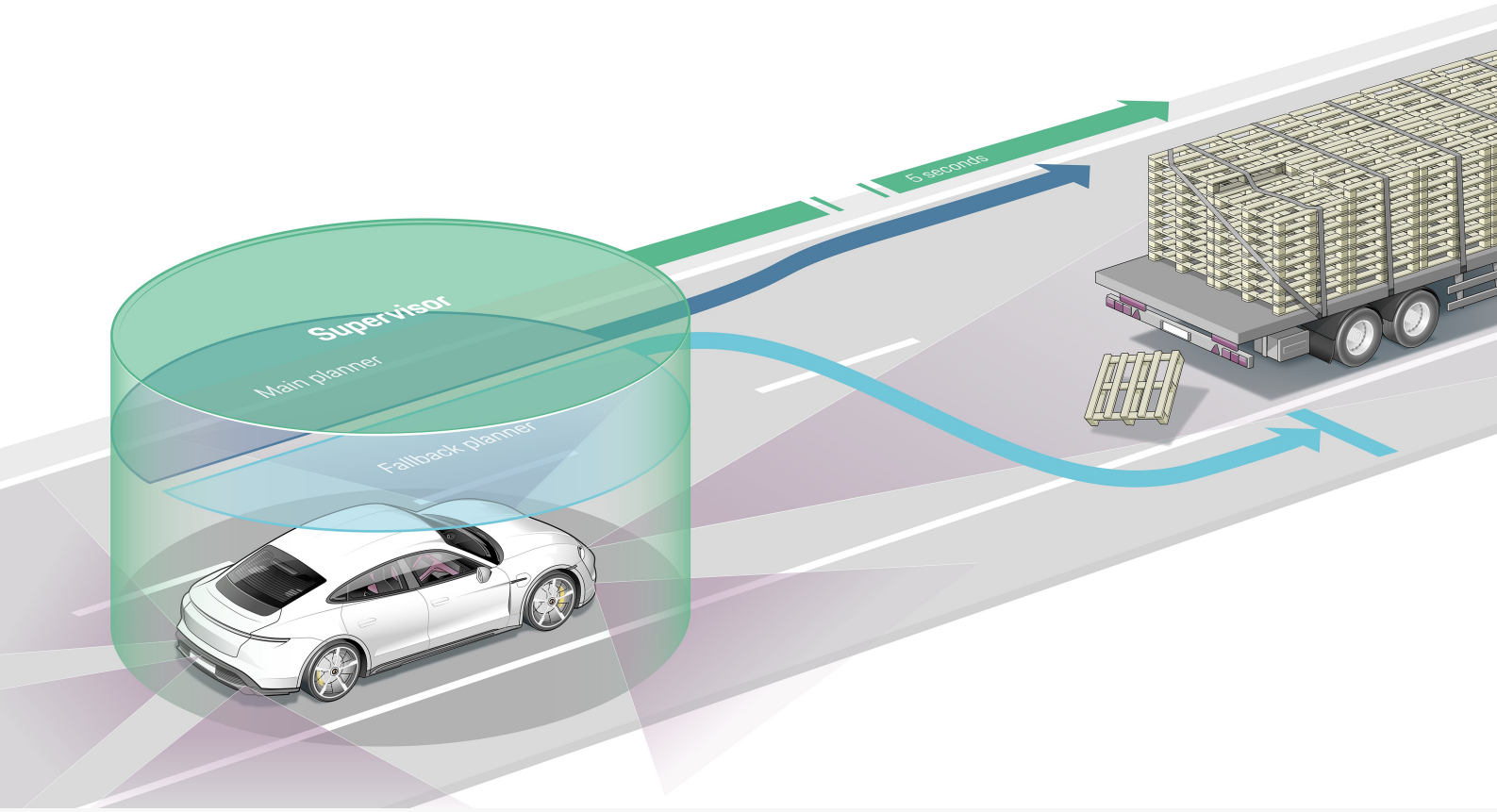

Monitored safety

04/02/2022 Highly automated driving functions must work safely and reliably in every situation – be it on the highway or in a multi-story car park. One of the ways developers achieve this is through redundancy; parallel systems observe the environment and decide what to do in critical situations.

