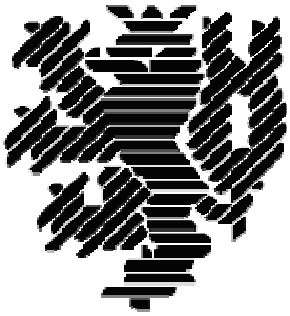
Beitrag zur Entwicklung einer alternativen Vorgehensweise für eine Proven-in-Use-Argumentation in der Automobilindustrie



Vom Fachbereich D – Abteilung Sicherheitstechnik der

Bergischen Universität Wuppertal

zur Erlangung des akademischen Grades

Doktor-Ingenieur (Dr.-Ing.)

genehmigte Dissertation

von

Diplom-Ingenieur Marco Heinz Schlummer

aus Soest

Gutachter:

Univ.-Prof. Dr.-Ing. habil. Arno Meyna

Univ.-Prof. Dr.-Ing. Stefan Bracke

Tag der mündlichen Prüfung:

16.03.2012

D468

Die Dissertation kann wie folgt zitiert werden:

urn:nbn:de:hbz:468-20120405-124552-2
[http://nbn-resolving.de/urn/resolver.pl?urn=urn%3Anbn%3Ade%3Ahbz%3A468-20120405-124552-2]

Für meinen Vater

Danksagung

Die vorliegende Arbeit entstand während meiner Tätigkeit als wissenschaftlicher Mitarbeiter im Fachgebiet „Sicherheitstheorie und Verkehrstechnik“ der Abteilung Sicherheitstechnik im Fachbereich D der Bergischen Universität Wuppertal.

Mein ganz besonderer Dank gilt meinem Mentor und Doktorvater Herrn Univ.-Prof. Dr.-Ing. Arno Meyna für die hervorragende fachliche Betreuung und die unglaubliche persönliche Unterstützung während meiner gesamten Zeit am Lehrstuhl.
Weiterhin möchte ich mich bei Herrn Univ.-Prof. Dr.-Ing. Stefan Bracke für die Übernahme des Koreferats bedanken.

Bei den weiteren Mitarbeiter am Lehrstuhl, Herrn Dr.-Ing. Dirk Althaus, Herrn Dr.-Ing. Andreas Braasch, Herrn M.Sc. Fabian Plinke, Herrn M.Sc. Benjamin Günnel und Herrn B.Sc. Jens Michalski, zu denen ich sagen kann, dass aus Kollegen wirklich Freunde werden können, möchte ich mich für die großartige Hilfe und die fachlichen Diskussion bedanken. In einem solchen Team wird das wissenschaftliche Arbeiten nicht nur von Erfolg gekrönt, sondern auch von Freude begleitet.

Ein weiterer Dank gilt meinen Kollegen bei einem großen deutschen Automobilhersteller, die nicht zuletzt die Projektarbeiten erst ermöglichten, die der vorliegenden Arbeit zugrunde liegen, sondern mich außerdem in allen Belangen vor Ort unterstützt haben.
Außerdem möchte ich mich bei Frau Dr.-Ing. Maria Binfet-Kull bedanken, die mich während meiner Studien- und Diplomarbeit erst auf den Bereich der Funktionalen Sicherheit und den damit zusammenhängenden Regelwerken und ihren Problemfeldern aufmerksam gemacht hat.

Mein größter Dank gilt aber meinen Eltern, die mir eine akademische Laufbahn erst ermöglichten, insbesondere meinem verstorbenen Vater, dem ich diese Arbeit widmen möchte, meinen beiden Schwestern und ihren Familien, die mich unterstützt haben, und natürlich meiner Freundin, die immer mein stärkster Rückhalt gewesen ist.

Kurzfassung

Der Einsatz von elektronischen Systemen in Kraftfahrzeugen nimmt immer weiter zu, insbesondere da ein Großteil der heutigen Innovationen im Automobilbereich mit elektronischen Systemen eng verknüpft ist. Die Funktionsumfänge solcher Systeme steigen dabei genau so an wie deren Komplexität. Wenn diese Systeme einen Sicherheitsbezug aufweisen, muss künftig die Automobilnorm ISO 26262 für den Bereich der Funktionalen Sicherheit berücksichtigt werden. Dadurch soll gewährleistet werden, dass von den Systemen keine Gefährdungen aufgrund von Funktionsausfällen oder Fehlfunktionen ausgehen. Hierbei stellt die Norm Anforderungen an den gesamten Lebenszyklus eines Produkts. Die ISO 26262 richtet sich vor allem an Neuentwicklungen. Sie stellt darüber hinaus für die Bewertung der Normenkonformität von Komponenten und Systemen, die die Automobilindustrie bereits seit Jahren im Einsatz hat und die sich über Tausende von Kilometern bewährt haben, eine so genannte Proven-in-Use-Argumentation zur Verfügung, die auf der Auswertung von Felddaten beruht.

Im Rahmen der vorliegenden Arbeit werden die normativ vorgegebenen Angaben und Anforderungen der Proven-in-Use-Argumentation kritisch untersucht und interpretiert. Als Konsequenz der dabei gewonnenen Erkenntnisse wird eine neue Vorgehensweise bei einem Betriebsbewährtheitsnachweis entwickelt, die praxisorientiert ist, erstmalig das reale Feldverhalten des Betrachtungsgegenstands berücksichtigt und die Möglichkeit einer individuellen Bewertung bietet. Diese neuartige Methodik wird anhand eines konkreten realen Beispiels aus dem Kraftfahrzeugbereich validiert und ihre Praxistauglichkeit verifiziert.

Abstract

The application of electronic systems in road vehicles is continuously rising, particularly because most of today's innovations in automotive industry are closely linked to such systems. The functional range of these systems increases as well as their complexity. If the systems are safety related, the upcoming standard for Functional Safety in road vehicles (ISO 26262) must be considered. Thereby, it shall be ensured that the system does not cause any hazards due to functional failures or malfunctions. The ISO 26262 provides requirements to the complete safety lifecycle of a product, especially focussing on new developments. Furthermore, the norm provides a so called proven-in-use-argument in order to show compliance with the standard for components and systems that have been used and still are in use in the field for many years. This procedure is based on the analyses of field data.

Within this paper, the normative specifications and requirements regarding the proven-in-use-argument are critically examined and interpreted. The results of this examination lead to the consequence of developing a new procedure to show that automotive items are proven in use. It has to be applicable for practice in everyday use, to consider the real field behaviour of an item and to provide the opportunity to do an individual assessment. The new approach is validated with a concrete example from the automotive industry and its suitability for daily use is verified.

Résumé

L’utilisation de systèmes électroniques dans les véhicules automobiles ne cesse de croître, notamment car la plupart des innovations actuelles du secteur automobile est étroitement liée aux systèmes électroniques. Les domaines d’application de ces systèmes se multiplient autant que leur complexité augmente. Lorsque ces systèmes sont utilisés en relation avec la sécurité, la norme automobile ISO 26262 doit être prise en compte pour le domaine de la sécurité fonctionnelle. Il doit alors être garanti qu’aucune menace n’émane des systèmes en raison de défaillances de fonctions ou de dysfonctionnements. En l’occurrence, les exigences énoncées par la norme concernent tout le cycle de vie d’un produit. La norme ISO 26262 s’adresse avant tout aux développements de nouveaux produits.
Qui plus est, pour l’évaluation de la conformité de la norme de composants et systèmes en service depuis des années dans l’industrie automobile et éprouvés sur des milliers de kilomètres, elle met à disposition une argumentation dite « Proven-in-Use », qui consiste en l’évaluation des données terrain.

Dans le cadre de cette thèse, les instructions normatives et les exigences de l’argumentation « Proven-in-Use » seront analysées et interprétées de façon critique. Grâce aux connaissances alors acquises, une nouvelle démarche, orientée vers la pratique, sera développée pour prouver l’aptitude à la pratique. Cette démarche prend pour la première fois en compte le comportement réel du système considéré sur le terrain et permet une évaluation individuelle. Cette nouvelle méthodologie sera validée au moyen d’un exemple concret et réel du domaine des véhicules automobiles et son application dans la pratique sera vérifiée.

Inhaltsverzeichnis

1 Einleitung und Motivation

Das tägliche Leben ohne Elektronik ist heutzutage nur noch schwer vorstellbar. Es spielt dabei keine Rolle, ob die Betrachtung in Richtung Arbeitsumfeld (Einsatz von Robotik und Maschinen, Notebooks und Beamer im Büro etc.), Konsumgüter (Spielkonsolen, Tablets, Smart Home etc.), Kommunikation (Smartphones, Internet etc.) oder Mobilität (Navigationsgeräte, EBike etc.) gelenkt wird; überall sind technische und elektronische Systeme im Einsatz, um den Menschen in allen Situationen und bei verschiedenen Tätigkeiten zu unterstützen und zu unterhalten. Sowohl die Gesellschaft als auch die Wirtschaft gewöhnen sich sehr schnell an die sich immer ändernden neuen Gegebenheiten und Innovationen. Der deutsche Informatiker und Professor der Technischen Universität Chemnitz Gerhard Faber stellte diesbezüglich fest, dass die Menschen eine „menschengerechte, eine verzeihliche, fehlertolerante, sanfte Technik benötigen, die die Stärken, aber auch die Schwächen des Menschen berücksichtigt“ [FAB 98]. Darin warnt der Kritiker fortschreitender Technik davor, dass der Mensch durch den zunehmenden Einsatz von technischen Systemen nicht entmündigt werden darf. Insbesondere im Zusammenhang mit sicherheitskritischen Systemen, wie einem Kernkraftwerk oder einem Flugzeug, stellt er die Behauptung, dass die Eliminierung des Menschen aus dem Mensch-Maschine-System zu mehr Sicherheit führt, als unbewiesen dar. Gerade in möglichen zeitkritischen und gefährlichen Situationen kann es stark auf die Erfahrung und die Intuition des Menschen ankommen.

