

Post-production Cybersecurity Support.

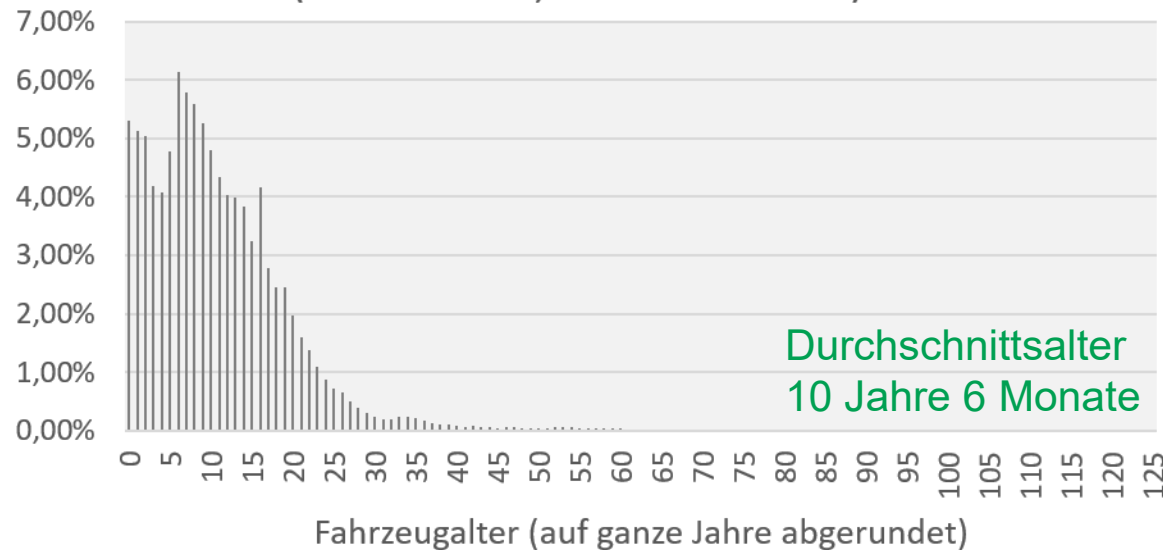
Österreichischer Verkehrsrechtstag 2026, 1.10.2026, Wien.



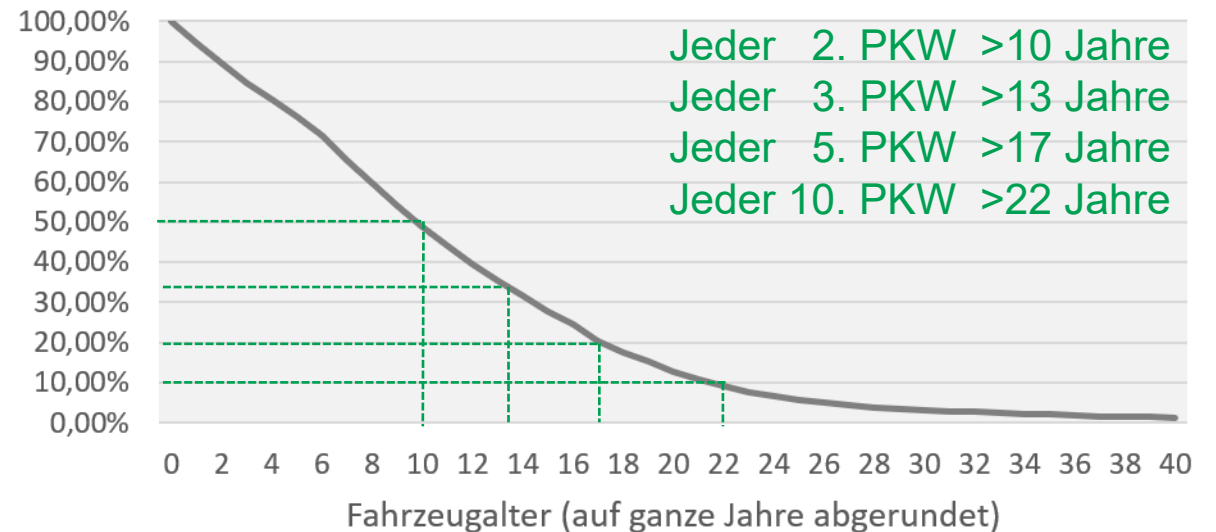
Fahrzeuge sind langlebige Wirtschaftsgüter von hoher gesellschaftlicher Bedeutung.

