Springer Vieweg

ATZ extra

Proof of Safety for an Electronic Parking Lock in Automated Form

KÜSTER

Automated Proof of Safety for an Electronic Parking Lock

Proofs for functional safety in accordance with ISO 26262 are becoming increasingly complex. The automated, hierarchical failure analysis can serve as a solution for hardware and software investigations. In this article, Küster and the University of Wuppertal demonstrate the advantages of this analysis procedure using the example of a parking lock actuator. The simulation time for the electronic circuits examined was reduced by more than 90 % without any loss of information.

Due to the increasing complexity of software-based systems, the number of components for which functional safety must be verified in accordance with the ISO 26262 standard continues to go up. At the same time, these proofs are becoming increasingly difficult and time-consuming, as the range of functions of the components themselves is also growing. With conventional methods, a complete coverage is almost no longer possible.

In today's motor vehicles, more and more safety-related mechatronics functions are controlled by complex soft-

WRITTEN BY

Kevin Pender
is Group Leader System Development, Simulation, and Functional Safety at Küster Group in Ehringshausen (Germany).

Karsten Roth
is Group Leader Hardware Development at Küster Group in Ehringshausen (Germany).

Dr.-Ing. Levent Ergün
is Senior Engineer at the Chair of Sensor Technology and Measurement Systems and Head of the Functional Safety Working Group at the University of Wuppertal (Germany).

Prof. Dr.-Ing. Stefan Butzmann
is Head of the Chair of Sensor Technology and Measurement Systems at the University of Wuppertal (Germany).

ware-based systems. When developing such systems, one challenge is to verify their safety and reliability. Traditional manual methods, such as the Failure Modes, Effects, and Diagnostic Analysis (FMEDA), quickly reach their limits, as the number of possible failure combinations increases exponentially with the complexity of each system. Even with an average of four failures per electronic component, a control unit with 1000 components results in 4000 possible single failures and almost eight million double failures, all of which would have to be considered and analyzed [1]. This growth is often referred to in the technical literature as a "combinatorial explosion." [2].

A complete manual analysis is no longer feasible given the complexity of such a system. Also, computer-assisted analyses cannot be carried out within a reasonable amount of time anymore. Even with a simulation duration of only 15 s per run, the failure analysis would take around 925 days for 1000 components and an average of four failures per component, **FIGURE 1**. With an average of five failures per component, the total analysis would take over four years.

Another important issue is the inconsistencies that frequently arise when using multiple independent simulation tools from different providers. For example, transferring the results of a simulation to an FMEDA program usually requires manual intervention by the developer. Furthermore, the behavior of the system in the event of a component failure is usually not simulated at all but estimated by the developer or the team. However, such expert guesses can be incorrect and then jeopardize the safety of the entire system.

PARKING LOCK ACTUATOR

The parking lock actuator ensures that parked passenger car always remains securely in place – even a heavy vehicle which is parked on particularly steep terrain, where enormous forces act on the system. A video [3] shows how the actuator works. Selecting the P drive

