchased for.

Is this the reason why TÜV SÜD’s claim was updated last year to “Add value, inspire trust”? Yes, it is. We are hereby focusing on the key concept behind our work—the way the vast majority of our customers see it: the trust in our neutrality and in our experts’ knowledge is the foundation of everything that we do. We create trust, for instance, by providing our customers with safety and security, by providing access to markets and supporting them in terms of sustainability. “Inspire trust” goes far beyond the previous “choose certainty.” We’re certainly not bidding farewell to our commitment to safety, but instead are strengthening it. We’re doing this by clearly acknowledging that safety serves to create more trust in technologies, processes and partners. We must continue to earn this trust from our customers every single day. That’s why we must constantly work on making our services and our employees excellent in every way. We’re placing a great deal
of emphasis on this as part of the company’s Strategy 2025.

What does trust specifically mean in the modern world, where progress is strongly influenced by software and digital technologies? Digitalization is the major driver of innovation. But one thing must remain clear: every innovation is associated with risks that must be controlled in some way. Ensuring safety and security in the digital era is therefore a very central aspect of digitalization. Without security for IT systems and applications, there is no way to maintain trust in digital processes and technologies over the long term.

What does this mean for a company like TÜV SÜD? We’ve been deliberately expanding our expertise in the digital environment for years. Firstly, we’ve been augmenting existing services with added digital value, for example by advancing the development of automatic image recognition for damage appraisals. We’re also moving into very new technologies, such as additive manufacturing and highly automated driving. We’ve also been hiring personnel for some time now to set up our own cybersecurity unit. Meanwhile our Cyber Security Services has almost 100 employees and operates in Germany, Asia and the United States. I’m confident that there won’t be any service we offer that isn’t affected by digitalization. We’ve synthesized this cultural transformation, which is of central importance for all of TÜV SÜD, into the slogan “from steam to cloud.”

Since last summer, TÜV SÜD has also been involved in the “Charter of Trust”—with the term trust right there in the name. What is that? It’s a cross-sector initiative with 15 strong international partners that was founded over a year ago, spearheaded by Siemens and the Munich Security Conference. What distinguishes the partners in the Charter of Trust is that they have recognized that there will be no long-term trust in the digital economy without cybersecurity. To achieve this we urgently need regulations—and where there aren’t any, we must help create them. That’s why we’re involved.

What are the specific goals of the Charter of Trust? The initiative has developed ten specific principles to help cyber security become an integral part of our society and business. Among other things, we consider it absolutely imperative to take responsibility in digital supply chains and have put together some baseline cybersecurity requirements along the digital supply chain. These requirements address all aspects of cybersecurity, including people, processes and technology. One current focus is also on making cyber security an essential part of university education and of professional development. This is what we’re promoting and what the members of the Charter of Trust are committed to doing.

Public trust in independent technical inspections has been shaken this year. At the end of January, there was an accident in Brazil when a dam collapsed at an iron mine in Brumadinho. TÜV SÜD performed the inspections of the dam in Brazil. The dam breach was a human tragedy and an ecological disaster, and we all grieve with the victims’ families. The investigations of the investigating authorities must uncover what ultimately led to the dam’s collapse. That will definitively take some time due to the complexities of the situation.

What is TÜV SÜD doing concretely to restore the trust that may have been lost as a result? Our over 24,000 employees around the world do a fantastic job, day in and day out. To ensure this, we’ve been implementing comprehensive compliance and control mechanisms throughout the company for many years. These help guarantee the independence, neutrality and high quality of our services. This also includes extensive transparency. In the case of Brazil, it was therefore clear from the outset that we would fully cooperate with the investigating authorities. Furthermore, we’re also undertaking an investigation into internal processes and possible causes for the dam collapse in Brumadinho, supported by in-house and outside experts. Since late February, there is also a scientific expert group with us, comprised of external geotechnical and mining engineers. We brought them in to deal with the assessment of technical issues. We will do everything on our part to completely clear up what happened, and to uphold the trust that people have placed in us.

--- Personalia

Prof. Dr.-Ing. Axel Stepken has been the Chairman of the Board of Management of TÜV SÜD since 2007. He previously held various management positions at ABB in the power transmission and distribution segment in Germany and Indonesia. Stepken was born in Essen, studied electrical engineering at RWTH Aachen and received his doctorate in the field of high-voltage engineering. He’s held an honorary professorship at TU Munich since 2015.
There are 38,000 kilometers of railway track in Germany. A highly complex monitoring system—from barrier gates to encrypted remote control—ensures safety along the routes.