*) Bestand, NICHT durchschnittliche Nutzungsdauer

PKW-Bestand^{*)} in Deutschland nach Alter
(Quelle: KBA, Stand 1.1.2026)



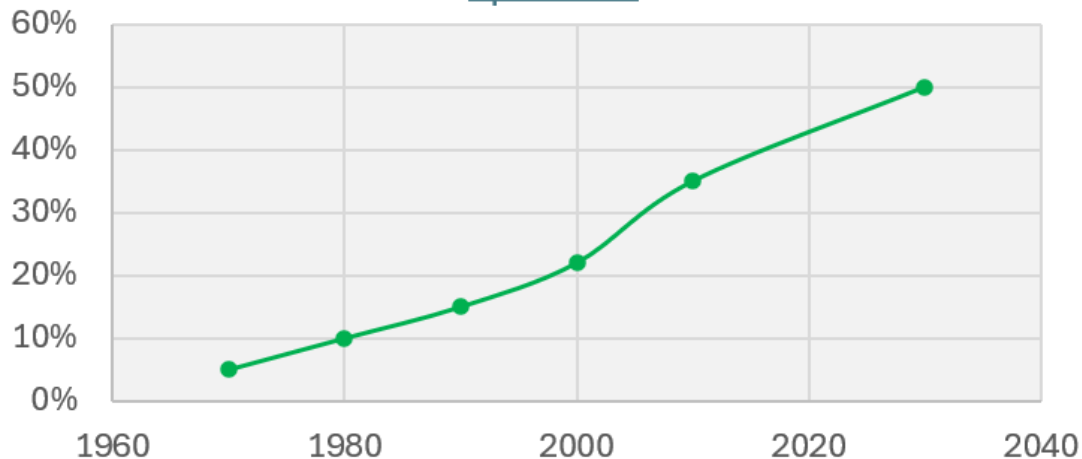
Akkumulierter PKW-Bestand^{*)} in Deutschland
(Quelle: KBA, Stand 1.1.2026)



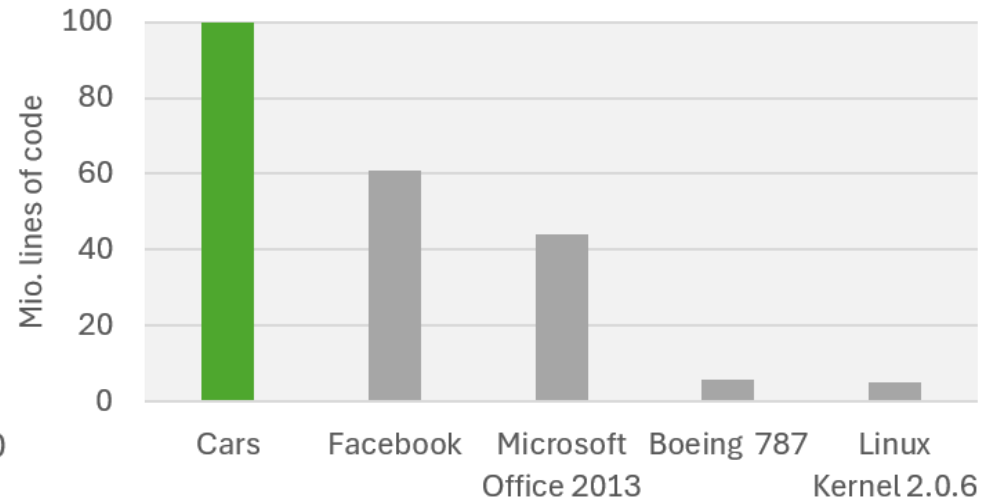
Industrie, Aftermarket und Infrastruktur sind auf diese langen Nutzungszeiträume ausgerichtet. Sie sind ein wichtiger Faktor für individuelle Mobilität, gesellschaftliche Teilhabe, Ressourceneffizienz und Werterhalt. Regulatorische Anforderungen sollten daher auch die Auswirkungen auf die langfristige Nutzbarkeit von Fahrzeugen berücksichtigen.

Digitalisierung erhöht Nutzen aber auch Cybersecurity-Relevanz.

Elektronikanteil an Fahrzeugkosten
Quelle: [How Software Is Eating the Car - IEEE Spectrum](#)



Software in 2017, Quelle: [Infographic: How Many Millions of Lines of Code Does It Take?](#)



Nach einer Schätzung von 2020 soll Level 5 automatisches Fahren 1 Mrd. Zeilen Code benötigen

Vernetzung, Software und Elektronik ermöglichen neue Komfort-, Sicherheits- und Mobilitätsfunktionen. Gleichzeitig entstehen zusätzliche Schnittstellen und potenzielle Angriffswege. Cybersecurity dient deshalb nicht nur der Zuverlässigkeit digitaler Funktionen, sondern auch dem Schutz von Verkehrssicherheit, Privatsphäre und Eigentum. Sie liegt damit sowohl im individuellen als auch im gesellschaftlichen Interesse.