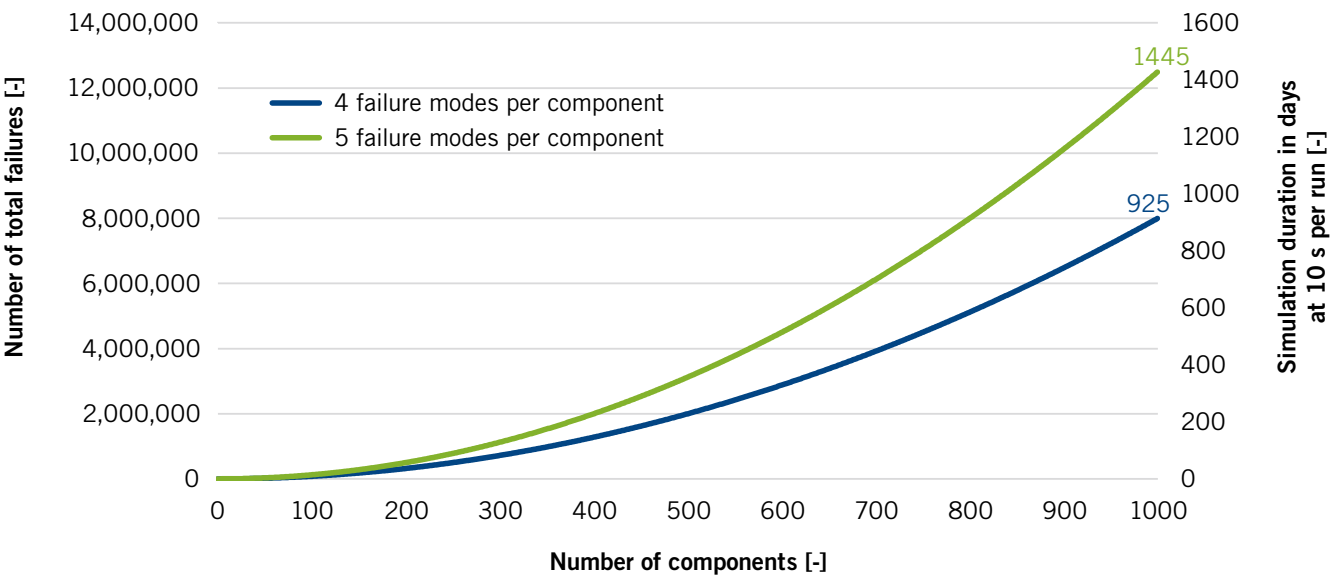

FIGURE 1 Total failure and total simulation duration as a function of the number of components (© University of Wuppertal)

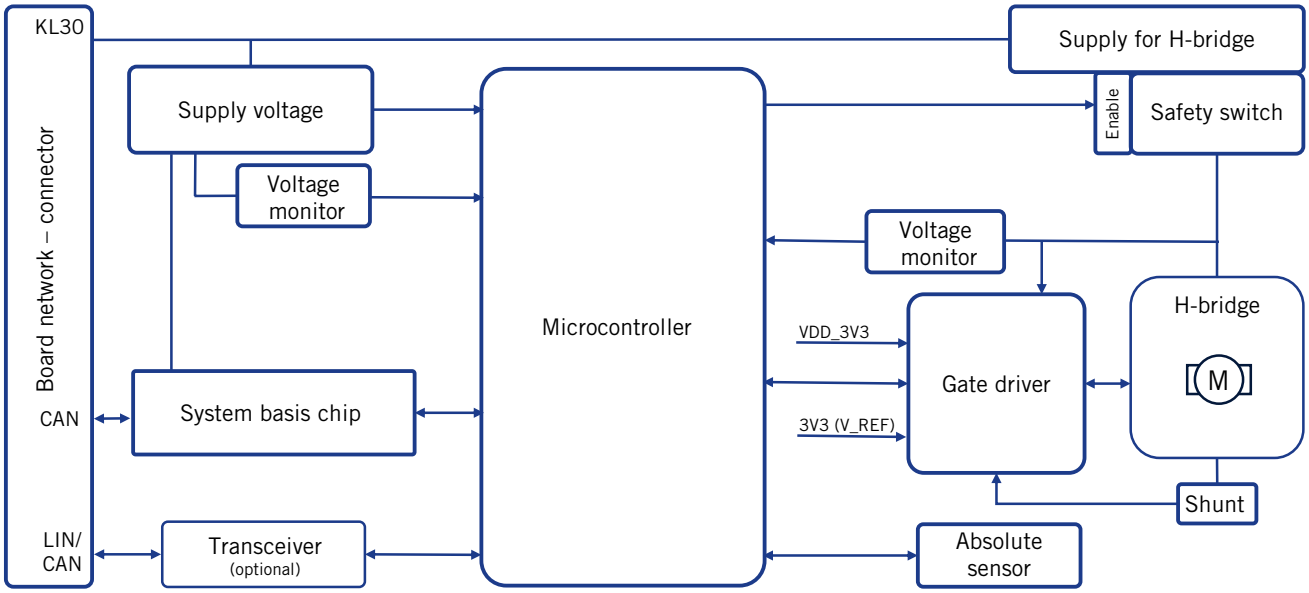

FIGURE 2 Block diagram of the parking lock actuator (© Küster Holding GmbH)

mode activates the actuator: The torque of the electric motor is transmitted to the output shaft of the actuator via a self-locking worm gear. This rotational movement engages the pawl in the vehicle transmission and secures the vehicle with the following advantages against rolling away:

- engaging/disengaging the pawl at an application time of 470 ms
- measurement concept with an absolute sensor
- lifetime of up to one million operating cycles.

The latest generation of the parking lock actuator considered here is designed for ASIL-C applications. The two main safety goals are fulfilled in the implemented solution, **FIGURE 2**:

- No operation of the actuator should be possible without a request.
- The output position must correspond to the actual position of the actuator output.

