hoch3 FORSCHEN

SCIENCE QUARTERLY

Autumn 2016

TECHNISCHE UNIVERSITÄT DARMSTADT

Imprint

Publisher
President of TU Darmstadt,
Karolinenplatz 5,
64289 Darmstadt,
Germany

Editor
Corporate Communication
Jörg Feuck (Editor-in-chief)
Ulrike Albrecht (Graphic Design)
Patrick Bal (Images)

Conceptual design
conclouso GmbH & Co. KG,
Mainz, Germany

Photography (title)
Katrin Binner

Circulation
5700

Next issue
15th of December 2016

Service for readers
presse@pvw.tu-darmstadt.de

Newsletter subscription
www.tu-darmstadt.de/newsletter

ISSN
2196-1506

Would you like to receive the next issue of hoch³FORSCHEN? Please send an E-mail to presse@tu-darmstadt.de

The route to brain software

People make sense of their surroundings by gathering impressions, recording them as internal representations within the brain, and using them to derive behavioural responses. Scientists at the TU Darmstadt are working on developing similar abilities for computers in the near future.

By Hildegard Kaulen

Professor Constantin Rothkopf of the Cognitive Science Centre at the TU Darmstadt is facing a Herculean challenge. He wants to understand how seeing and taking action are intertwined, and how these cycles can be simulated by algorithms. To this end, he needs to understand how nerve cells collect, encode and calculate sensory signals, and how they derive solutions to pending tasks from these processes. Because technical systems will increasingly be equipped with cognitive algorithms in the future, Rothkopf hopes to develop software that can, to some extent, think and act like humans do.

He has the best possible prerequisites for the task. He is trained both in cognitive and computer science, was one of the founding members of the Centre for Cognitive Science and is currently serving as its first director. But, has machine learning not already left his field in the starting blocks? Not according to Rothkopf: „it's true that machines are very capable when it comes to language, number and object recognition", he explains, „and recently the world champion in Go was forced to concede defeat to a computer. Yet", he cautions, „none of these advances really explain how we perceive, decide and act. We don't understand the connections between machine solutions and human solutions. So, if we are interest in developing brain-like software, we need to understand how the brain processes the necessary data, whereby machine learning does help us to a certain extent, but, because it can also result in other solutions than those that we find, we need the aid of cognitive science".

„Not only will cognitive science research lead to new intelligent solutions to difficult problems, it will also teach us a lot about ourselves".

How come our three pound brains can vastly outperform any supercomputer? „The brain works with incomplete data" Rothkopf explains. „It generalises. When children know what a cat is, they recognise every kind of cat, even in the form of stuffed toys or sketches on paper. So far, computers have struggled to match this ability. In addition, the brain learns autonomously and is self correcting. Computers work comparatively unidirectional".

Rothkopf is particularly interested in natural behaviour, which always involves uncertainties. Planning in conditions of uncertainty is therefore one of his research foci. He has his test subjects spread peanut butter on a slice of bread. From a data processing perspective, this is a highly complex procedure, because, as with any sequential task, spreading on bread needs to be learned and planned. You need a plate, a knife, bread and peanut butter, all of which needs to be fetched and placed on the table. Then, all of these things need to be located in the right order, picked up, used correctly and put down again. „A process of this kind requires eye movement, attention, a working memory, sensory information processing and the ability to direct actions", says Rothkopf. „It involves a lot of observation and data processing. Children only acquire the ability of perfect sequential planning around the age of 9 to 11.

Because Rothkopf is particularly interested in seeing and taking action, he tracks the eye and body movements of his test subjects as they make a sandwich. „Seeing helps them to reduce uncertainties during the process", he says. The process is accompanied by many rapid eye movements. On average, people decide where to look three-times per second. „In a recently completed study", says Rothkopf, „we were able to demonstrate that, in controlled laboratory environments, our test subjects were able to learn the regular temporal features of their visual surroundings in an optimum manner and to take into account their own visual and action uncertainties to plan their eye movements. The data processing models we use in this context not only collate the data based on empirical observations, but they derive behaviour from

Information

The Psychology of Information Processing
Prof. Constantin Rothkopf, PhD.
Phone: ++49 (0)6151/16-23367
E-mail: rothkopf@psychologie.tu-darmstadt.de
www.pip.tu-darmstadt.de

Photo: Jan-Christoph Hartung

Professor Constantin Rothkopf (left) and David Hoppe discuss simulation results.

general information processing principles. Thus, we propose a computational model of human information processing. One of the big questions now is how this model can be applied to everyday actions such as making a sandwich".

