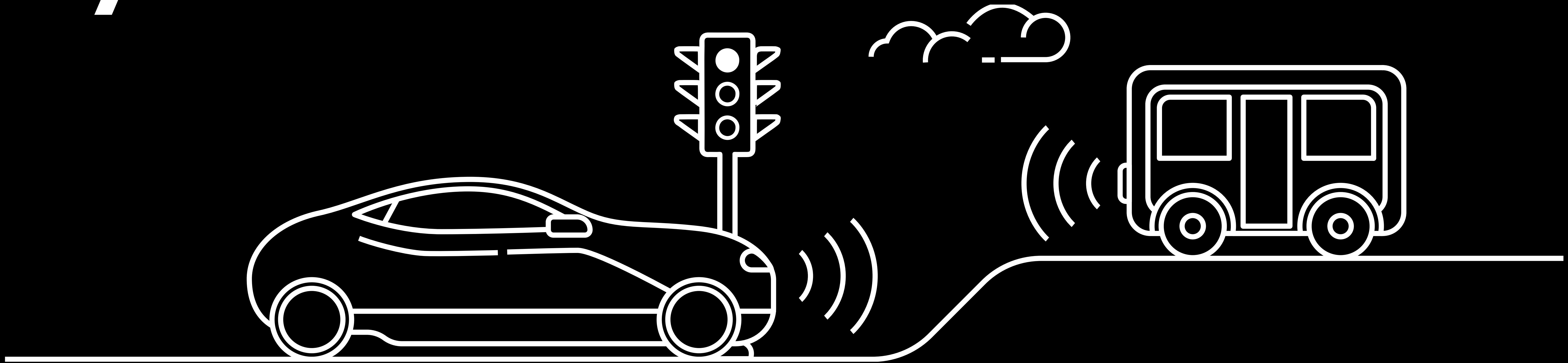
Ansys



Innovating Safe and Secure Mobility

Safety and security are the leading differentiators in autonomous and software-defined vehicles. Engineering simulation and model-based approaches help master these two pillars to enable the survival of vehicle development.

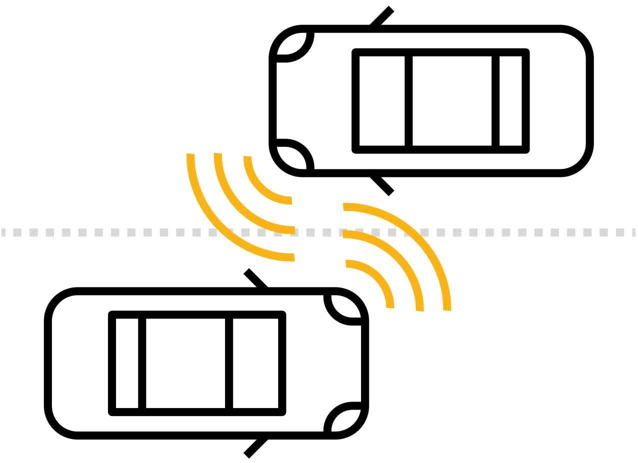
Investing in Automated Mobility Features

Since 2010, over **USD 330 billion** has been invested into more than **2,000** mobility companies focused on vehicle automation, connectivity, electrification, and shared ownership (ACES) development.

THE SIX LEVELS OF VEHICLE DRIVING AUTOMATION SYSTEMS OFFER DIFFERENT MOBILITY EXPERIENCES

LEVEL 0	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Driver responsible for safety			Breaking point from a safety perspective for driver responsibility		
Driver-enabled	Feet off	Some hands off	Hands off/eyes off	Fully-Autonomous	Fully-Autonomous
Zero Autonomy	Driver-Assisted	Low Automation	Conditional Automation/High Automation	In known areas and within operational limits due to geographic changes/weather conditions	Everywhere
	Adaptive Cruise Control	Highway Cruising Systems already on the road and Level 2+ add-ons such as lane changing, automatic merging, traffic light detection	Mercedes' Level 3 Traffic Jam Pilot is first step to taking attention off the road. OEMs are approaching Level 3/4 capabilities beyond traffic jams involving progressive improvements, at higher highway speeds		

Highlighted columns indicate OEMs' progress in reaching full autonomy, working somewhere between levels 3 and 4. Big plays continue to be made in levels 2-3 however, at level 3 the ownness for safety begins to shift from driver to OEM.