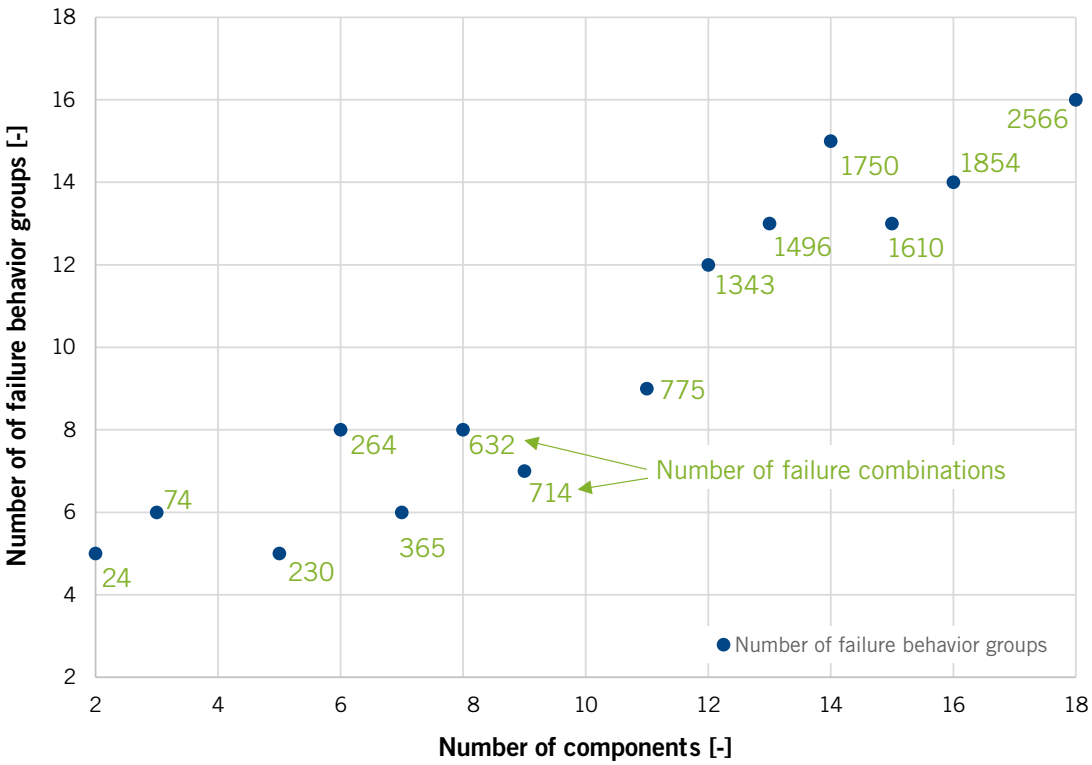

FIGURE 3 Number of failure behavior groups depending on the number of components in the system (© University of Wuppertal)

In addition to the main components shown here, the circuit consists of approximately 200 electronic components (resistors, capacitors, transistors, etc.). To ensure a complete safety analysis, peripheral units, for example Analog-to-Digital Converters (ADCs), Digital-to-Analog Converters (DACs), and multiplexers, are also considered in the presented integrated circuits.

This results in more than two million possible single and double failure combinations. Assuming a simulation duration of around 15 s, including compilation and data storage per operation run, the complete analysis would take over twelve months. This approach is not practical for actuators of this complexity, due to increasingly rapid time-to-market and consequently shorter development times.

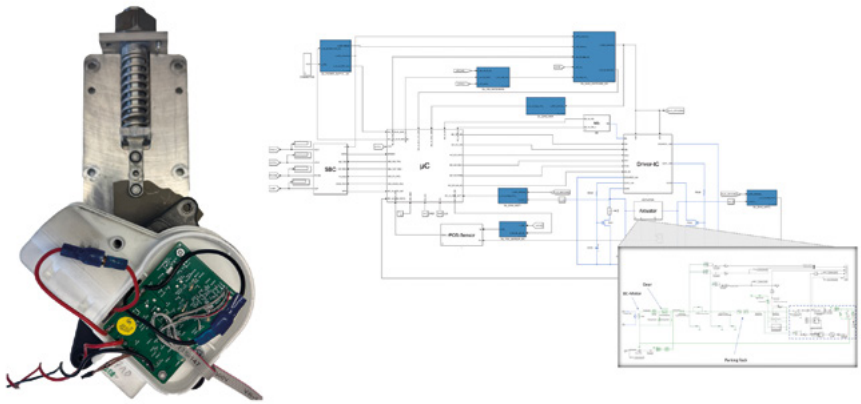

FIGURE 4 Mechanical mode of operation of the parking lock actuator – simulation on the test bench (left) and Simulink model (right) (© Küster Holding GmbH)