Auch vor dem Automobilbereich macht diese Entwicklung keinen Halt, ganz im Gegenteil. Nahezu jeder Bereich und jede Funktion im Kraftfahrzeug (Motorsteuerung, Aktive Sicherheit, Passive Sicherheit, Fahrwerksabstimmung, Fahrerassistenzsysteme, Bordnetz etc.) beruht auf dem Einsatz von Elektrik und Elektronik, so dass ein heutiges Automobil ohne solche E/E[1]-Systeme nicht mehr denkbar erscheint. Dem Fahrer ist dabei oftmals gar nicht bewusst, wie viele elektronische Systeme ihn bei seinen Fahrten unterstützen. Oft wird ihm dies erst deutlich, wenn diese Systeme ausfallen oder Fehler verursachen und er dadurch gezwungen ist, mit seinem Fahrzeug in die Werkstatt zu fahren. Es sind auch schlimmere Fälle denkbar, wie das Liegenbleiben in einer kalten Winternacht auf einer abgelegenen Landstraße oder gar die Verwicklung in einen Verkehrsunfall, die auf Elektronik- oder damit zusammenhängenden Softwarefehlern beruhen. Der betroffene Fahrer wird aus seinen Erfahrungen eventuell entsprechende Konsequenzen ziehen und beispielsweise die

[1] Elektrik/Elektronik

Fahrzeugmarke wechseln und die negativen Erfahrungen in seinem Bekanntenumkreis verbreiten. Solche Elektronikfehler sind keine Seltenheit mehr. Durch die zunehmende Komplexität der Systeme und die immer kürzer werdenden Entwicklungszeiten, um nur einige Ursachen zu nennen, sind auch vermehrte Widrigkeiten in Sachen Zuverlässigkeit mit in die Fahrzeuge eingeflossen. Einen Überblick über den heutigen Einsatz und die Auswirkungen von E/E-Systemen im Automobil wird in Kapitel 2 gegeben.

Neben den „normalen“ Systemausfällen, die in der Regel „nur“ zu einem verärgerten Kunden führen, sind insbesondere Fehlfunktionen ein nicht zu vernachlässigendes Risiko. Jeder Automobilhersteller will beispielsweise den Fall vermeiden, dass eine Lenkunterstützung aufgrund eines Softwarebugs einen falschen Lenkbefehl ausgibt und das Fahrzeug deswegen von einer kurvigen Landstraße abkommt und vor einen Baum prallt. Die hierzu notwendigen Überlegungen und Tätigkeiten fallen in den Bereich der „Funktionalen Sicherheit“. Darunter werden Maßnahmen verstanden, die zur Reduzierung des inhärenten Risikos eines Fahrzeugs bzw. der Fahrzeugfunktionen beitragen, so dass es nicht zu Gefährdungen von beteiligten Personen kommen kann. Hierzu wird die international abgestimmte Norm ISO 26262 für den Automobilbereich einen erheblichen Beitrag leisten.

Ausführliche Informationen zur Funktionalen Sicherheit sowie Beschreibungen und Vergleiche der relevanten normativen Regelwerke für unterschiedliche Branchen sind in Kapitel 3 zu finden. Der Schwerpunkt wird in dem Kapitel auf die Beschreibung der automobilspezifischen Norm ISO 26262 gelegt. Dieses Normenwerk umfasst bei Betrachtung des gesamten Sicherheitslebenszyklus eines automotiven Produktes alle notwendigen Tätigkeiten, um die Funktionale Sicherheit von sicherheitsrelevanten E/E-Systemen im Kraftfahrzeug zu gewährleisten. Das Hauptaugenmerk der Norm richtet sich auf die Neuentwicklung von Komponenten und Systemen. Allerdings haben die Automobilhersteller und die beteiligten Zulieferunternehmen seit Jahren Komponenten und Systeme auf dem Markt, die sich im täglichen Einsatz über Tausende von Kilometern bewährt und die zu keinen sicherheitskritischen Ausfällen geführt haben. Um solche Produkte hinsichtlich der Normenkonformität bewerten zu können, bietet die ISO 26262 die Möglichkeit, einen Betriebsbewährtheitsnachweis durchzuführen. Diese Vorgehensweise beruht auf der Auswertung von Felddaten, um dadurch sozusagen nachträglich den Beweis zu erbringen, dass das Produkt mindestens eine genauso hohe Sicherheit bietet, als wenn es nach Normvorgaben entwickelt worden wäre. Die normativen Vorgaben zum automotiven

Nachweis der Betriebsbewährtheit (original: Proven in Use, PiU) und der damit zusammenhängenden Vorgehensweise werden in Kapitel 4 vorgestellt. Darin wird auch eine kritische Auseinandersetzung und Interpretation dieser Vorgaben vorgenommen.

Aus den Ergebnissen, der während der kritischen Auseinandersetzung mit den Normvorgaben gewonnenen Erkenntnissen, ergibt sich die Motivation der vorliegenden Arbeit, nämlich eine Alternative zur normativen PiU-Untersuchung zu entwickeln. Eine solche wird in Kapitel 5 präsentiert. Diese neue Vorgehensweise berücksichtigt erstmalig das tatsächliche Verhalten des Betrachtungsgegenstandes im Feld und geht somit nicht von Annahmen aus. Weiterhin werden individuelle Bewertungskriterien entwickelt, die einen neuartigen Betriebsbewährtheitsnachweis für die Automobilindustrie zulassen.

Um die Anwendbarkeit des neu erarbeiteten Verfahrens zu verdeutlichen, wird die Methode in Kapitel 6 exemplarisch für einen Kandidaten einer sicherheitsrelevanten Fahrzeugfunktion durchgeführt. Die dabei verwendeten Informationen stammen aus realen Datenbanken eines deutschen Fahrzeugherstellers und spiegeln das tatsächliche Betriebsverhalten der E/E-Komponente wider.

In Kapitel 7 werden die durchgeführten Analysen sowie der neue Ansatz zusammenfassend dargestellt und rückblickend bewertet. Ein Ausblick auf weitere erforderliche Schritte und zukünftige Arbeiten runden dieses Kapitel ab, ehe der Hauptteil der vorliegenden Arbeit mit dem Literaturverzeichnis in Kapitel 8 abgeschlossen wird.

Im Anhang befinden sich schließlich ein Verzeichnis der in der Arbeit verwendeten Abkürzungen sowie eine umfangreiche Zusammenstellung der Ergebnisse der durchgeführten Analysen.

2 Überblick Elektronikeinsatz im Automobilbereich

Elektrischen und elektronischen Systemen in Kraftfahrzeugen kommt eine immer stärker werdende Bedeutung zu. Sie tragen zum Einen dazu bei, den Fahrspaß des Fahrers, die Leistung des Fahrzeugs und natürlich die Sicherheit der Verkehrsteilnehmer zu erhöhen, und zum Anderen sollen durch ihren Einsatz die Kosten, die Emissionen und der Kraftstoffverbrauch reduziert werden. Fast alle Neuerungen in Kraftfahrzeugen sind heutzutage mit elektronischen oder mechatronischen[2] Systemen in Verbindung zu bringen. Dies belegt eine Aussage aus dem Jahr 2005 von Branchenbeobachter Nick Margetts vom Marktforschungsinstitut Jato, der in einer Pressemitteilung des Themendienstes der Deutschen Presseagentur sagte, dass „in der Elektronik das weitaus größte Potenzial für gewinnträchtige Neuerungen steckt“ [HB 05a]. Elektronik und auch Mechatronik sind folglich längst zu „Schlüsseltechnologien“ für die Automobilindustrie geworden. Im Jahr 2003 stellte der Darmstädter Wissenschaftler Rolf Isermann fest, „dass 80% bis 90% der Innovationen rund um Maschinen und Autos auf mechatronische und elektronische Erfindungen zurückgehen“ [GRA 03]. Andere Experten sehen diesen Prozentsatz nicht ganz so hoch: der Anteil an den Innovationen bei Software und Elektronik wird in [HB 05b] mit rund 70% angegeben. Anhand dieser Aussagen wird deutlich, welchen Stellenwert elektronische und mechatronische Systeme mit der darin enthaltenen Software in Kraftfahrzeugen haben. Mit zunehmender Elektronik im Auto erhöht sich auch der Softwarebedarf. Noch offensichtlicher wird diese Tatsache daran, dass ein modernes Automobil eine deutlich höhere Rechenleistung aufweist als die des Raumfahrzeuges der Raumfahrtmission Apollo 13 [GNE 06]. In heutigen modernen Oberklasse-Personenkraftwagen sind rund 80 Steuergeräte[3] u.a. für Motor, Getriebe und Bremse verbaut [HB 05a], ein aktueller Audi A8 verfügt sogar über jeweils etwa 50 Hauptsteuergeräte und 50 kleinere Steuergeräte [VDI 11]. Aber auch bei den gegenwärtigen Nutzfahrzeugen sind nach [GNE 06] mittlerweile mehr als 70 Steuergeräte vorhanden. Wird der Fokus auf die Wertschöpfungskette gelegt, so wird deutlich, dass im Jahr 2002 der Anteil der Elektronik bei 22% lag und er Prognosen zufolge bis 2010 auf 35% ansteigen wird [REI 11a]. Zum Vergleich lag der Elektronikanteil bei Lastkraftwagen im Jahr 2002 bei 7% und für 2010 werden hier 15% erwartet [GNE 06]. Ob diese für das Jahr 2010 prognostizierten Werte tatsächlich erreicht worden sind, konnte bislang nicht ermittelt werden. Die Bedeutung

[2] Unter Mechatronik wird nach [ISE 08] ein interdisziplinäres Gebiet verstanden, bei dem Maschinenbau, Elektrotechnik und Informatik zusammenwirken.
[3] Steuergeräte stellen sozusagen die Zentrale eines jeden elektronischen Systems dar [REI 11a].

von Elektronik und Software wird weiterhin deutlich, wenn die Entwicklung von Computerchips in Fahrzeugen betrachtet wird. 2006 waren nach [GNE 06] Chips im Wert von 250 Euro in jedem Auto und von etwa 1.000 Euro in jedem Lastwagen verbaut. Bis 2010 werden hier Steigerungen auf 300 Euro bis 350 Euro für Pkws und auf etwa 2.500 Euro bei Lkws prognostiziert.