A truck in front loses its load. An unloaded pallet suddenly falls onto the road and blocks the lane. What causes a moment of shock for a human driver today will be mastered with ease by the highly auto mated vehicles of the future. The reason is that it works with three parallel systems: the main planner handles normal driving operations and acts in a comfort oriented manner. It brakes and accelerates gently. System two, the fallback planner, simultaneously calculates a trajectory that quickly maneuvers the vehicle into a safe position if necessary. The third system, the supervisor, constantly checks whether a risk is posed by the main or the fallback path and selects the safest alternative in each case. That's why a pallet falling out of the truck unexpectedly would not be a problem for the highly automated vehicle. Because even in the unlikely event that the main planner overlooked the obstacle, the vehicle would safely take evasive action thanks to the fallback planner – or stop on the shoulder if it were not possible to drive around it.

Such a scenario could soon become reality. Porsche Engineering is working flat out to make highly

automated driving (HAD) functions safe and reliable in this way. The crucial strategy along the way is called “decomposition.” Instead of having the vehicle controlled by a single system, several planners as well as supervisors are applied as parallel instances. “Together, the systems achieve a much higher level of failsafety than a single one,” explains Jan Gutbrod, team leader for the development of driving assistance systems at Porsche Engineering.

“The biggest challenge is to master every last con ceivable situation,” says Albrecht Bo□ttiger, head of the ADAS/HAD Project House at Porsche AG. In other words: the overall system must be able to cope with different vehicle types and driving styles, recognize road markings in different colors – even when they are weathered – and safely avoid known and unknown obstacles. This requires a coordinated interaction of the three subsystems, which must prove itself in tests and road trials.

Strict technical segregation of the systems

Parallel systems have been in use in aviation for a long time. Their safety, however, critically depends on the technical design. “To achieve true redundancy, it is im portant not to simply copy systems,” stresses Andreas Nagler, Head of Systems Engineering and Architecture at Cariad, the Volkswagen Group’s software and technology company. What that means is that the in stances must be technically isolated from each other, i.e. each must have its own hardware, software and data sources. This is the only way to minimize what are known as “common cause” errors, i.e. failures due to a shared cause.

To achieve this technical separation, the supervisor only uses object lists to make an image of the environment. These lists are generated by the vehicle sensors themselves. A radar sensor, for example, provides a list of all vehicles or objects that can be detected in the vicinity, including their direction of movement. The main and fallback planners, on the other hand, do not work with object lists, but with the raw data from the sensors, for example point clouds from laser scanners (LiDAR). In addition, some components access map data – which the supervisor does not.

Data processing also differs between systems. Main and fallback planners, for example, apply what is known as sensor data fusion: if only a single sensor reports an object in the space, while all other sensors explicitly do not, the algorithm of a sensor data fusion may decide to assess this signal as a false detection and to discard it. The supervisor, on the other hand, considers all sensors strictly separately. The different functional principles of the individual systems ensure that each can form its own picture of the situation. The combined strengths of the systems ensure a safe response.

Taking driving dynamics thresholds into account

The task of the supervisor is to check the paths calculated by the main and fallback planners for possible risks. To this purpose, it constantly generates forecasts with different time horizons. A so-called “ballistic approach” can be used for the immediately upcoming meters of travel: the supervisor assumes that the objects will basically maintain their direction of motion and velocity due to inertia and

mass. A second forecast extends several seconds into the future.

To predict traffic events so far ahead, highly complex software with thousands of parameters is required. Among other things, speed, road surface, weather conditions, historical motion profiles of surrounding road users and stationary cars are taken into account. This forecast forms the basis for the decision that now follows: “the supervisor puts the trajectories of the path planners into its future scenario,” Gutbrod explains. If, for example, the so-called “sovereignty zone” around the vehicle, into which no object is allowed to enter, were to be violated on the planned course, the supervisor would veto this and initiate a path change. It “throws off a planner,” as the developers put it.

In doing so, the planning software must be very sensitive. If the supervisor classifies the criticality of potential hazard scenarios too high too quickly, the vehicle can act too cautiously and thus also unsafely. Developers call this effect “too soon too safe.” If this occurs, the brakes are applied much too early, for example. The supervisor must also recognise emergency situations in which a change of path would only cost unnecessary time and possibly have negative effects.

With all measures, it is also important to keep an eye on the specified dynamic driving limits. If – as in the highway example – an obstacle suddenly appears, the systems must react so quickly that there is still time to brake comfortably. In the future, paths could, for example, have the option of raising an “emergency flag,” Gutbrod says: “in this case, planners could ask the supervisor to enable measures beyond the currently set limits.”

Automated parking has to cope with unexpected situations of a completely different kind. Cariad demonstrated what this new function will be able to do in the future at IAA Mobility last September: the driver of a Porsche Cayenne E-Hybrid droppd off their SUV in a special transition zone in the parking garage and issued the command to park via smartphone. The Cayenne then started moving towards the parking space.