To achieve high- or full-level autonomy safely, the vehicle must be able to see its surroundings, perceive obstacles, and react without a driver.

In order to achieve increasingly automated functions, AV developers are required to produce a detailed safety case either by:

Using data acquired from well-defined physical testing executed over millions of miles

— or —

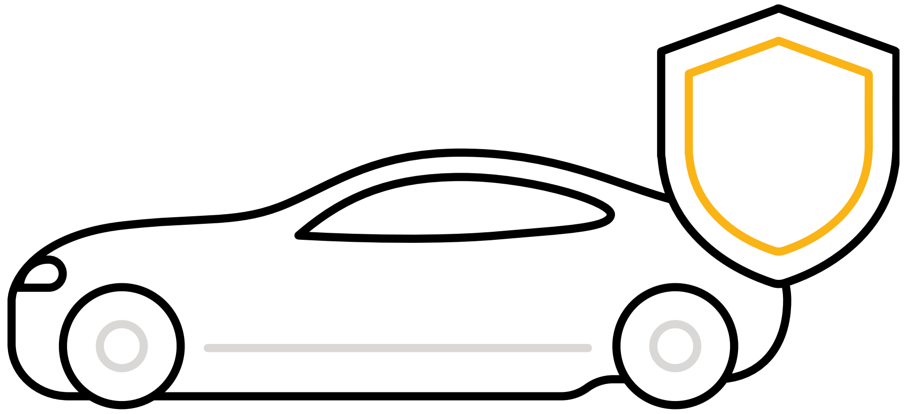
Performing virtual testing, verification, and validation of real-world scenarios where permitted by regulations.

Safety and Security at Top of Mind

Safety and data security are a central concern in the automotive industry and without adequate proof the public will neither trust nor support AV adoption.

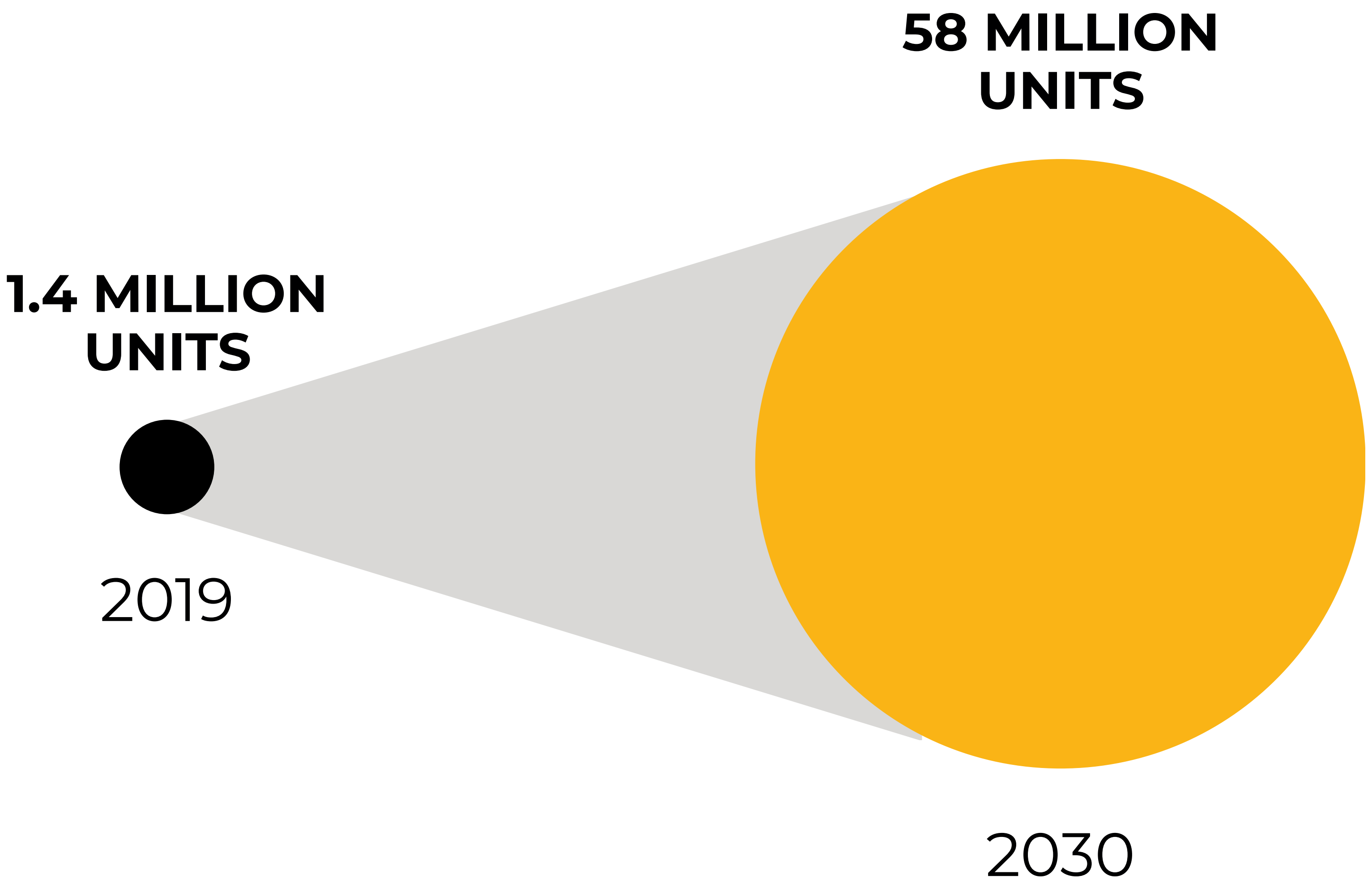
MAIN CUSTOMER CONCERNS OF AUTONOMOUS CARS*