An dem Zweck der zunehmenden „High-Tech-Ausstattung“ von Fahrzeugen zweifeln allerdings immer mehr Experten. Franz Fehrenbach, Vorsitzender der Geschäftsführung der Robert Bosch GmbH, konstatierte 2005 beispielsweise, dass, wenn bei der zunehmenden Technisierung „der Kundennutzen nicht erkennbar sei, die Industrie auf technische Spielzeuge in den Fahrzeugen verzichten solle, um die Komplexität nicht unnötig zu erhöhen“ [HB 05c]. Auch Thomas Weber, damaliger Vorstand für Entwicklung bei DaimlerChrysler, stellte im Jahr 2004 in [EFL 04] fest, dass Innovationen, die dem Kunden keinen Nutzen bringen, nicht mehr angeboten werden. Im Jahr zuvor hatte Mercedes rund 300 „Gimmicks“ aus seinen Modellen herausgenommen, deren Existenz vom Kunden noch nicht einmal bemerkt worden waren, wie z.B. eine Tunnel-Schaltung für die Klimaanlage. Die Autohersteller wollen künftig also nach dem Motto „weniger ist mehr“ verfahren. Dies zielt in erster Linie auch auf die Komplexität der Systeme ab, die weiter reduziert werden soll, allerdings ohne auf sinnvolle Innovationen und Funktionen zu verzichten.

Der zunehmende Einsatz von Elektronik im Automobil birgt neben dem offensichtlichen Nutzen, wie z.B. steigender Komfort und stetig wachsende Sicherheit, auch ein nicht zu vernachlässigendes Fehler- und Gefahrenpotenzial. In nachfolgender Abbildung Bild 2-1 ist die Entwicklung des Pkw-Bestandes der Bundesrepublik Deutschland den Zahlen der im Straßenverkehr Getöteten gegenübergestellt. Die Daten stammen dabei vom Statistischen Bundesamt, dem Kraftfahrt-Bundesamt (KBA) sowie dem Allgemeinen Deutschen Automobil-Club (ADAC).

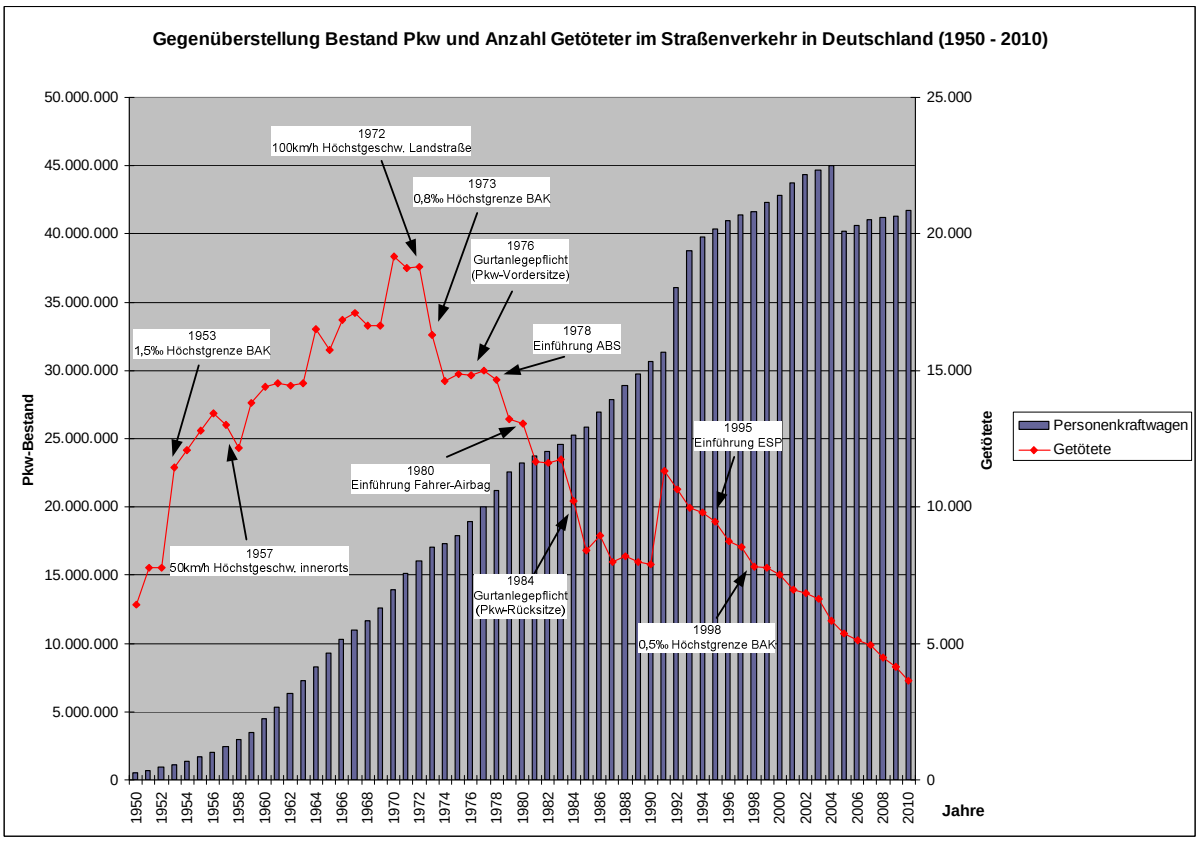


Bild 2-1: Gegenüberstellung Pkw-Bestand und Anzahl Getöteter im Straßenverkehr in Deutschland (1950 - 2010)

In Bild 2-1 ist zu erkennen, dass die Zahl der Personenkraftwagen in Deutschland seit dem Jahr 1950 deutlich und stetig zunimmt. Die beiden Sprünge in dem Verlauf sind wie folgt zu erklären:

- Sprung 1991/92: Deutsche Wiedervereinigung
- Sprung 2004/05: ab 2005 ohne vorübergehend stillgelegte Fahrzeuge.

Des Weiteren ist ersichtlich, dass die Zahl der im deutschen Straßenverkehr Getöteten bis zum Jahr 1970 angestiegen und seitdem in der Tendenz kontinuierlich gefallen ist. Auffällig ist hier der Peak von 1990 nach 1991, der auf der deutschen Wiedervereinigung beruht. Im Jahr 2010 waren zwar immer noch 3.651 Verkehrstote in Deutschland zu beklagen, diese Zahl wurde aber von ihrem Maximalwert von 19.193 Getöteten im Jahr 1970 deutlich reduziert. Auch im vergangenen Jahrzehnt wurde die Zahl der Verkehrstoten mehr als halbiert (2000 starben noch 7.503 Personen auf deutschen Straßen). Zu dieser Entwicklung haben neben gesetzlichen Vorgaben (u.a. Einführung von Höchstgeschwindigkeiten und der „Promillegrenze“), den Verbesserungen in der Infrastruktur (Ausbau von Straßen, Leitplanken etc.) und der Einführung von passiven Sicherheitseinrichtungen in den Kraftfahrzeugen (u.a.

Sicherheitsgurt, Airbags) nicht zuletzt auch die aktiven Sicherheitssysteme, wie das ABS (Antiblockiersystem) oder ESP (Elektronisches Stabilitätsprogramm), einen erheblichen Beitrag geleistet. Einige dieser „Meilensteine“ sind in Bild 2-1 dargestellt.

Die modernen Elektroniksysteme zeichnen sich zunehmend durch eine sehr hohe Komplexität aus und sind dadurch gekennzeichnet, dass eine Vielzahl von Informationen zwischen ihnen ausgetauscht wird. Oftmals sind Funktionen sogar über mehrere Steuergeräte verteilt, die intelligent miteinander vernetzt sein müssen, so dass es teilweise zu unübersichtlichen Systemverbünden kommt, bei denen schwer festzustellen ist, wo genau ein Fehler liegt. Je komplexer ein System wird, desto zunehmender scheint auch das Fehler- und Ausfallrisiko zu sein. Hinzu kommt, dass gerade in Kraftfahrzeugen die Systeme einer Vielzahl an Einflüssen ausgesetzt sind und diesen widerstehen müssen, wie z.B. Feuchtigkeit, Vibrationen, elektromagnetischen Störeinflüssen oder starken Temperaturschwankungen. So kommt es zu einer Reihe von Fehlern und Mängeln, die ihre Ursache im Komplex der Elektrik/Elektronik haben. In nachfolgendem Bild 2-2 sind die Mängelanteile des Jahres 2010 dargestellt, die der Auto Club Europa (ACE) bei seinen rund 100.000 Einsätzen bei Autopannen in Deutschland verzeichnete.