If the driver wishes, the car will first drive to a charging station, where a robotic arm with a charging plug will automatically dock. Then it will automatically move on to the actual parking space. If the driver needs the car again, they can call it back to the transfer zone via the app. The advantages for the driver: the time-consuming search for a space and maneuvering are eliminated, and they can also use the time for recharging.

In principle, automated parking can be implemented in two ways: either the vehicle steers itself to the parking space or the surrounding infratructure takes over control. In the latter case, the parking system would give the vehicle the path via radio signals and accelerate or decelerate it as appropriate. The Cariad demonstration at IAA Mobility took this approach. Which of the two approaches will prevail in automated parking in the long run remains to be seen. "Control via the infrastructure is easier to implement and secure,” explains Bo□ttiger. “On the other hand, vehicle-based automated parking allows more parking garages to be used.” It is therefore conceivable that there will be a long-term trend towards complete autonomy, including in parking garages.

If, on the other hand, parking is controlled by the infrastructure, redundant systems must be used here – just as in the vehicle itself. The parking control system should therefore work with several parallel instances. In this way, emergency situations could be safely managed, for example pedestrians appearing suddenly in front of the car. This is to be expected, as autonomous and conventional vehicles will continue to share parking garages for some time to come.

Emergency stop concept for maximum safety

Ensuring safety is a task for everyone involved. "We will be closely examining the algorithms of the infrastructure operators," says Sebastian Reikowski, project manager for parking systems at Porsche Engineering. In order to implement externally controlled parking safely, however, extensive adjustments are also necessary in the vehicle. "All communication with the infrastructure via 5G or WiFi must be encrypted to prevent unauthorized access," explains Reikowski. If the radio connection breaks down, the vehicle stops automatically. An emergency stop concept is also needed: if the primary braking system fails, a secondary system would have to kick in and ensure a safe stop. One idea would be to use the recuperation power of the electric motor in conjunction with the parking brake and parking lock.

Further coordination work is needed for a common communication standard – only then could it be possible for vehicles from all manufacturers to use the parking service. A standard defining an interface between vehicles and infrastructure is already in the works (ISO 23374). "In addition, lawmakers still have to define at what point responsibility is transferred from the vehicle to the infrastructure – at what point the parking garage would have to be liable for damage, for example," adds Reikowski.

As with highly automated driving in general, continuous improvement will be essential. "A new mindset is needed: the software of vehicles will be continuously developed in the future – much like smartphones today," emphasizes system architect Nagler from Cariad. The vision of this "data-driven development": fleets of test vehicles will continuously collect data and transfer it to the cloud. There, the data will be used to improve HAD algorithms. This creates what is known as a "big data loop". A special algorithm in the test vehicle, called the Scene Selector, detects unusual situations or situations that have not yet occurred and transmits them to a central server. There, the scenes are used to further train the neural network of the cut-in detection system. "This continuous learning is the path to robust systems," Nagler emphasizes.

In brief

Redundant, strictly separated systems make highly automated driving functions safe by enabling switching between different trajectories. In automated parking, the parking garage can take over control. But even in this case, emergency systems in the vehicle ensure safety in all situations.

Info

Text first published in the Porsche Engineering Magazine, issue 1/2022

Text: Constantin Gillies

Illustrations: Andrew Timmins

Consumption data

Taycan Turbo S (Predecessor model)

*Further information on the official fuel consumption and the official specific CO_2 emissions of new passenger cars can be found in the "Leitfaden über den Kraftstoffverbrauch, die CO_2-Emissionen und den Stromverbrauch neuer Personenkraftwagen" (Fuel Consumption, CO_2Emissions and Electricity Consumption Guide for New Passenger Cars), which is available free of charge at all sales outlets and from DAT (Deutsche Automobil Treuhand GmbH, Helmuth-Hirth-Str. 1, 73760 Ostfildern-Scharnhausen, www.dat.de).

Link Collection

Link to this article
https://newsroom.porsche.com/en_AU/2022/innovation/porsche-engineering-monitored-safety-highly-automated-driving-functions-27274.html

Media Package
https://pmdb.porsche.de/newsroomzips/4d895af3-626a-43b0-957b-8403500543aa.zip

External Links
https://www.porscheengineering.com/peg/en/

Dr. Ing. h.c. F. Porsche Aktiengesellschaft
Porscheplatz 1
70435 Stuttgart