Information processing in the brain also involves learning and the concept of a potential reward. Rothkopf cites the so-called marshmallow test as evidence of this. In this test, a young child is asked not to eat a marshmallow lying on a table until the instructor has fetched a second one. Then the child is left alone with the sweet. For decades, the child's behaviour was interpreted as an expression of his or her self control. Rothkopf views it as the result of a computation within the brain. The brain, he explains, processes all impressions, experiences and desires, includes any uncertainties in the calculation and then takes the best decision possible under the circumstances prevailing at that moment.

Rothkopf supports this assertion on the basis of new results from colleagues at the University of Rochester. They found that children who had received a promised reward just before the test last an average of four times longer than those kids who are fobbed off with empty promises shortly before the start of the test. As Rothkopf explains: „waiting for the second marshmallow only makes sense to the child if he or she knows from experience that the chances of a second treat are high. In the absence of any such experience, the clever option is to snaffle the tangible sweet". For him, what psychologists have for years been interpreting as a character trait is actually a rational reaction to the result of a calculation of all available data and representations. This is also evident when test subjects are given tasks to solve having just played a computer game either with great success or a total lack of it. „Two minutes of euphoric or depressing play has extreme effects on how the test subjects behave afterwards", Rothkopf says. „The observed effects are significantly more pronounced than those that have traditionally been attributed to personality differences".

He even goes a step further and views certain mental conditions as the result of computation processes within the brain. „Colleagues at the Swiss Federal Institute of Technology in Zurich (ETH)", he explains, „have used computer models to demonstrate convincingly that a person who continuously experiences the fact that nothing in his or her life ever changes, regardless of what they do, will calculate that all further efforts are a waste of time. This learned sense of helplessness, a kind of passivity, can then lead to depression".

Rothkopf has high expectations of cognitive science: „This research will not only lead to new intelligent solutions to difficult problems, but will also teach us a lot about ourselves. It's basically a matter of self-revelation".

The author is a science writer and holds a doctorate in Biology.

Publication:
David Hoppe & Constantin A. Rothkopf: Learning rational temporal eye movement strategies, Proceedings of the National Academy of Sciences (PNAS) 2016
doi: 10.1073/pnas.1601305113
www.pnas.org/content/113/29/8332

With big data to vehicle 5.0

Data Mining involves opportunities and risks – including for the automotive industry. An interdisciplinary team at the TU Darmstadt is looking into ways it can utilise vehicle operating data in a targeted and transparent manner.

Photo: Jan Ehlers

Discussion between experts: Hermann Winner (left) and Stephan Rinderknecht, Professors of Mechanical Engineering.

By Jutta Witte

Data mining itself is nothing new, and is extremely controversial in this country due to its aggressive use in the American digital economy. This notwithstanding, the mass collection and analysis of data also holds potential for the optimisation and development of vehicles. Yet, how can one fully exploit the new technological possibilities without riding rough shod over data protection legislation, Internet security and user interests?

This is the question currently facing the German automotive industry: Christian Beidl, Head of the Institute for Internal Combustion Engines and Powertrain Systems at the TU Darmstadt, describes the situation this way: "it needs to evolve out of the realms of traditional business acumen, but in a revolutionary environment". Scientists working in mechanical engineering, computer science as well as human sciences and economics want to resolve this problem nexus in the context of a joint research initiative.

They want to use vehicle operational data not in a random manner, but rather for clearly defined research and development purposes. As Project Coordinator Professor Stephan Rinderknecht emphasises: "we state in advance which data we need for which application". The objective is, not just to improve the characteristics of the entire fleet on the basis of a single vehicle in this way, but rather to drive the technical development from the rules-based to knowledge-based vehicle, which is capable of "learning", controlling and optimising its performance based on its own data.

Until now, says Rinderknecht, Head of the Institute of Mechatronic Systems in Mechanical Engineering, research in this field has not been strongly focused on linking Big Data and automotive technology. "To this extent", he explains, "our research project is unique and exemplary both at the national and international levels". What is special about the Darmstadt approach is that, right from the start, experts from ten different disciplines will be linking the subject of Big Data and the development of new technologies with questions of data protection, cyber security, so-called human factors such as privacy protection, changed customer expectations, and economic aspects. "It is important for our concept to ensure transparency in order to gain the users' trust and acceptance", says Rinderknecht. With the three main pillars, lightweight design, powertrains and efficiency as well as autonomous driving, the research alliance has the primary topics in automotive engineering firmly in its sights. As Hermann Winner, Head of the Institute of Automotive Engineering, explains: "based on these application examples, we want to engage with various cross-disciplinary topics that are relevant with a view to digital transformation".