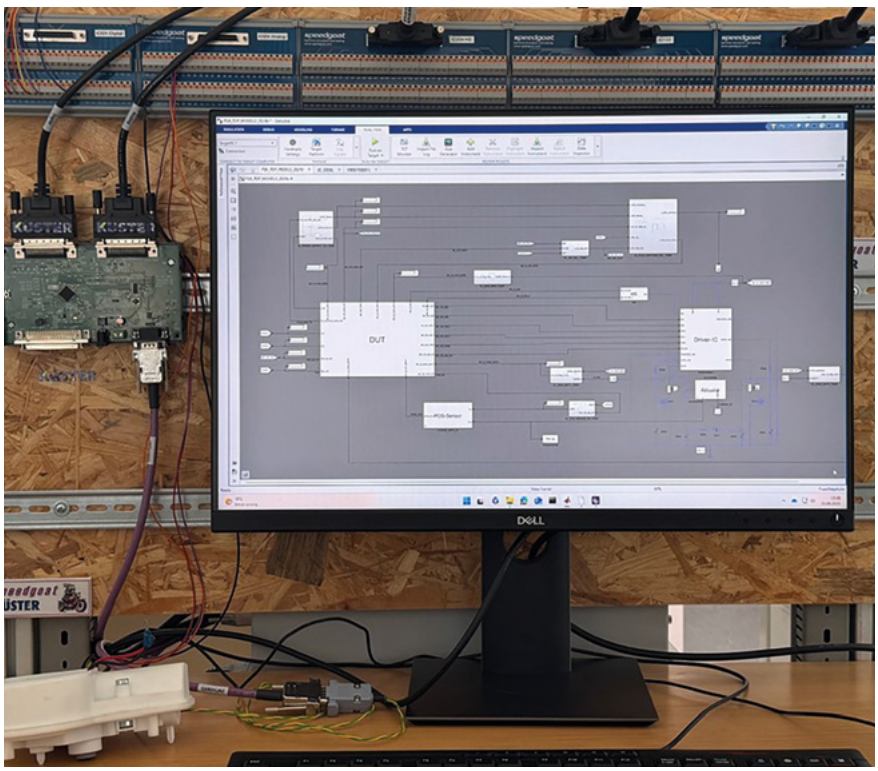

FIGURE 5 Hardware model environment with processor-in-the-loop test bench (© Küster Holding GmbH)

AUTOMATED PROOF OF SAFETY WITH THE HIERARCHICAL FAILURE ANALYSIS

This is where the methodology of the Chair of Sensor Technology and measurement equipment at the University of Wuppertal comes into play, enabling automated proof of safety of electronic systems. The approach pursued here combines automated and hierarchical failure analysis with intelligent failure grouping.

Initially, all relevant single and double failures are generated automatically, and the behavior of individual subsystems is analyzed for each failure or combination of failures. This is followed by a cluster analysis in which up to several thousand failure causes are grouped based on the resulting subsystem behavior in such a way that the respective subsystem can be described with only a few characteristic failure effects. This is made possible by mathematical algorithms that group failures with a similar failure behavior. The methodology described makes use of what is known as equality of failure effects. Complexity is significantly reduced without losing any safety-related information.

FIGURE 3 shows the reduction in complexity when applying the cluster analysis described before to the example of 14 electronic circuits examined [1]. Even with this moderate number of 14 components, a three- to four-digit number of failure combinations would have to be considered. However, this high effort is significantly reduced by means of the cluster analysis.

Using the methodology described before, the simulation time for the circuits examined can be reduced by more than 90 % without any loss of information. Instead of complex analyses, the automated methodology delivers reliable and objective results in just a few days. Efficiency increases significantly; inconsistencies and misjudgments are avoided.