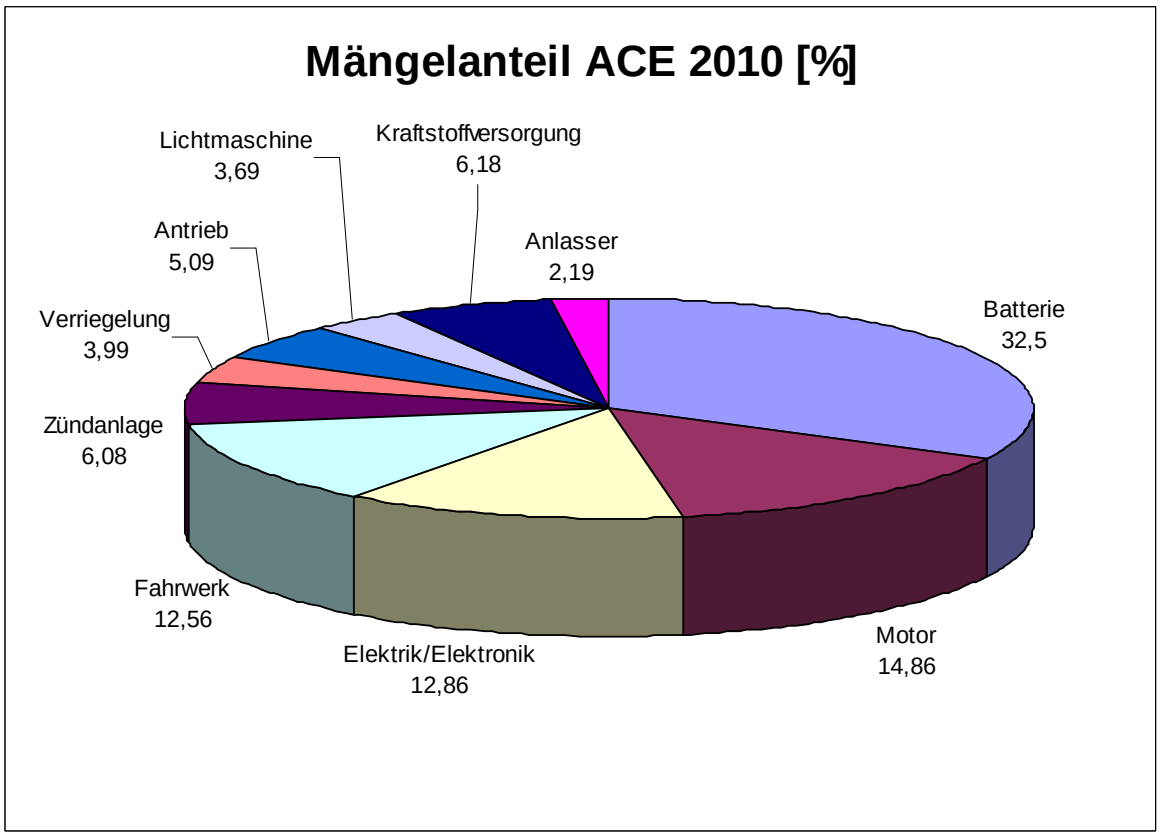


Bild 2-2: Mängelanteil Deutschland 2010 nach [ACE 11]

Bild 2-2 zeigt, dass knapp ein Drittel aller Autopannen auf funktionsuntüchtige Batterien zurückzuführen ist. An zweiter Stelle der Pannenstatistik des ACE liegen defekte Motoren, die etwa 15% ausmachen. Mit knapp 13% aller Mängel nimmt eine störanfällige Elektrik/Elektronik den dritten Platz ein. Das Center Automotive Research der Fachhochschule Gelsenkirchen kam im Jahr 2004 aufgrund der Analyse der Pannenstatistik des ADAC sogar auf einen Wert von über 60%, den die Elektrik und Elektronik an Autopannen hatte [DUD 04]. Bei den ADAC-Daten wurde allerdings nur von Mängeln an der „Allgemeinen Fahrzeugelektrik“ gesprochen, wozu z.B. auch Probleme mit der Batterie zählen. Die Gründe für das Ansteigen der Ausfälle sind vielschichtig und reichen nach [DUD 04] von zu schneller Integration noch nicht ausgereifter Innovationen bis zur Überbeanspruchung des elektrischen Bordnetzes im Automobil.
Experten aus der Automobilindustrie halten hier jedoch dagegen und stellen fest, dass bei vielen Berichterstattungen zu pauschal von Elektronikpannen ausgegangen wird, während die wirklichen Ausfallursachen gar nicht oder nicht differenziert genug dargelegt werden. Oftmals werden z.B. schlichte Elektrikprobleme durch mechanische Defekte verursacht und diese werden im Nachhinein nur als Elektronikproblem benannt (s. [BOH 04] und [WEI 03]). Die dennoch vorliegenden Schwierigkeiten sind unabhängig vom Hersteller, so dass von einem Branchenproblem gesprochen werden muss [DUD 04].

Interessant ist in diesem Zusammenhang auch die Auswertung von Gründen für Rückrufaktionen im Automobilbereich der vergangenen Jahre (s. Bild 2-3). Die in nachfolgender Abbildung verwendeten Daten stammen allesamt aus den Jahresberichten des Kraftfahrt-Bundesamts [KBA 10].

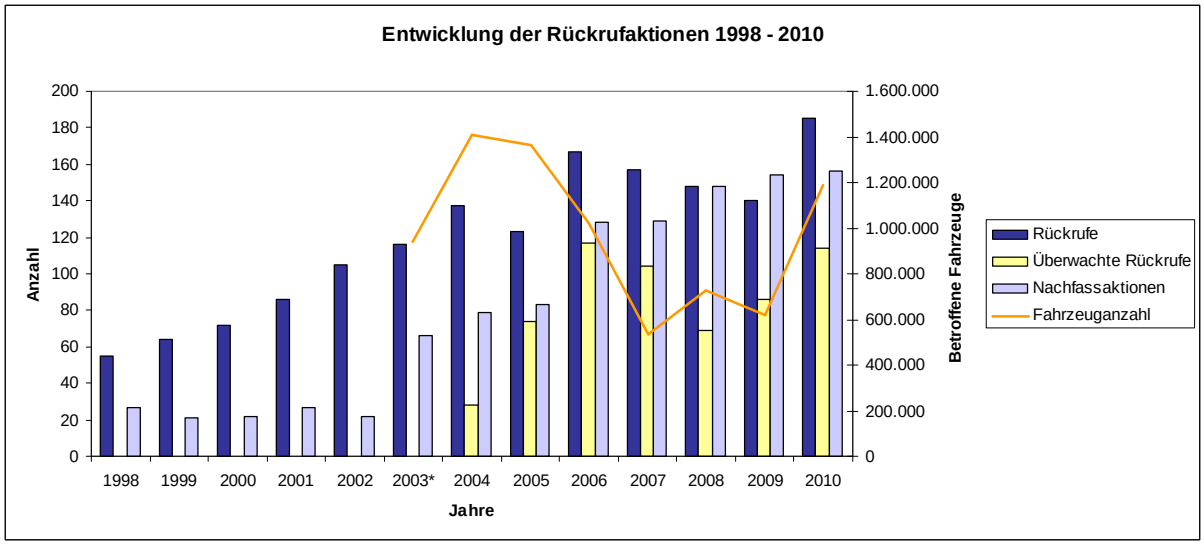


Bild 2-3: Entwicklung der Rückrufaktionen in Deutschland von 1998 bis 2010 nach KBA

In obiger Abbildung sind

- die vom KBA veranlassten Rückrufe[4] (in dunkelblauer Farbe),
- die vom KBA überwachten Rückrufe[5] (in hellgelber Farbe),
- die vom KBA durchgeführten Nachfassaktionen[6] (in hellblauer Farbe) sowie
- die von den Rückrufen betroffene Fahrzeuganzahl (in oranger Farbe)

von 1998 bis 2010 dargestellt. Im Jahr 2003 fand bei der Berechnung der Rückrufe eine Anpassung des betrachteten Zeitraums statt, so dass ab diesem Zeitpunkt immer ein komplettes Jahr in die Betrachtung einfloss. Aus diesem Grund ist in Bild 2-3 ein Sternchen beim Jahr 2003 zu erkennen.

In Bild 2-3 ist zu erkennen, dass die Anzahl der Rückrufaktionen bis zum Jahr 2006 in der Tendenz stetig zugenommen hat (bis auf einen Rückgang von 2004 nach 2005) und dann drei Jahre rückläufig gewesen ist. Im Jahr 2010 musste allerdings mit 185 veranlassten Rückrufen der vorläufige Höhepunkt der Aufzeichnungen verzeichnet werden. Auch stieg die betroffene Fahrzeuganzahl im Vergleich zu den Vorjahren auf einen Wert von rund 1,19 Millionen Fahrzeuge deutlich an. Neben den absoluten Zahlen zu den Rückrufaktionen veröffentlicht das KBA in seinem Jahresbericht außerdem eine baugruppenbezogene Verteilung der Mängel bezüglich der überwachten Rückrufe. Für das Jahr 2010 muss dabei festgehalten werden, dass

[4] Eine Rückrufpflicht besteht, wenn von einem in Verkehr gebrachten Verbraucherprodukt Gefahren für die Sicherheit und Gesundheit von Personen ausgehen.
[5] Bei besonderer Gefährlichkeit des Mangels muss der Rückruf vom KBA überwacht werden.
[6] Nachfassaktionen sind vorzunehmen, wenn sich Fahrzeughalter aufgrund einer ersten Information über den Mangel nicht bei einer Werkstatt zur Mangelbeseitigung gemeldet haben. Sie erfolgen in der Regel bei überwachten Rückrufaktionen.

über 60% aller Mängel mechanische Ursachen hatten. Der Elektrik/Elektronik wird ein Anteil von 27% an den Mängeln bei den überwachten Rückrufen zugeordnet. Das KBA gibt allerdings an, dass hierbei teilweise mechanische oder hydraulische Probleme mit einzubeziehen sind [KBA 10].