SAFETY RISK DUE TO MACHINE ERROR	61%
SAFETY RISK DUE TO HUMAN ERROR	51%
INSUFFICIENT TECHNOLOGICAL READINESS LEVEL	35%
DATA SECURITY/PRIVACY	30%



* Worldwide; Arthur D. Little; 2021; 8,500 respondents

As consumer confidence steadily improves, global sales of private and commercial autonomous vehicles - with at least autonomy level 3 - are expected to increase.



That is an increase of over

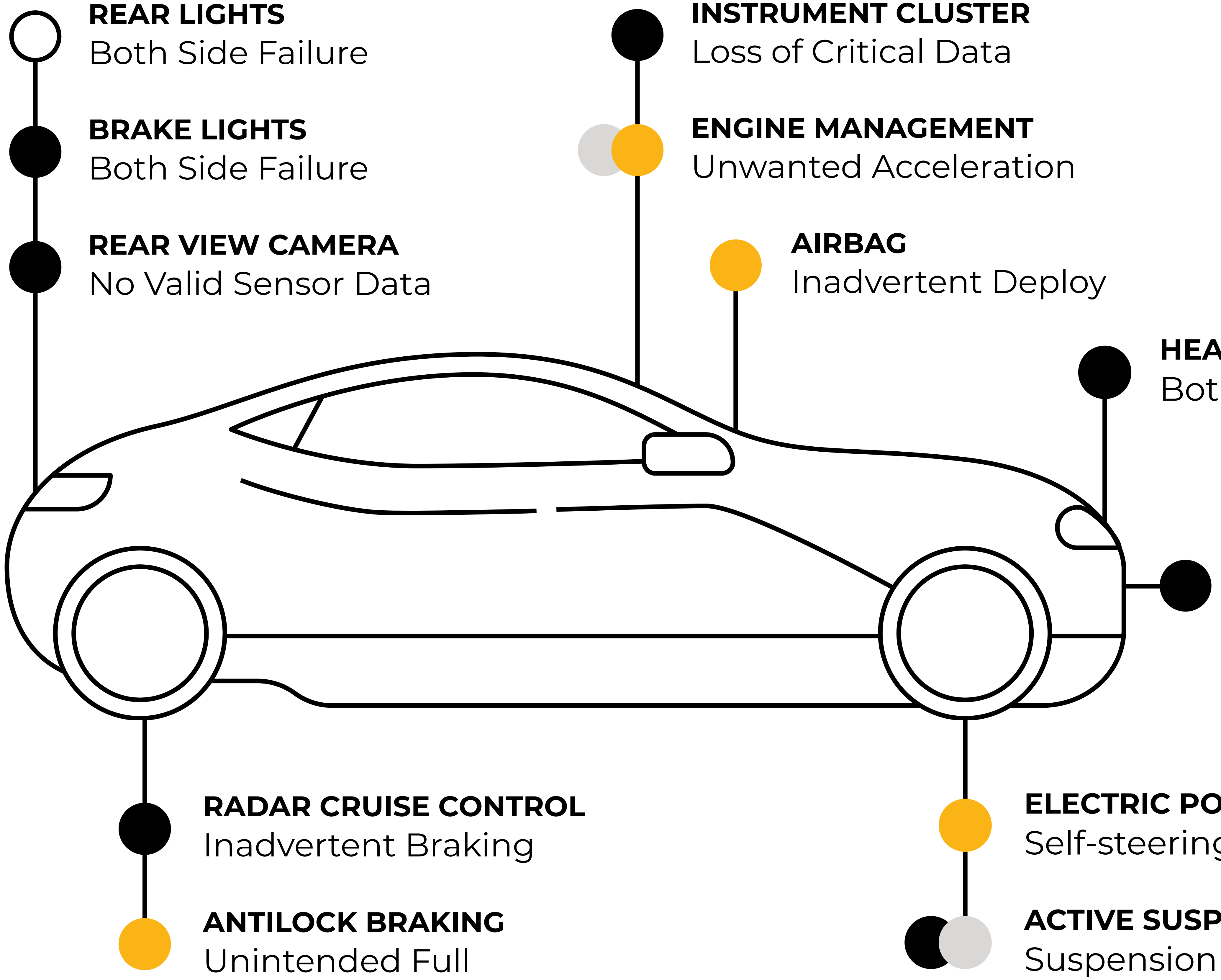
4000%

With effective execution - automated driving features have the potential to save thousands of lives from car accidents and reduce congestion. Still, handing over full driving control **requires tremendous confidence in the safety and security** of AVs.

Navigating Safely and Efficiently into the Future

Confirmation of system safety takes mileages of validation and verification for both ISO 26262 and SOTIF scenarios.

The four ASIL levels within ISO 26262 determine the requirements and mitigate risks and damage, ensuring **functional safety** throughout the process life cycle, from conceptualization through to design.



○ **REAR LIGHTS**
Both Side Failure

● **BRAKE LIGHTS**
Both Side Failure

● **REAR VIEW CAMERA**
No Valid Sensor Data

● **INSTRUMENT CLUSTER**
Loss of Critical Data

⚪🟡 **ENGINE MANAGEMENT**
Unwanted Acceleration

🟡 **AIRBAG**
Inadvertent Deploy

● **HEAD LIGHTS**
Both Side Failure

● **VISION ADAS**
Incorrect Sensor
Feedback

● **RADAR CRUISE CONTROL**
Inadvertent Braking

🟡 **ANTILOCK BRAKING**
Unintended Full
Power Braking

🟡 **ELECTRIC POWER STEERING**
Self-steering

●⚪ **ACTIVE SUSPENSION**
Suspension Oscillates