**BORDER CROSSERS**
Train control systems ensure that trains stop when they ignore signals or exceed permitted speeds. More than twenty different train control systems are in use across Europe. To ensure that cross-border train traffic can flow even more smoothly, the common **European Train Control System (ETCS)** standard will be replacing national solutions like the PZB and LZB—intermittent and continuous train protection systems, respectively. The Erfurt-Leipzig line is the first and currently only connection in Germany that already fully complies with all ETCS specifications.

**MESSAGING SERVICE**
The future ETCS wouldn’t work at all without **Eurobalises**. These small boxes are transponders installed directly on the track bed and are indispensable for vehicle positioning in the GSM-R—the Global System for Mobile Communications—Railway. The data they collect provide the foundation for all communication between signal boxes, trains and operations centers throughout Europe.

**TUNNEL VISION**
The sections of track inside tunnels are especially secured, with emergency exits allowing access to the outside in the event of any problem. Newer tunnels can switch off the overhead power lines, have access to radio communications with local authorities and have water for firefighting at the ready. The **Finnie Tunnel** between Essleben-Teutleben and Bad Bibra is 6,965 meters long, the longest of the three tunnels on the Erfurt-Leipzig line.
Signaling systems were one of the earliest safety measures in the history of railways. With the gradual changeover to ETCS, the technology is moving from the tracks into the train. The Radio Block Centers act as the central interface between the train and the signal box. They continuously monitor the journey by radio, report all data to the train and issue the permission to travel on a stretch of track. They are an essential component of ETCS and replace the trackside signals.

Operations centers oversee about 24,000 of the 38,000 kilometers of tracks in the German railway network and ensure that train spacing and timetables are adhered to. The rest will be covered by the main control center.

Axle counters are an important part of the railway monitoring systems. Their sensors count the wagon axles at track entrances and compare them to the number counted at the track exit. The tracks won’t be signaled as free and clear for other trains unless the axle count number is identical.
Here were no public reports about exactly how the malware managed to infect the system of a mechanical engineering firm in Munich. The malicious ransomware could have landed in an employee's inbox as an email attachment disguised as a supposed invoice or advertisement. Once it was opened, no doubt chaos broke out all over the company. What is certain, however, is that the company was hit with a cyber attack in November 2018. With grave consequences: the control systems in production and assembly couldn’t be restarted because the ransomware had encrypted the necessary computer data, rendering it unusable. The company’s production capacity was severely limited for weeks on end. To be on the safe side, email connections to customers and suppliers had to be cut off, and a number of IT servers shut down so that the attack wouldn’t spread even further. The perpetrators allegedly demanded a ransom. No information about the financial losses was made public. At any rate, a massive amount of work was required to get the company back up and running again.

Volker Baier deals with cases like these every day when he reads about the newest cybercrime weapons in the internet forums of the hacker scene. “I’m a hacker myself,” he says. Baier is the chief information security officer at sec-IT, a TÜV SÜD subsidiary. In contrast to the criminal hackers, known as black hats, Baier doesn’t use his knowledge to harm people or organizations. Instead he actually fights cybercriminals by finding and closing security gaps in companies’ IT and computer systems. Baier is what is known as a white-hat hacker, one who hasn’t gone over to the dark side.

**PIRATES AND NINJAS AND SPIES: OH MY!**

“To realistically test a company’s security, I have to think and approach it just like a criminal hacker would,” Moradi explains. He coordinates sample cyber attacks by the good guys as team leader for Penetration Testing. The white hats use a variety of methods for their attacks: “During Penetration Testing, we hijack many security gaps and capture as much data as possible—kind of like pirates,” he notes. During “Red Team Exercises,” in contrast, he and his colleagues sneak in very quietly, like ninjas, and attack a very specific location, for instance a customer database or production controls.

Sometimes the white hats even work like traditional spies. Disguised as alleged visitors or suppliers, they sneak into a company and set out data storage devices, like USB sticks, containing malware. If an unsuspecting employee inserts one of those USB sticks into their computer, it triggers the cyber attack—naturally all completely legal and only with the customer’s consent. “Hackers may be using technology, but “ultimately what is always comes down to is people attacking other people,” says Moradi.