Zusammenfassend kann anhand der zuvor genannten Fakten festgehalten werden, dass elektronische Systeme zwar für viele positive Errungenschaften und Verbesserungen in allen Bereichen des Straßenverkehrs einen erheblichen Beitrag geleistet haben und immer noch leisten, mit der zunehmenden Komplexität der Systeme steigt aber auch das Ausfallrisiko. Durch einen Fehler oder Ausfall eines elektronischen Systems darf es nicht zu einer Gefährdung von Verkehrsteilnehmern kommen. Aus diesem Grund rückt die Funktionale Sicherheit zur Vermeidung von unakzeptablen Risiken durch mögliches Fehlverhalten von elektronischen Systemen immer stärker in den Vordergrund bei der Fahrzeugentwicklung. Gerade sicherheitsrelevante Fahrerassistenzsysteme (FAS) sollen den Fahrer entlasten, den Fahrkomfort erhöhen und vor allem die Sicherheit in Grenzsituationen verbessern. Unter FAS werden in diesem Zusammenhang auch Systeme für die Fahrdynamik und die aktive Sicherheit gezählt. Bei dem Einsatz solcher Systeme muss sichergestellt sein, dass sie kein zusätzliches Risiko darstellen, sondern vielmehr einen Sicherheitszugewinn leisten. Um dies zu erreichen, müssen die von einem System bzw. die von einer Funktion ausgehenden Gefährdungen und Risiken sinnvoll geschätzt werden, um eventuelle Gegenmaßnahmen einleiten zu können. Dies kann mit Hilfe einer so genannten Risikoanalyse gemacht werden, wie es in diversen Standards, wie z.B. der IEC 61508 oder ISO 26262, vorgeschlagen wird.
Der Themenkomplex der Funktionalen Sicherheit von elektrischen/elektronischen Systemen wird in zukünftigen Fahrzeugkonzepten nicht an Wichtigkeit verlieren. Insbesondere vor dem Hintergrund des Aufkommens und der stärker werdenden Bedeutung der Elektromobilität steht die gesamte Automobilindustrie vor weiteren interessanten Aufgaben. Es ist hierbei nach [FET 11] nicht auszuschließen, dass es durch die Elektrifizierung des Antriebsstrangs zu einem Umbruch in der etablierten Wertschöpfungskette kommen wird, da andere Kernkompetenzen erforderlich werden. Die Konsequenz ist daher, dass der bislang eher branchenfremde Bereich der Elektrochemie im Zusammenspiel mit der Elektronik und Mechanik an Einfluss gewinnen wird. Diese neuen Entwicklungen machen auch vor Fragestellungen der Funktionalen Sicherheit keinen Halt, so dass in Zukunft weitere Aufgaben und Herausforderungen auf die Ingenieure zukommen werden.

3 Funktionale Sicherheit

In diesem Kapitel werden zunächst Erläuterungen gegeben, die dem Grundverständnis bezüglich des Themengebiets der Funktionalen Sicherheit dienen. Des Weiteren werden die relevanten Normenwerke, die sich mit diesem Komplex beschäftigen, dargestellt und miteinander verglichen. Der Schwerpunkt wird auf das geltende Regelwerk für den Bereich der Automobilindustrie, die ISO 26262, gelegt.

3.1 Allgemeines zur Funktionalen Sicherheit

Funktionale Sicherheit (FuSi), auch Funktionssicherheit genannt, ist nach [LÖW 10] als der Teil der Gesamtsicherheit eines technischen Systems zu verstehen, der von der korrekten und einwandfreien Funktion des sicherheitsbezogenen Systems abhängt. [BÖR 11] erklärt die Funktionale Sicherheit allgemein damit, dass eine Komponente bzw. ein System seine sicherheitsgerichtete Aufgabe entsprechend des abzudeckenden Risikos korrekt zu erfüllen hat. Dies muss auch beim Auftreten interner Fehler oder Ausfälle geschehen - oder ein entsprechend definierter sicherer Zustand muss eingenommen werden. Insbesondere hinsichtlich sicherheitsrelevanter Aufgaben, wie beispielsweise der Steuerung von Fahrzeugen jeglicher Art oder der Überwachung von Kraftwerken, werden digitale Systeme mit einer Vielzahl an Komponenten eingesetzt. Der FuSi kam in den vergangenen Jahren und Jahrzehnten eine immer stärker werdende Bedeutung in allen technischen Bereichen zu. Natürlich haben sich die Hersteller technischer Produkte auch vorher bereits Gedanken zu der Sicherheit und den möglichen Auswirkungen ihrer Erzeugnisse gemacht, allerdings kam es erst in den späten 1980er und 1990er Jahren zu den ersten Standardisierungsversuchen, um sicherheits- und zuverlässigkeitstechnische Methoden systematisch in einen Entwicklungsprozess zu implementieren.

Hierzu stellen Normen eine wichtige Informationsquelle für die Hersteller und Entwicklungsingenieure dar. Diese erreichen bei Beachtung und Einhaltung solcher Vorschriften, die keine rechtliche Bindung haben, eine gewisse Sicherheit, dass sie nach bekannten und effektiven Methoden vorgegangen sind, welche den Stand von Wissenschaft und Technik widerspiegeln. Ein Verstoß dagegen kann allerdings erhebliche rechtliche Konsequenzen nach sich ziehen, vor allem wenn ein bewusstes Handeln oder Fahrlässigkeit mit im Spiel sind. Eine gute Kenntnis der relevanten Normenlandschaft sowie deren Anwendung sind folglich notwendig. Neben Normen existieren weitere Quellen, die

notwendige Tätigkeiten bei der Systementwicklung aufzeigen. Hierzu zählen u.a. industriespezifische Richtlinien, wie sie z.B. aus der Luftfahrtindustrie oder der chemischen Industrie bekannt sind. [BÖR 11] gibt weiterhin an, dass auch durch Überlegungen von Aufsichtsbehörden und der Industrie selbst Risiken definiert und geregelt werden, woraus sich wiederum industriespezifische Normen entwickeln. Daneben existieren generische Normen, welche branchenübergreifend sind und Gültigkeit für alle Industriebereiche haben. Eine solche Sicherheitsgrundnorm für den Bereich FuSi ist die IEC 61508. Darin wird die Funktionale Sicherheit als Teil der Gesamtsicherheit, bezogen auf die EUC[7] und das EUC-Leit- oder Steuerungssystem, die von der korrekten Funktion des E/E/PE[8]-sicherheitsbezogenen Systems, sicherheitsbezogenen Systemen anderer Technologie und externer Einrichtungen zur Risikominderung abhängt, definiert [DIN 02b]. Sie hat ihren Hintergrund in der Anlagentechnik und der Prozessindustrie. Der Begriff „sicherheitsbezogen“ trifft nach [elp 05] auf jedes programmierte System zu, in welchem ein Fehler (allein oder in Kombination mit anderen Fehlern) zu Verletzung oder Tod von Menschen, katastrophalen Schädigungen der Umwelt oder Zerstörungen von Sachgütern führen kann. Mit Einführung der IEC 61508 wurde eine branchenübergreifende Richtlinie für alle sicherheitsgerichteten Systeme geschaffen.

3.2 IEC 61508

In diesem Abschnitt werden einige wichtige Aspekte zum Hintergrund, Aufbau und Inhalt der IEC 61508 erläutert.

3.2.1 Historie

Die Normenreihe IEC 61508 zur Funktionalen Sicherheit wurde nach [DKE 02] im Juli 2001 durch das technische Büro der europäischen Normungsorganisation CENELEC[9] als Normenreihe EN 61508 ratifiziert und übernommen. Sie wurde im August 2001 europaweit veröffentlicht. Seitdem erfolgte weltweit die nationale Implementierung der Norm. In Deutschland wurde die Normenreihe im November 2002 als DIN EN 61508 ins deutsche Normenwerk übernommen. Dabei handelte es sich um die Teile 1 bis 5 der Norm, die im Juli

[7] Unter Equipment Under Control (EUC) versteht [DIN 02b] eine Einrichtung, eine Maschine, einen Apparat oder eine Anlage, die zur Fertigung, Stoffumformung, zum Transport, zu medizinischen oder anderen Tätigkeiten verwendet wird.
[8] Elektrisch/elektronisch/programmierbar elektronisch
[9] CENELEC (Comité Européen de Normalisation Électrotechnique) ist das europäische Komitee für elektrotechnische Normung.

2003 mit den deutschen Fassungen der Teile 6 und 7 vervollständigt wurde. Im Herbst 2005 wurde ein Beiblatt zur DIN EN 61508 veröffentlicht, welches den Teil 0 „Funktionale Sicherheit und die IEC 61508“ der Normenreihe darstellt. Hierin enthalten sind die deutschen Übersetzungen des Technischen Berichts IEC/TR 61508-0:2005 sowie häufig gestellter Fragen zur Norm aus der „Functional Safety Zone“ der IEC-Homepage. Im Februar 2011 erschienen überarbeitete Versionen aller Normenteile, die dem Autor der vorliegenden Arbeit allerdings nicht zur Verfügung standen.
Nachfolgend wird der internationale Standard verwendet, da er in der Fachwelt verbreiteter ist, die Verweise beziehen sich jedoch auf das nationale Regelwerk.