UN R155 schafft einen regulatorischen Rahmen für Fahrzeug-Cybersecurity.

UN R155 wurde im Rahmen des UNECE-Weltforums WP.29 entwickelt und kann von den Vertragsparteien des Übereinkommens von 1958 angewendet werden.

UN R155 bildet die Grundlage für international harmonisierte Anforderungen an Fahrzeug-Cybersecurity und Cybersecurity-Managementsysteme.

Das CSMS enthält Prozesse zur:

- Beobachtung, Erkennung und Behandlung von Cybersecurity-Schwachstellen, Bedrohungen und Angriffen
- Identifikation, Bewertung, Kategorisierung und Behandlung von Cybersecurity-Risiken
- Überprüfung der Aktualität von Risikobewertungen und Schutzmaßnahmen
- Prüfung der Cybersecurity eines Fahrzeugtyps

Das CSMS muss Entwicklungs-, Produktions- und Post-Production-Phase abdecken. Die Post-Production-Phase endet nach der Definition der UN R155 erst, wenn kein Fahrzeug des betreffenden Fahrzeugtyps mehr in Betrieb ist.

Beinhaltet präventive/pro-aktive so wie reaktive/passive Maßnahmen

In der späten Post-Production-Phase verändern sich die technischen und organisatorischen Handlungsmöglichkeiten.

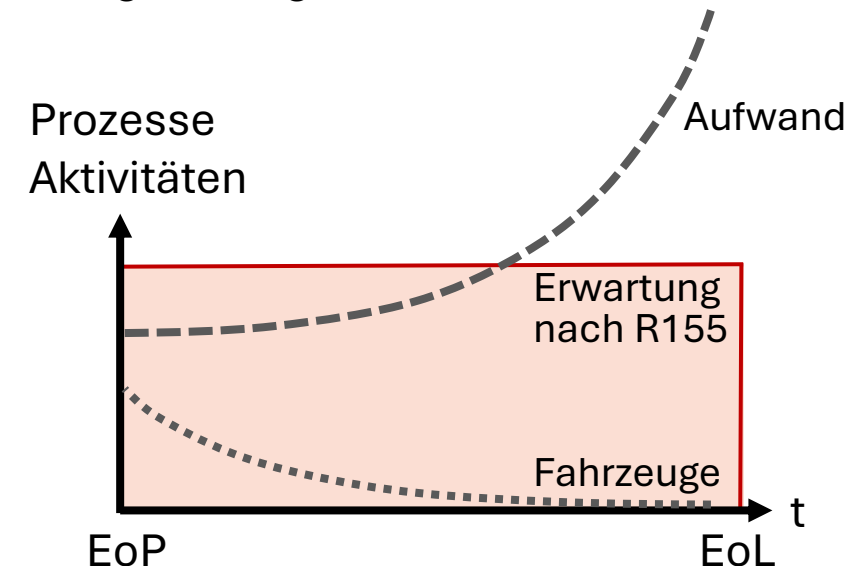
Grenzen für Softwareupdates

- begrenzte Prozessorleistung und Speicherkapazität (CPU, RAM, ROM)
- auslaufender Support für Entwicklungswerkzeuge und Softwarekomponenten
- nicht mehr gepflegte Open-Source-Komponenten
- eingeschränkte Verfügbarkeit von Zulieferern und Entwicklungsumgebungen
- zunehmender Verlust von Wissen über ältere Systemarchitekturen