APPLICATION OF THE METHODOLOGY FOR THE PARKING LOCK ACTUATOR

The basis for applying this methodology is the physical system architecture and its simulation. **FIGURE 4** show examples of how the actuator works and how it is implemented (both electronically and

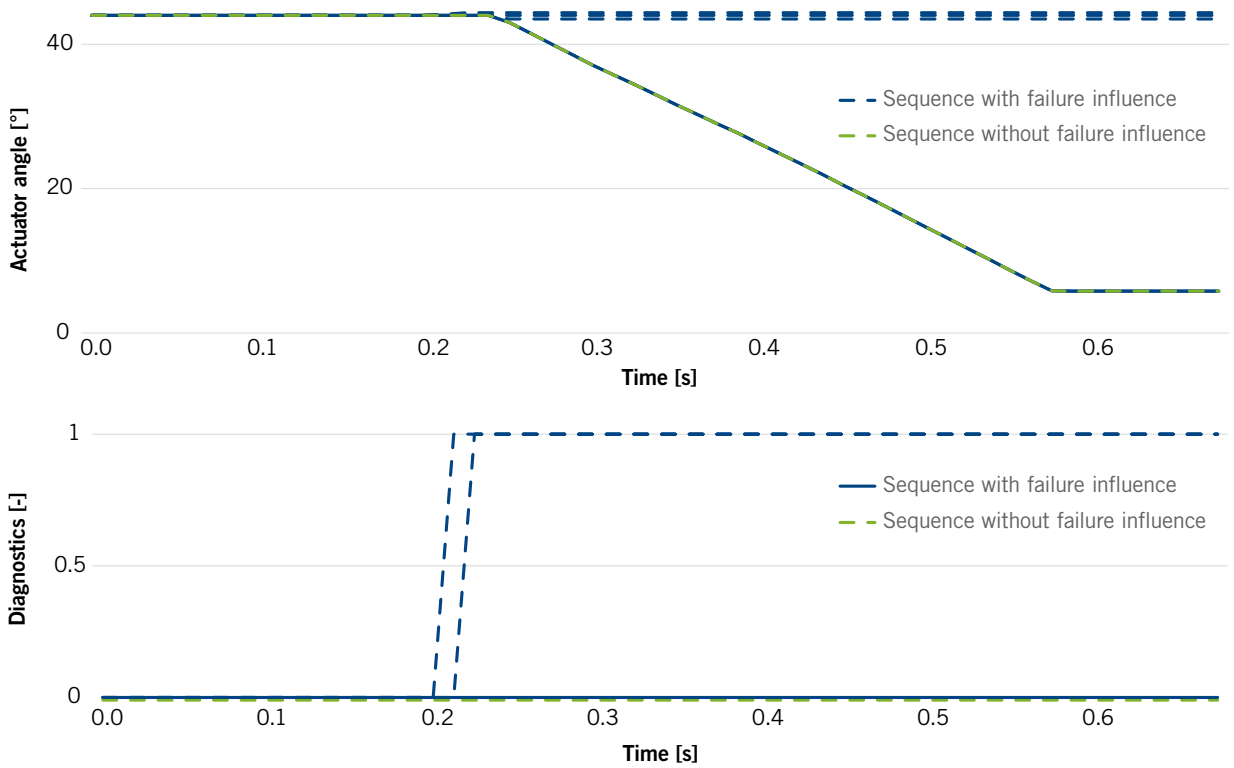

FIGURE 6 Excerpt from the single failure analysis: motion of the actuator (top) and diagnostics (bottom) (© Küster Holding GmbH)

mechanically) in the Simulink modeling software of Mathworks.

This model forms the basis. In the failure simulation itself, the tolerances of each component and their exceedances up to failure are automatically considered. By using the hierarchical failure analysis approach, the number of simulation runs required can be reduced from more than two million to approximately 125,000.

The simulation did not reveal any critical single failures or latent failures. This meant that the proof of safety was completed in a fragment of time that would otherwise be required for such an analysis. Not only does this ensure the safety of the product, but it also shows where diagnostics and replacement reactions can increase the reliability and availability of the component.

AUTOMATED SOFTWARE VALIDATION

The methodology described also facilitates the validation of the system software. For this purpose, the target processor, including the software, is connected to a hardware-in-the-loop simulation platform, that means, the virtual failure environment is linked to the real control unit. In this environment, the behavior of the software can be specifically tested in interaction with failure states and failure combinations that were previously identified in the hardware analysis. The microcontroller's inputs are "played" with the signals that occur in a real failure case. The software's response to each of these failure conditions is automated and verified in real time. It is validated whether

- failures are reliably detected
- the intended safety measures are activated
- the system meets the requirements of ISO 26262 and other relevant standards.