Modern cars already collect data, including such things as combustion engine load profiles, which provide insights into how they have been used and determine when the next oil and filter change is due. However, a complete evaluation of all such profiles is not yet possible, and optimisation efforts are still based on reference applications. The experts at the TU Darmstadt are convinced that enormous improvement potentials could be the result if "the operation phase were to become a further development phase".

Information

Department of Mechanical Engineering
Prof. Dr.-Ing.
Stephan Rinderknecht
(Project Coordinator)
Institute for Mechanic System in Mechanical Engineering
Email: rinderknecht@ims.tu-darmstadt.de
Phone:++49 (0)6151/16-23250

The starting point for their research is the concept of the individual vehicle. Winner explains that, with the approved tolerances, there will never be two vehicles that are exactly the same, and that are used in exactly the same way. Thus, every vehicle generates a unique set of data and can transmit it to a server for logging. This information is then analysed to enable the gathering of evidence that is applicable to the fleet as a whole. However, any improvements based on this information will only take effect in the next generation of vehicles. In the future by contrast, a vehicle could make use of Big Data technologies for self-optimisation as well as transmitting it to the server and other vehicles thereby contributing the collective intelligence that would be generated on this basis.

"The vehicle would generate its own data and benefit from it", Winner explains. One of the reasons this is important is that problems don't tend to develop under regular operating conditions, but rather during dynamic processes such as braking and accelerating on wet roads or steep inclines. The vehicle then reacts in a rule-based manner, i.e., there is a compromise for every operating condition. "However", Christian Beidl believes, "a self-learning vehicle could generate the optimum driving profile under any circumstances". On the basis of temperature data and load figures, he goes on to say, a vehicle of this type would adapt its operating and driving strategy with a view to achieving certain specific objectives such as lower emissions or less loading of certain components.

„It is important for our concept to ensure transparency in order to gain the users' trust and acceptance".

For Beidl, this is a benefit that should not be underestimated when considered in light of emissions and environmental friendliness. Current exhaust purification systems need to be designed for various rule-based adaptations for environmental situations whilst still being economically viable. In light of this conflict of interests, optimisation is practically impossible to achieve. However, this conflict of interests can be resolved through an intelligent drive system that generates the optimum configuration on a case-by-case basis. For example, it would be possible to ensure that a particular operating mode would take over in an urban centre suffering from a high emission load, to prevent any further pollution of the air quality. "That means", the expert continues, "that we would achieve better results for people and the environment whilst using fewer resources".

A consideration of lightweight design also reveals the new possibilities. For example, gears are usually designed to cope with the most extreme application scenario. People whose driving style matches this extreme application scenario are known as "99% drivers". In the future, it would be possible to record torque and temperature profiles for specific events such as hard gear changes and spinning wheels and to provide advance notice when various vehicle components have reached their utilisation limits.

Building on this knowledge, one can imagine completely new business models: the one-time exchange of certain component groups in the wake of extreme utilisation scenarios could be planned into the calculation right from the start with a view to a more lightweight and resource saving construction method. On the other hand, people who treat their cars carefully, could be rewarded via a bonus system. In addition, more precise information would be available for determining the value of a used car. New testing methods could be developed.

Thus, there are indications of imminent paradigm change in many aspects for the German automotive industry. The researchers want to think it through scientifically in advance. "The crucial thing", Rinderknecht emphasises, "is that we start collecting the data now, which we will need for our development goals".

The author is a science writer and holds a doctorate in History.

Research foci:

- Accepted autonomous driving
- Real-drive optimised powertrains
- Software-based lightweight design

Cross-sectional subjects:

- Big Data
- Economy and ecology
- Human Factors
- Technical methods

Present partner-discipline joint ventures at TU Darmstadt

- Automotive Engineering
- Business Information Systems, Software Business & Information Systems
- Control Methods and Robotics
- Ergonomics & System Design
- Internal Combustion Engines and Powertrain Systems
- Mechatronic Systems in Mechanical Engineering
- Psychology of Information Processing
- Security Engineering
- System Reliability, Adaptronics and Machine Acoustics
- System Security Lab

Core team member of the Research Alliance: Professor Christian Beidl (right.).