3.2.2 Motivation und Hintergrund

Zum Zeitpunkt der Entwicklung der Normenreihe IEC 61508 gab es zahlreiche Anwendungsbereiche, die bereits viele Jahre lang Sicherheitsfunktionen von Systemen ausführen ließen, die aus elektrischen und/oder elektronischen Bauteilen bestanden. Systeme, welche auf digitalen Rechnern basieren (so genannte programmierbare elektronische Systeme (PES)), wurden zum damaligen Zeitpunkt vor allem zur Ausführung von Nichtsicherheitsfunktionen genutzt. Dies traf auf den Bereich der Anlagentechnik zu, der dieser Norm zugrunde liegt, nicht jedoch auf den Bereich der Automobilindustrie. Hier kamen PES seit vielen Jahren beispielsweise beim Antiblockiersystem oder beim Airbag zum Einsatz.
Laut Aussagen von Carsten Gregorius in [MON 03] war einer der Hauptgründe für die Entwicklung der IEC 61508 die Tatsache, dass es insbesondere für den Einsatz von komplexen elektronischen Systemen keinen international anerkannten Standard gab. Außerdem mangelte es den bestehenden Standards, wie z.B. der EN 954, einer umfassenden Betrachtung der Funktionalen Sicherheit. Die fehlenden Regeln wurden nach [MRL 02] vor allem von der Prozessindustrie (zum Beispiel in den Bereichen Chemie und Verfahrenstechnik) vermisst. Dass die IEC 61508 ihren historischen Hintergrund in der Anlagen- bzw. Verfahrenstechnik hat, spiegelt sich in vielen Einzelregelungen der Norm wider. Diese lassen noch den spezifischen Regelungsbedarf der Verfahrenstechnik erkennen.
Weiteres Bestreben bei der Entwicklung dieser Norm war es laut [MRL 02], zusätzliche sicherheitstechnische Regeln aufzustellen. Mit deren Hilfe sollte Technik, die auf Mikroprozessoren basiert, für Sicherheitsaufgaben eingesetzt und nutzbar gemacht werden. Durch den Einsatz von Rechnern in immer komplexeren Steuerungen wurden nach [WRA 10] neue spezifische technische Regeln dringend benötigt, um ungeeignete und unsichere

Lösungen als solche einfach erkennen zu können. Diese Technologie birgt viele Vorteile, kann aber aufgrund ihrer Komplexität nicht mit den traditionellen Bewertungsmaßstäben der diskreten Elektrik und Elektronik beurteilt werden.

3.2.3 Struktur

Die IEC 61508 umfasst sieben Teile und weit über 500 Seiten: die Teile 1 bis 4 sind normativ, die Teile 5 bis 7 informativ. Die informativen Teile und Anhänge beinhalten Informationen sowie praktische Beispiele, die den Umgang mit der Norm erleichtern sollen, und sind nicht Teil des Normeninhaltes. Wie bereits erwähnt, wird die IEC 61508 auch als Sicherheitsgrundnorm verstanden, wobei dies natürlich nur für die normativen Teile gilt.

Der erste Teil legt die grundsätzlichen Anforderungen fest, die auf alle Teile der Norm anwendbar sind. Alle weiteren Teile behandeln spezifischere Themengebiete.
Die Teile 2 und 3 der Norm enthalten zusätzliche und besondere Anforderungen für sicherheitsbezogene E/E/PE-Systeme (hinsichtlich Hardware und Software). Teil 2 legt beispielsweise fest, wie Sicherheitsanforderungen und ihre Zuordnung auf die sicherheitsbezogenen E/E/PE-Systeme verfeinert und in funktionale Anforderungen umgesetzt werden.
In Teil 4 sind Definitionen und Abkürzungen enthalten, die in der gesamten Norm Anwendung finden.
Hinweise für die Anwendung von Teil 1 zur Festlegung von Sicherheits-Integritätsleveln finden sich in Teil 5 anhand von einigen Beispielen. Darin enthalten sind Informationen zu verschiedenen Risikokonzepten in Abhängigkeit von der auszuführenden Sicherheitsfunktion. Des Weiteren finden sich hier Informationen zum Zusammenhang von Risiko und Sicherheitsintegrität.
Teil 6 liefert Hinweise für die Anwendung der Teile 2 und 3. Darin werden u.a. Verfahren aufgezeigt, mit denen die Wahrscheinlichkeiten von Hardwareausfällen oder die Ausfallwahrscheinlichkeiten infolge von Fehlern gemeinsamer Ursache berechnet werden können.
Im siebten und letzten Teil der Norm ist ein Überblick über verschiedene Sicherheitsverfahren und –maßnahmen für die Anwendung der Teile 2 und 3 enthalten.

In Bild 3-1 ist der Gesamtrahmen des Normenwerkes schematisch dargestellt. Neben dem Gesamtrahmen der Norm ist dort auch eine Anforderungsaufteilung enthalten. Es wird dabei

in technische und andere Anforderungen unterschieden. Anhand der Darstellungsweise der Abbildung ist darüber hinaus eine Reihenfolge für die Umsetzung der Norm ersichtlich.

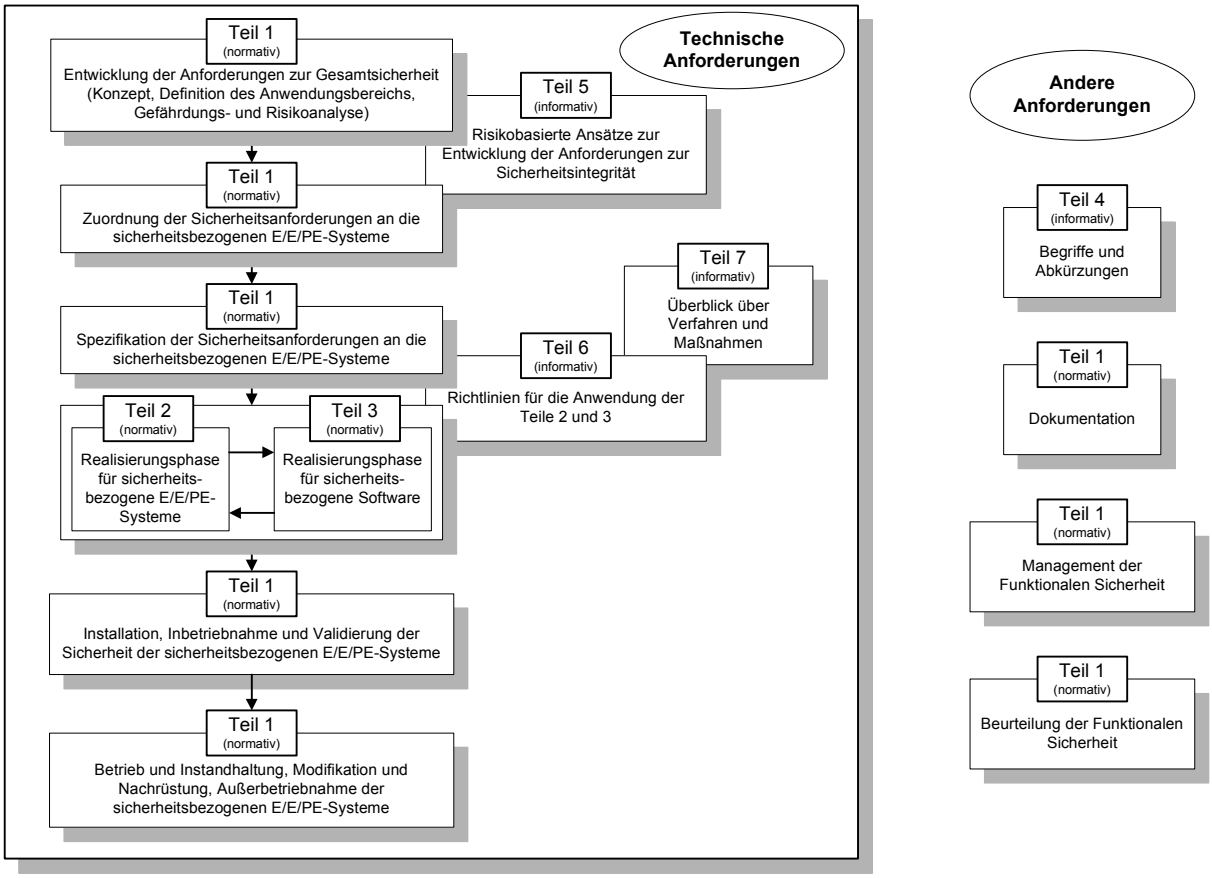


Bild 3-1: Struktur der IEC 61508 nach [DIN 02a]

Zuerst müssen die gesamten Sicherheitsanforderungen entwickelt werden (Konzept, Definition des Anwendungsbereichs, Gefährdungs- und Risikoanalyse). Anschließend erfolgen die Zuordnung und die Spezifikation der Sicherheitsanforderungen an das sicherheitsbezogene E/E/PE-System, bevor die Realisierungsphasen für das System (Hardware) bzw. für die Software betrachtet werden können. Hierbei ist zu beachten, dass die Realisierungsphasen für die Hard- und die Software miteinander verknüpft sind, da die Anwendungsbereiche der entsprechenden Teile der Norm zum Teil ineinander übergehen. Danach folgt die Betriebsphase des sicherheitsbezogenen E/E/PE-Systems. Dazu zählen Installation, Inbetriebnahme, Betrieb, Instandhaltung, Modifikation sowie Außerbetriebnahme. Dies alles stellt den Bereich der technischen Anforderungen dar. Daneben werden eine Reihe von anderen Anforderungen beispielsweise an die Dokumentation, die Beurteilung und das Management der Funktionalen Sicherheit gestellt.

Diese anderen Anforderungen müssen während der gesamten Umsetzung der Norm berücksichtigt werden.

3.2.4 Allgemeines

Die IEC 61508 weitet nach [WRA 10] im Gegensatz zur EN 954 das Prinzip der Risikoreduzierung auf die gesamte Sicherheitsfunktion aus, in der E/E/PE-Systeme eingesetzt werden. Darüber hinaus, und dies ist durchaus als bedeutende Neuerung anzusehen, erhielt mit der IEC 61508 der Probabilismus Einzug bei der Bestimmung von Zuverlässigkeiten, indem hierfür statistische Wahrscheinlichkeiten vorgegeben wurden. In Abschnitt 4.4.4 werden die normativ angegebenen probabilistischen Werte näher betrachtet.