The automation described answers these questions not only for individual failure cases but also for the entire spectrum of all conceivable component failures.

The aforementioned methodology gives software developers better insights into how the software behaves when individual components fail. Critical system behavior is detected and corrected early in the development phase. At the same time, the effort required for software validation is significantly reduced, as the automated test execution is continuous and requires no human intervention. The methodology also demonstrates its advantages in the verification of software updates. While in classic software validation, every update must be manually tested from scratch, here the check can be performed fully automatically at the push of a button, as the simulation model of the hardware is already available.

APPLICATION OF THE PROCESSOR-IN-THE-LOOP METHODOLOGY TO THE PARKING LOCK ACTUATOR

The hardware model environment described before, **FIGURE 5**, for this specific application is connected to the target processor with the compiled series software for this purpose. This environment precisely "plays" the signals that could occur in real operation because of component failures or combinations thereof. This makes it possible to automatically

test the software's response to all component failures considered in real time.

An excerpt from the failure analysis is shown in **FIGURE 6**. The green curves show the failure-free reference case in which the parking lock is successfully engaged. The actuator moves from 44° to 6°, **FIGURE 6** (top). The blue curves represent the system responses to various failure scenarios. In some cases, the movement request was not accepted; the actuator position remains at 44°, **FIGURE 6** (top). This concerns component failures, for example, in the power electronics or the sensor technology. However, the implemented diagnostics ensure that these potential malfunctions are detected in advance and reported to the vehicle.

The approach presented here combines hardware and software validation with consistent, automated proof of safety. The practical benefits of this methodology have been proven in many different applications.

Using the presented methodology, it can be investigated that many component failures occurred within a few days, and both the hardware architecture and the behavior of the software can be evaluated. For all failure cases considered, the correct system behavior of the parking lock actuator can be verified. This is due in no small part to the redundant shutdown paths. In addition, the software has extensive plausibility checks and diagnostic measures. The results highlight both the high quality of the system design and the effectiveness and significance of the analysis procedure shown.

SUMMARY

The automated, hierarchical failure analysis combines efficiency with a high degree of safety and transparency. Not only does it ensure compliance with regulations and the necessary technical maturity, but Küster also demonstrates that it significantly reduces the amount of work and testing effort required in the exemplary development of a parking lock actuator.

REFERENCES

[1] Ergün, L.: Entwicklung einer Methodik für den automatisierten Sicherheitsnachweis elektronischer Systeme. Wuppertal, University, dissertation, 2024, ISBN: 978-3-8440-9607-1

[2] Behrends, E.; Gritzmann, P.; Ziegler, G. M.: Pi und Co. – Kaleidoskop der Mathematik. Berlin/Heidelberg, Springer, 2018, ISBN: 978-3-540-77889-9

[3] Küster (ed.): Video: Functionality of the actuator. In: e-magazine of ATZ worldwide 12/2025, November 28, 2025

THANKS

The authors would like to thank Roman Müller-Hainbach, M. Sc., whose dedication and ideas contributed significantly to the success of hierarchical failure analysis, and the entire development team at Küster.

IMPRINT
Special Edition 2025 in cooperation with KÜSTER Automotive GmbH, Am Bahnhof 13, 35630 Ehringshausen;
Springer Fachmedien Wiesbaden GmbH, Postfach 1546, 65173 Wiesbaden, Amtsgericht Wiesbaden, HRB 9754, USt-IdNr. DE81148419

MANAGING DIRECTORS:
Stefanie Burgmaier I Andreas Funk I Joachim Krieger

PROJECT MANAGEMENT: Anja Trabusch

COVER PHOTO: © Küster Holding GmbH

KÜSTER

WELCOME TO OUR PRODUCT UNIVERSE!

KÜSTER MOVING SMART – WHERE EXPERIENCE MEETS INNOVATION

Almost 100 years of company history, almost 90 years as an automotive supplier, and always at the cutting edge: that is KÜSTER, your reliable partner for moving solutions in the automotive sector.

We research, develop and produce your products for a wide range of requirements – whether for cars or commercial vehicles. Our multi-actor family opens up new possibilities and paves the way for advanced mobility solutions.

KÜSTER Unternehmensgruppe
Am Bahnhof 13
35630 Ehringshausen
Postfach 1157
Telefon: +49 (0) 6443 62 - 0
E-Mail: info@kuester-group.com

Discover our innovative solutions