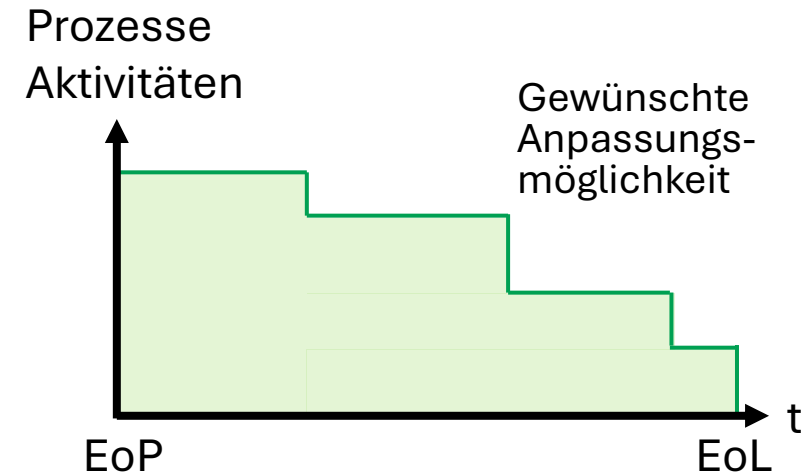
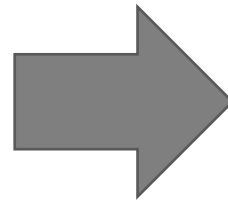
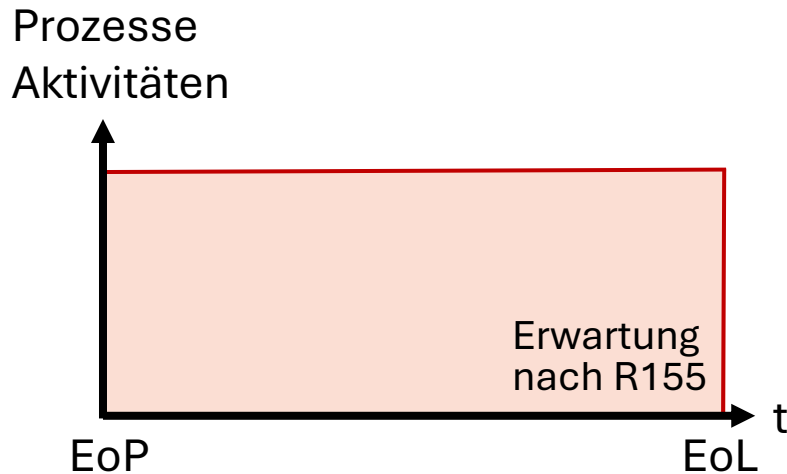
Grenzen für Hardwareupdates

- nicht mehr verfügbare oder nicht mehr produzierte Bauteile/HW
- veränderte Schnittstellen und Abhängigkeiten zwischen STGs
- mögliche fehlende technische Kompatibilität neuer Komponenten
- konstruktive Einschränkungen, etwa bei Bauraum, Energieversorgung oder Kühlung

Technische Einschränkungen können tlw. kompensiert werden. Der erforderliche Aufwand steigt mit zunehmendem Fahrzeugalter, während die Zahl der noch betriebenen Fahrzeuge eines Typs regelmäßig sinkt.



UN R155 sollte eine rechtssichere, risikobasierte Anpassung ausdrücklich ermöglichen.