Die Norm betrachtet das Sicherheitsprodukt nicht nur aus der Sicht der Produktentwicklung. Sie verwendet als technischen Rahmen das Modell eines **gesamten Sicherheitslebenszyklus** (GSLZ), um diejenigen Tätigkeiten auf systematische Art und Weise zu behandeln, die für die Gewährleistung der funktionalen Sicherheit der sicherheitsbezogenen E/E/PE-Systeme notwendig sind. Dadurch sollen Aspekte der Zuverlässigkeit und Sicherheit nachvollziehbar geplant und kontrolliert werden können. In folgender Abbildung ist der GSLZ mit den entsprechenden Phasen dargestellt. Der Lebenszyklus begleitet das Produkt sozusagen von der ersten Idee (Phase 1: Konzept) bis hin zu seiner Stilllegung (Phase 16: Außerbetriebnahme oder Ausmusterung).

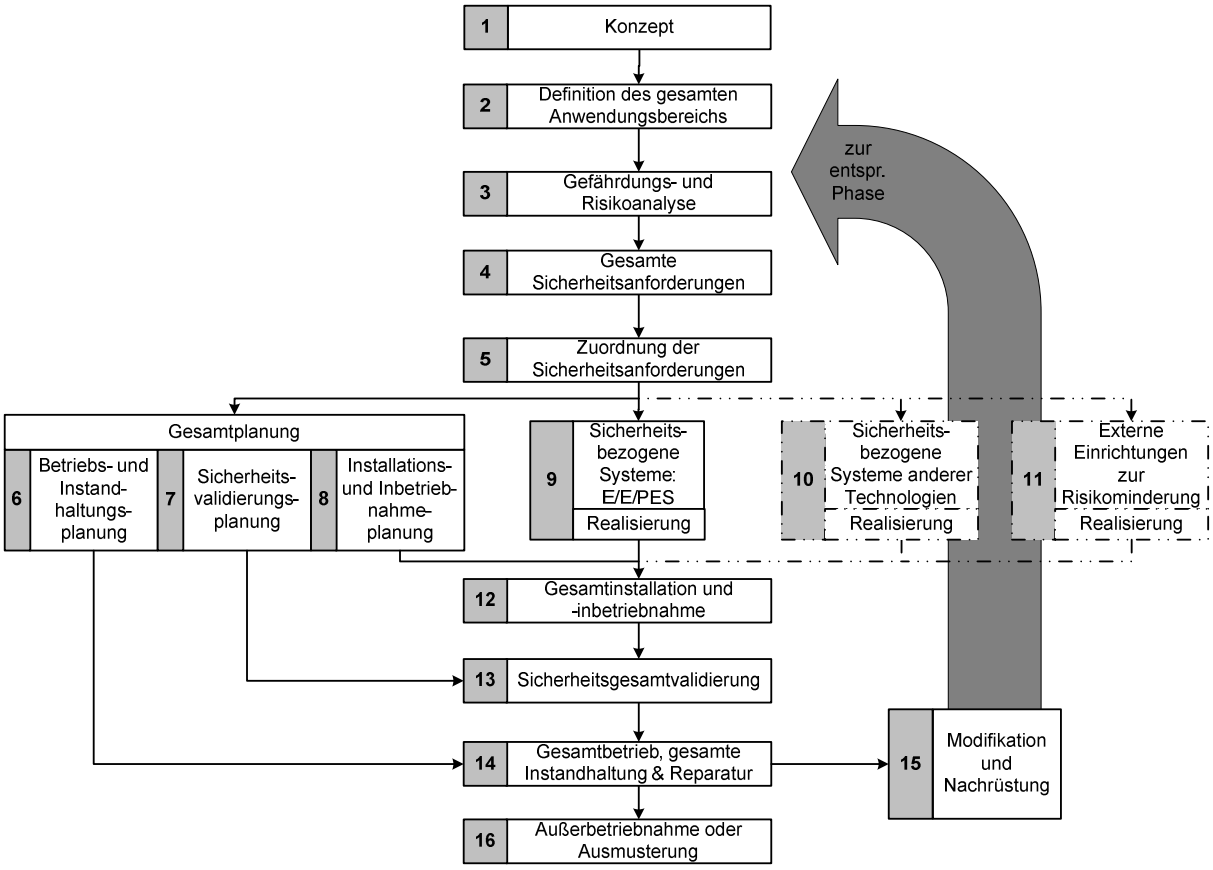


Bild 3-2: Gesamter Sicherheitslebenszyklus nach [DIN 02a]

Bei dem in Bild 3-2 dargestellten GSLZ handelt es sich um eine vereinfachte Betrachtung der Realität. Einzelne Phasen und Zwischenphasen können ggf. iterativ mehrfach durchlaufen werden. Tätigkeiten, die sich auf das Management, die Verifikation und die Beurteilung der Funktionalen Sicherheit beziehen, sind aus darstellungstechnischen Gründen nicht gezeigt. Sie müssen in den jeweiligen Phasen, in denen sie erforderlich sind, berücksichtigt werden. Die in Bild 3-2 gestrichelt dargestellten Phasen 10 und 11 liegen außerhalb des Anwendungsbereiches der Norm.

Für alle Phasen des gesamten Sicherheitslebenszyklus gibt die IEC 61508 Ziele und Anforderungen an, die es zu erreichen bzw. zu erfüllen gilt, um die Funktionale Sicherheit zu gewährleisten. Auf einige dieser Anforderungen und der damit zusammenhängenden Tätigkeiten, die für das weitere Verständnis wichtig sind, wird im Nachfolgenden eingegangen.

In Phase 3 des GSLZ wird die Durchführung einer **Gefährdungs- und Risikoanalyse** anhand realer Anwendungsszenarien gefordert. Ziel hierbei ist es, eine systematische Erfassung der potentiell von dem betrachteten System ausgehenden Gefährdungen durchzuführen, und zwar

in allen Betriebsarten. Diese Bestimmung muss für alle vernünftigerweise vorhersehbaren Umstände, einschließlich Fehlerbedingungen und Fehlanwendungen vollzogen werden.
Darüber hinaus müssen nicht nur die Gefährdungen an sich, sondern auch die Abläufe von Ereignissen bestimmt werden, die zu den erkannten gefährlichen Vorfällen führen können. Des Weiteren sollen im Rahmen der Gefährdungs- und Risikoanalyse die mit den festgelegten gefährlichen Vorfällen verbundenen Risiken sowie deren mögliche Auswirkungen bestimmt werden.
Mit Hilfe einer Risikoanalyse wird also die Sicherheitsrelevanz des betrachteten Systems festgelegt. Dabei müssen alle kritischen Systemzustände und deren Gefahrenpotential ermittelt werden. Für jede kritische Funktion des Systems sind mögliche Fehlfunktionen zu betrachten und entsprechende Parameter zu bestimmen. Mit dieser Vorgehensweise soll eine systematische und risikobasierende Art und Weise der Bestimmung der Sicherheitsanforderungen für die sicherheitsbezogenen E/E/PE-Systeme gewährleistet werden.

In den Anhängen von [DIN 02c] werden neben Informationen zum Zusammenhang von Risiko und Sicherheitsintegrität auch Verfahren (quantitativ und qualitativ) zur Bestimmung der Sicherheits-Integritätslevel dargestellt.
Unter **Sicherheitsintegrität** versteht die Norm die Wahrscheinlichkeit, dass ein sicherheitsbezogenes System die geforderte Sicherheitsfunktion unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraums anforderungsgemäß ausführt [DIN 02b]. Damit wird die Wirksamkeit einer Sicherheitsfunktion eines sicherheitsbezogenen Systems unter anforderungsgemäßen (fehlerfreien) Bedingungen beschrieben. Die Sicherheitsintegrität stellt also die Fähigkeit eines Systems dar, Fehler während des Betriebs zu erkennen und zu behandeln [elp 05]. Sie beinhaltet dabei laut Norm sowohl die Sicherheitsintegrität der Hardware (Teil der Sicherheitsintegrität, der sich auf zufällige Hardwareausfälle mit gefahrbringender Ausfallart bezieht) als auch die systematische Sicherheitsintegrität (Teil der Sicherheitsintegrität, der sich auf systematische Ausfälle mit gefahrbringender Ausfallart bezieht).
Um Sicherheitsfunktionen hinsichtlich ihrer Sicherheitsintegrität einzustufen, werden **Sicherheits-Integritätslevel** (SIL) verwendet. Ein SIL ist definiert als eine von vier diskreten Stufen zur Spezifizierung der Anforderung für die Integrität der Sicherheitsfunktionen, die dem sicherheitsbezogenen E/E/PE-System zugeordnet werden. Dabei stellt der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität dar und der SIL 1 die niedrigste.

Je höher der SIL eines sicherheitsbezogenen Systems ist, desto geringer ist die Wahrscheinlichkeit, dass es die geforderte Sicherheitsfunktion nicht ausführen kann.

Es besteht folglich eine Unterscheidung zwischen Risiko und Sicherheitsintegrität. Das **Risiko**[10] wird allgemein definiert als ein Maß für die Wahrscheinlichkeit und die Auswirkung eines bestimmten gefahrbringenden Vorfalls [DIN 02c]. Die Sicherheitsintegrität ist als Maß für die Wahrscheinlichkeit eines sicherheitsbezogenen Systems anzusehen, die erforderliche Risikominderung in Bezug auf die festgelegte Sicherheitsfunktion zufriedenstellend zu erreichen.
Es ist unbestritten, dass es praktisch nicht möglich ist, gefährliche Situationen komplett zu verhindern. Ein gewisses Risiko wird immer vorhanden sein. Hierbei wird oftmals vom verbleibenden Risiko oder auch Restrisiko gesprochen. Das Wort „Restrisiko“ ist hierbei allerdings ein irreführender Begriff. In diesem Zusammenhang wird oftmals fälschlicherweise davon ausgegangen, dass, wenn ein bestimmtes Restrisiko durch etwaige Sicherheitsvorkehrungen erreicht worden ist, die Möglichkeit eines zukünftigen Schadens praktisch ausgeschlossen ist. Das ist allerdings nicht der Fall, da auch ein Restrisiko immer noch ein Risiko und somit das Gefährdungspotential nicht gleich Null ist.