**MIND THE (SECURITY) GAP**

Even if “white” hacking uses the same methods criminals do, the white hats have completely opposite goals—for a company’s benefit. “Our approach is planned in advance with the clients,” Baier explains. In workshops after the “attack,” the white hats provide recommendations about how the security gaps they found can be sealed, for instance by making changes to software systems or by training employees about cyber security. The planned countermeasures in the event of a cyber attack can often also be better orchestrated. As a result, a white-hat attack can help bring a company’s IT security up to an optimal level.

Statistics show how necessary this is: in Germany, nearly half of all medium-sized enterprises have been victims of stolen data, exposed secrets or espionage. Despite this, companies still underestimate the dangers. “Our tests discovered that thousands of industrial facilities are linked to the internet using simple DSL connections,” Moradi says. “These are open gateways for criminals.” So there’s plenty for him and his colleagues to do from their offices in Germany, China, India, Singapore and the United States. Even when a company has made improvements, it doesn’t mean that the white hats can’t find new weaknesses. As Moradi explains, “We find security gaps that nobody thought of.”
They call themselves white hats, snooping around to find IT weaknesses on behalf of the companies that hire them. Meet the good hackers from TÜV SÜD.
Organic foods are traditionally viewed very critically. That’s why their producers have to strive constantly for credibility. It was the same for us in the beginning, when my father switched from traditional sausage-making to organic farming. We no longer wanted to have to lie about the origin and production of our food products, but instead wanted to be able to present them with a clear conscience. Many consumers are worried. They often don’t believe that the meat, eggs or vegetables labeled as organic actually meet the standards for quality that they demand.

The official seals for organic quality are much more reliable than some reports say. It is a criminal offense for companies to wrongly label food as organic. And there are regular inspections for compliance with the regulations. That’s why, as an organic farmer, I can speak for my entire sector when I say: if it’s labeled organic, it is organic.

It’s very important to us that all of our customers can really trust all the foods we offer. Only then are they also willing to pay the price, which is often a bit higher than for other foods because of the more complicated production process. That’s why we don’t rely solely on the organic seal, but instead do a lot more to guarantee our credibility as a producer of organic and artisanal foodstuffs. For example, we list absolutely everything that is in a product on our ingredients lists, even if an additive is below the prescribed threshold. That’s how consumers know exactly what they’re buying.

Furthermore, we focus on transparency. Our customers can take a look behind the scenes everywhere. We offer tours of our farm, bakery, butcher’s shop, cheese dairy, brewery and coffee roaster. All of our customers can assure themselves as to whether our animals are naturally raised, our fields carefully and sustainably cultivated and our foods processed in an unadulterated manner. This creates credibility. Visitors can even watch an animal being slaughtered as gently as possible. Although the killing of an animal is naturally not a pretty sight. However I do recommend that everyone who eats meat should attend a slaughter at least once. So that they know what it means.

Our customers should get to know us as people. While organic seals are reliable and necessary, credibility is even stronger when it develops through contact with people that you trust. And one more thing: it’s not enough for customers to be able to trust in the organic quality of the food. They have to be able to taste it as well.
I’ve been taking photographs from helicopters and small planes for my *Aerial Views* project since 2010. You can show humanity’s interventions on the earth’s surface very well from the air, which is what my project is about. For this photo, I went to the Mojave Desert in California last October. We flew in a helicopter over thousands of mirrors that are set up in the desert there. This computer-controlled solar collector, also known as a heliostat, focuses sunlight on the receptors on the central towers. This solar energy is used to create steam, which in turn powers special steam turbines that generate electricity. This photo is part of my series about solar power plants in the United States and I’ve tried to find visually interesting images on the topic of sustainable and future-oriented energy production.

Bernhard Lang has been working as a photographer since the year 2000. While he got his start in the advertising industry, since 2010 he’s been focusing on his *Aerial Views* project, which has won several awards.
3D PRINTING will define our future, as will CRISPR, BLOCKCHAIN and AI. Why we will soon have to rely on seven key technologies.

Get the whole story at: TUV-SUD.COM/ABOUTTRUST/19_1/FUTURE