Photo: Jan Ehlers

Eavesdropping proh

Sometimes, when two people or software applications are communicating via the Internet, a third party is listening. Cryptographic protocols could prevent this situation, but software developers often find it difficult to correctly integrate them into applications. This is the reason why researchers at the TU Darmstadt want to automate encryption.

By Boris Hänßler

Andrea wants to send her friend Stefan a message via the Internet. To prevent anyone else from reading it, she communicates with Stefan and agrees on a secret code with him that only he and she will be able to decipher. Should the message fall into the wrong hands, it will consist of nothing more than an incomprehensible string of characters that cannot be deciphered without the key. However, what Andrea and Stefan don't know is that a spy has inserted himself between them. The secret code that they believe they established between themselves was actually generated by the spy. He sent it to both participants by pretending to be the other one in each case. Now he can read all of their messages and, for example, ask Andrea for an important password. She feels safe, as she thinks she's sending it to her friend.

This scenario gives a rough idea of a man-in-the-middle attack, during which an attacker manipulates Internet communication. In information technology, the relevant key or code is part of a so-called encryption algorithm. It is designed to protect data that is transmitted back and forth either within a single application or between different applications. Encryption protocols usually run in the background without the user noticing. If, for example, we visit an online shop, our browsers and the online shop automatically negotiate a unique key that is used to mathematically encrypt the data, be it details of the order or bank details. A third party could not do anything useful with the data without the key.

„Scientists from the fields of cryptography and software engineering are working closely together here; something that is still happening much too rarely around the world".

We encounter cryptography constantly: when using Apps, when sending emails, when communicating via messenger services or during in-house corporate communications – whenever sensitive data is involved. Encryption protocols ensure a certain level of security under certain assumptions concerning the abilities of the potential attackers, but only if the designer of an encryption protocol implements it correctly and the application developers have used and integrated it correctly in their code. And, it is in this context that one finds problems that should not be ignored. Configuring cryptographic components is difficult and one cannot expect software developers to be cryptography experts: they make mistakes. Between 2013 and 2015 alone, 1769 security vulnerabilities registered in the USA's „National Vulnerability Database" (http://nvd.nist.gov) were the result of such mistakes – as such, issues involving the integration of encryption protocols in applications were the fourth most frequent source of such registered vulnerabilities.

This is not surprising, if one considers several studies presented the most renowned scientific conferences relating to the area of cyber security over the past few years. These demonstrate that software integration is an important point of weakness, especially since the use of components of cryptographic libraries requires knowledge of too many details that application programmers often do not posses. For example, software developers need to ensure that the individual steps of an encryption protocol are executed in a specific order, for which concrete recommendations are available depending on what is to be protected. However, software developers frequently lack the time to read the relevant manuals. Another source of errors are so-called digital certificates that verify the validity of a given key. Developers sometimes disable the verification process for their software certificates, in order to speed up testing, but then forget to re-enable it for the production system. According to Mira Mezini, Head of the Software Engineering Research Group at the TU Darmstadt: „these are both common errors, even among serious software providers; and those are just two examples among many". Intruders always have the advantage that they only need to discover a single security vulnerability to be able to steal data, while developers are faced with the enormous challenge of closing all possible security gaps.

It is neither possible nor appropriate for all software developers to double up as encryption experts, especially when considering that according to a 2013 IDC report (available at: http://bit.ly/2a86Mju), 7.5 million out of 18.5 million software developers world wide are hobby programmers. According to Mira Mezini, this trend is increasing. „This is why", she explains, „cryptographic experts and software developers need to better augment each other's skills". This is precisely the approach of the „CROSSING" collaborative research center at the TU Darmstadt, funded by the German Research Foundation (DFG). An interdisciplinary team from the TU Darmstadt not only develops novel encryption protocols in the context of „CROSSING", but also new methods and tools to simplify the integration of encryption protocols into application codes and, thereby, to increase trust in computer technology in the long term.