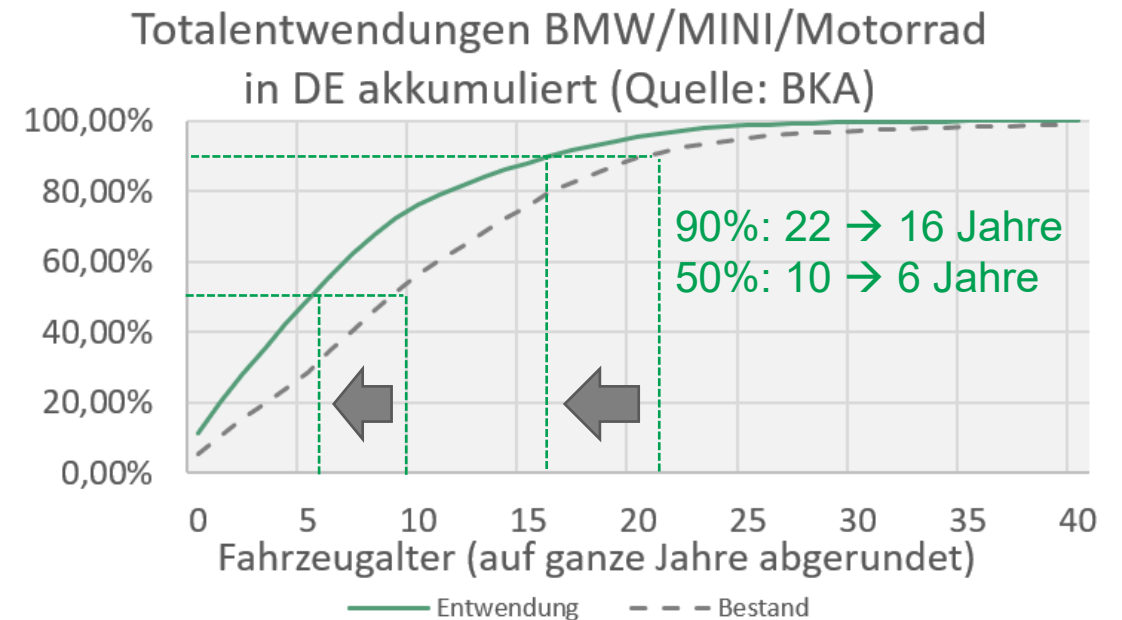
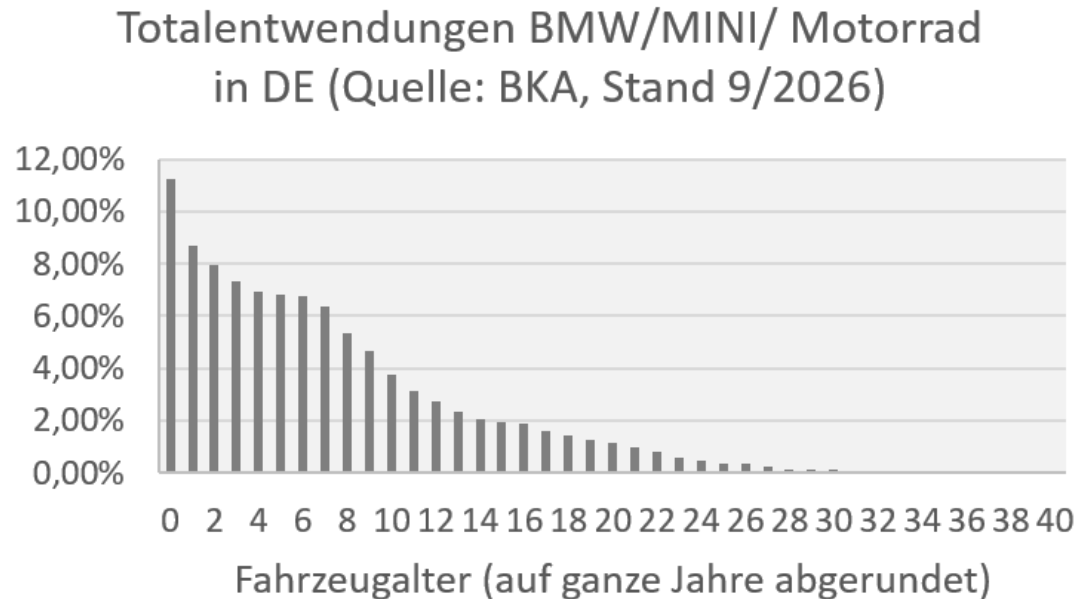


Das Interpretationsdokument zu UN R155 erkennt bereits an, dass Cybersecurity-Aktivitäten sich verändern könnten. Es nennt zudem die mögliche Deaktivierung nicht verpflichtender Funktionen.

Das Dokument ist jedoch eine Auslegungshilfe und schafft keine weltweit einheitlich verbindliche Regelung.

UN R155 selbst muss einen weltweit einheitlichen und rechtssicheren Rahmen für die risikobasierte Anpassung des Cybersecurity Supports in der Post-Production-Phase schaffen.

Beispiel Fahrzeugentwendung: Risiken können sich mit dem Fahrzeugalter verändern.



Die Altersverteilung bei Totalentwendungen zeigt beispielhaft, dass sich die Relevanz einzelner Angriffsszenarien im Fahrzeuglebenszyklus verändern kann. Daraus folgt keine generelle Entwarnung für ältere Fahrzeuge. Die Daten verdeutlichen vielmehr, warum Risiken differenziert nach Angriffsszenario, Eintrittswahrscheinlichkeit und möglicher Schadenswirkung bewertet werden sollten.

- **Das Schutzziel bleibt bestehen:** Auch in der Post-Production-Phase muss für Fahrzeuge ein dem jeweiligen Risiko angemessenes Cybersecurity-Niveau gewährleistet werden.
- **Die Rahmenbedingungen verändern sich:** Mit zunehmendem Fahrzeugalter werden bestimmte Prozesse und Maßnahmen technisch, organisatorisch und wirtschaftlich schwieriger oder verlieren gegenüber alternativen Maßnahmen an Wirksamkeit.
- **UN R155 sollte deshalb angepasst werden:** Die Regelung selbst muss eine rechtssichere und weltweit harmonisierte Möglichkeit schaffen, Prozesse, Aktivitäten und Schutzmaßnahmen in der Post-Production-Phase risikobasiert anzupassen.
- **Die Lösung erfordert gemeinsame Kriterien:** Industrie, Regulierungsbehörden, Nutzervertretungen und Aftermarket sollten einen Rahmen entwickeln, der Cybersicherheit, langfristige Fahrzeugnutzung, Werterhalt, Nachhaltigkeit und Mobilität miteinander verbindet.

Danke für Ihre Aufmerksamkeit!