*ASIL Levels are for illustration only

ASIL LEVEL* A ○ B ● C ⚪ D 🟡

But, what if there is a hazard without system failure? SOTIF acts as a complementary standard in this case.

ISO 21448, safety of the intended functionality (SOTIF), encompasses performance and environmental limitations of autonomous vehicle systems.

The types of scenarios that must be solved to achieve ISO 21448 compliance are incredibly complex and **can only be identified by bringing safety analysis and simulation together** to replicate real-world conditions and predict results in advance.

Mitigating Cybersecurity Threats

The automotive industry has benefited from the digital revolution, bringing consumers a host of electronics enabled features.

Software-defined vehicles are more prone to the possibility of cyberattacks and potential malice to critical functions like steering, powertrain and ECU.

Companies can gain a competitive edge by **systematically performing threat analysis and risk assessment** to improve the safety and security of in-vehicle systems.

Simulation Assures Safety and Mitigates Security Threats in Automotive

Accelerate the development of automated driving technologies

Facilitate the compliance process to help systems conform to the highest standards

Support the development, testing, and validation of systems to ensure safety

Ansys

Contact us to learn more about Ansys solutions for automated and software-defined vehicles.

Contact Us to Learn More

Sources: Ansys, EE World Online, Embitel, Global X, LinkedIn, McKinsey, SAE, Secura, Statista, World Economic Forum