There are three areas of focus at „CROSSING": One of these involves the development of new cryptographic primitives, which constitute the smallest building blocks in cryptographic protocols. The second research priority is concerned with creating new cryptographic systems from these primitives. In the research area, in which Mira Mezini is

Information

Specialism: Software Engineering
Prof. Dr.-Ing. Mira Mezini
Phone: ++49 (0)6151/16-21360
E-mail:
mezini@st.informatik.tu-darmstadt.de
www.stg.tu-darmstadt.de

ibited

Photo: Katrin Binner

Professor of Computer Science Mira Mezini, Head of the Software Engineering Research Group at the TU Darmstadt.

involved, the scientists support software developers in the integration of cryptographic primitives and systems in their applications without errors. It is precisely this kind of research that has received too little attention in cyber security research until now. „Till now", Mezini explains, „cyber security research has focused, if at all, on software end-users, to provide them with software tools with which they could protect themselves from harmful software". „CROSSING", she adds, is investigating issues concerning software developers.

Yet, how can the researchers help software developers? „Our assumption" says Mezini, „is that the errors they make when trying to properly integrate cryptographic protocols could be significantly reduced if we were to engage more with the requirements of the developers and provide them with active support in the integration of encryption protocols in application codes by way of intelligent tools. This means intelligent encryption libraries the components of which would, to a significant degree, automatically install themselves in the application codes". In an initial step, Mezini's team has approached developers themselves to ask for their views on the core question as part of an empirical study. „Developers work in a task-oriented manner", she says. „They want encryption libraries that tell them: this encryption component is available for the task you wish to achieve, and this is how to configure, combine and use it to ensure the security of this particular task. It would be best if the libraries could take over these tasks, i.e., do them automatically for the developers". For example, a developer might wish to encrypt a communication channel. The library would then suggest the best components to use for the encryption and explain how to configure them to prevent them from negatively impacting one another. The objective is to develop appropriate software-oriented methods and procedures that would be built into encryption libraries. In a follow-up step, the process would be further automated. Ultimately, the intelligent encryption library would include two interfaces: one interface for the designers of cryptographic protocols to check that they had been correctly implemented, and another interface for the software developers to ensure that correctly implemented encryption protocols would also be correctly integrated into and used in application software. In this way, the procedures would be checked twice – when first integrated into the encryption library and then during the implementation of the application software. Ideally, the latter would take place directly within a software development environment.

Today, software is programmed in this type of development environment. This involves integrated tools that simplify software programming, checking and testing. The most popular development environment for the widely adopted programming language JAVA is „Eclipse". According to Mezini: „we first want to enhance the functionality of Eclipse by linking it to our encryption library such that, even during programming, continuous checks would be running in the background to ensure that cryptographic algorithms are placed at the right points and are correctly configured and deployed. Other development environments could also be enhanced in a similar way". In addition, this approach would ensure that an application would remain secure even if the programmer were to upgrade it at some point, or if certain encryption procedures that had been integrated within the encryption library were suddenly to be deemed no longer secure. This would save the developers time, and they would always be able to be confident that they had implemented the best possible procedure currently available.

In addition to Mezini and her colleague Eric Bodden, who moved to the University of Paderborn a few months ago, two doctoral students and a post-doctoral researcher are working on the project. „What we hope", says Mezini, „is that an active community will emerge in the long term that will adopt and enrich our encryption library with more and new cryptographic components. „We have created an important basis by at least having brought cryptographers and researchers working on software methods and languages closer together at the TU Darmstadt, something that is still happening much too rarely around the world".

The author is a technology journalist.

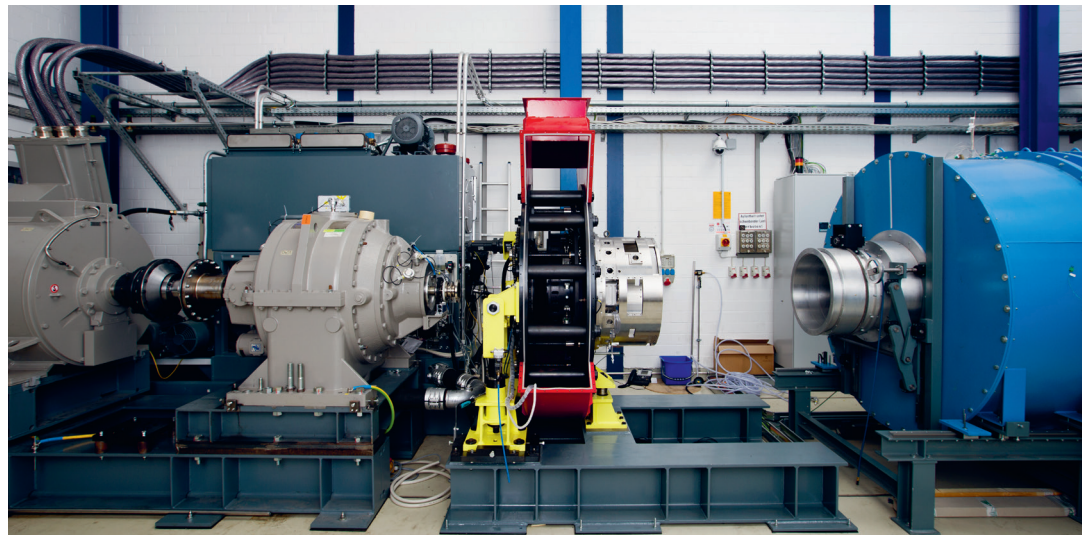

Photo: Katrin Binner

Experimentation under real-world flow conditions: new compressor test facility.

Turbo forces

A high performance test facility for compressors is being built at the TU Darmstadt with which gas turbines are to be adjusted for the energy transition.

By Boris Hänßler

A pipe with the diameter of a car tyre leads from the ceiling to the floor, changes direction and ends in a series of elements that remind one of an aeroplane propulsion unit. This machine at the TU Darmstadt's compressor test facility uses a set of rapidly rotating rotor blades to suck in air from outside the building and compress it, whereby, in some areas, the air reaches the speed of sound. If the room really did house a propulsion unit, the compressor system, with around 20 rotors, would compress the air step by step from 1 bar to 60 bar. By way of comparison, the pressure in a car tyre is 2 to 3 bar.

However, the researchers are only interested in the first rotor stages of the compressor. „They are the most interesting", explains Professor Heinz-Peter Schiffer, Head of the Gas Turbine and Aerospace Propulsion institute: „The highest velocities are achieved in the entry stages. That is where there is most to gain through optimisation". He goes on to say that gas turbines are already highly efficient, but that, given the high amount of energy that is processed, even the smallest improvements offer an enormous savings potential.

Since 1994 the TU Darmstadt has been operating a transonic compressor test facility at which companies such as MTU and Rolls Royce put aero-engine compressors through their paces. Eight years ago, Schiffer decided to install a second test facility in order to expand compressor research to include gas turbines. Gas turbines work in a similar way to aircraft propulsion units, but are larger and, instead of thrust, they generate shaft power. Therefore, the new test facility, which is due for completion at the end of the year, will realise twice the yield as the old one and, unlike that one, the researchers will also be able to test two stages of a compressor in future, instead of just one, and will, therefore, be able to analyse the interactions between the stages.

The compressor at the test facility is a scaled-down version of the originals used in gas turbine power plants, but the aerodynamic profiles are similar and pressure conditions identical. „It is the smallest possible version that still corresponds to real conditions", says Schiffer. Only under real-world flow conditions can the researchers analyse the operation in safety-critical circumstances, such as shortly before a stall or when the blades are damaged. Because any such damage would shut down the gas turbine, engineers at operational facilities avoid risks and do not fully exploit the performance that is theoretically possible. But they are throwing away some of the potential performance because, the harder they drive the compressor, the more efficient the entire machine becomes. „What we are expecting from the Darmstadt facility", says Christoph Biela of Siemens, partner in the test facility joint-venture, „are measurement data that we can use to refine the calibration of our design tools".

The instrumentation in Darmstadt really is unique. There are even sensors on the rotor, which monitor the blades and their oscillations. „In the test facility we will be analysing the flow fields at the intake and outlet and at every intermediate stage" Schiffer explains, „as well as the efficiency level under all operating conditions". It is that, he says, which makes this test facility so valuable during the energy transition era. During most oft he time gas turbines currently operate at a constant performance level. In future they will have to be operated dynamically to deal with peak loads in the electricity grids of tomorrow. However, rapid acceleration and deceleration impacts the efficiency level in ways that are not yet known

In addition to the compressor test facility, the TU Darmstadt is home to two turbine test facilities, making it one of the world's leading institutes in the field of turbo engineering.

The author is a technology journalist

Information

The Gas Turbines and Aerospace Propulsion Unit Research Group
Prof. Dr.-Ing. Heinz-Peter Schiffer
Phone: ++49 (0)6151/16-22113
Email:
schiffer@glr.tu-darmstadt.de