Ein qualitatives Verfahren zur Ermittlung der Sicherheits-Integritätslevel ist der **Risikograph**. Dabei wird zur Beschreibung der Umstände eine Reihe von Faktoren verwendet, die gemeinsam den Charakter der Gefährdungssituation beschreiben, wenn sicherheitsbezogene Systeme versagen oder nicht vorhanden sind. Die Vorgehensweise basiert auf der allgemeinen Risikodefinition, wonach Risiko als Kombination aus der Auftretenswahrscheinlichkeit einer gefährlichen Situation und der Schwere ihrer Auswirkung beschrieben wird:

$$R = f \cdot C \tag{3-1}$$

mit R: Risiko ohne sicherheitsbezogenes System,

f: Häufigkeit des gefährlichen Vorfalls ohne sicherheitsbezogenes System und

C: Auswirkung des gefährlichen Vorfalls (die Auswirkungen können auf den Schaden, der mit Gesundheit und Sicherheit oder mit Umweltschäden einhergeht, bezogen werden).

[10] Weiterführende Informationen zur Definition, Darstellung und Anwendung des Risikobegriffs sind u.a. in [SFK 04] zu finden. Dort sowie in [BRA 12] wird auch auf die Unterscheidung zwischen Kollektivrisiken (welche eine gesamte Gruppe betreffen) und dem Individualrisiko einer Person eingegangen.

Die Häufigkeit des gefährlichen Vorfalls f setzt sich dabei aus drei Einflussfaktoren zusammen:

- der Häufigkeit und Zeit des Aufenthalts im Gefahrenbereich,
- der Möglichkeit, den gefährlichen Vorfall zu vermeiden und
- der Wahrscheinlichkeit des Auftretens des gefährlichen Vorfalls, ohne das Vorhandensein irgendeines sicherheitsbezogenen Systems – wird als „Wahrscheinlichkeit des unerwünschten Ereignisses“ bezeichnet.

Dies führt zu den folgenden vier **Risikoparametern** für den Risikographen:

- C: Auswirkung des gefährlichen Vorfalls,
- F: Häufigkeit und Zeit des Aufenthalts im Gefahrenbereich,
- P: Möglichkeit, den gefährlichen Vorfall zu vermeiden und
- W: Wahrscheinlichkeit des unerwünschten Ereignisses.

Für jeden dieser Parameter existiert ein Parametersatz, wie nachfolgende tabellarische Übersicht verdeutlicht.

Tabelle 3-1: Klassifizierung der Risikoparameter nach [DIN 02c]

Risikoparameter		Klassifizierung
Auswirkung (C)	C_1	Geringe Verletzung
	C_2	Schwere irreversible Verletzung einer oder mehrerer Personen; Tod einer Person
	C_3	Tod mehrerer Personen
	C_4	Tod sehr vieler Personen
Häufigkeit und Aufenthaltsdauer im gefährlichen Bereich (F)	F_1	Seltener bis häufiger Aufenthalt im gefährlichen Bereich
	F_2	Häufiger bis dauernder Aufenthalt im gefährlichen Bereich
Möglichkeit, den gefährlichen Vorfall zu vermeiden (P)	P_1	Möglich unter bestimmten Bedingungen
	P_2	Beinahe unmöglich

Fortsetzung von Tabelle 3-1

Risikoparameter		Klassifizierung
Wahrscheinlichkeit des unerwünschten Ereignisses (W)	W_1	Eine sehr geringe Wahrscheinlichkeit, dass die unerwünschten Ereignisse auftreten, und nur wenige unerwünschte Ereignisse sind wahrscheinlich.
	W_2	Eine geringe Wahrscheinlichkeit, dass die unerwünschten Ereignisse auftreten, und wenige unerwünschte Ereignisse sind wahrscheinlich.
	W_3	Eine relativ hohe Wahrscheinlichkeit, dass die unerwünschten Ereignisse auftreten, und häufige unerwünschte Ereignisse sind wahrscheinlich.

Die Kombination der zuvor beschriebenen Risikoparameter ermöglicht es, einen Risikographen wie in Bild 3-3 zu entwickeln. Die gezeigte Darstellung ist allerdings nur als Beispiel anzusehen, da es je nach Fall notwendig sein kann, die entsprechenden Parameter und ihre Gewichtungen anzupassen.

Die Verwendung der Risikoparameter C, F und P führt zu einer Anzahl von Ergebnissen $X_1, X_2, ..., X_n$ (die genaue Anzahl hängt von dem vom Risikographen abzudeckenden besonderen Anwendungsgebiet ab – im gezeigten Beispiel sind es acht Ereignisse). Jedes Einzelergebnis ist auf eine von drei Skalen (W_1, W_2 und W_3) abgebildet. Jeder Punkt dieser Skalen stellt einen Anhaltspunkt für die erforderliche Systemintegrität dar, die durch das betrachtete sicherheitsbezogene E/E/PE-System erreicht werden muss.

Durch die Abbildung auf W_1, W_2 oder W_3 wird ein Beitrag anderer Maßnahmen zur Risikominderung berücksichtigt wie beispielsweise durch sicherheitsbezogene Systeme anderer Technologien und externe Einrichtungen zur Risikominderung. Das bedeutet, dass die Skala W_3 für einen kleinsten Beitrag durch andere Maßnahmen zur Risikominderung steht, da die höchste Wahrscheinlichkeit des unerwünschten Ereignisses vorliegt. W_2 steht analog für einen mittleren und W_1 für einen höchsten Beitrag.

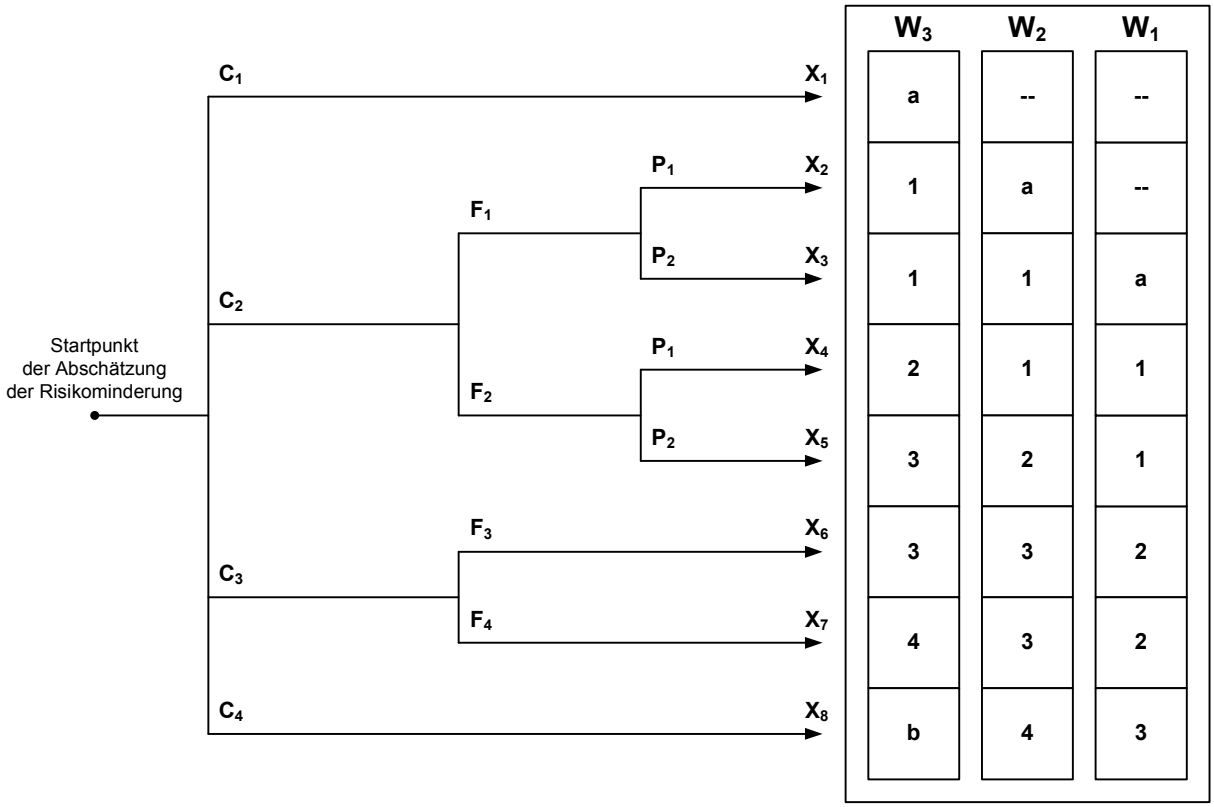


Bild 3-3: Allgemeine Darstellung eines Risikographen (abgeleitet aus [DIN 02c])

Für ein bestimmtes Zwischenergebnis X und ein bestimmtes Maß von W gibt der Risikograph in Bild 3-3 den SIL des sicherheitsbezogenen E/E/PE-Systems an. Dabei gelten folgende Bewertungskriterien:

- --: keine Sicherheitsanforderungen,
- a: keine speziellen Sicherheitsanforderungen,
- b: ein einzelnes E/E/PE-System ist nicht ausreichend und
- 1,2,3,4: Sicherheitsintegritätslevel.

Bezüglich der Vorgehensweise über den Risikographen sind noch einige Anmerkungen zu machen. Die Methode ist zwar sehr einfach und schnell anzuwenden, allerdings ist sie auch nicht präzise. Sie bietet eine Menge Raum für Interpretationen, wenn es um die Definitionen der einzelnen Parametersätze geht. Wo verläuft beispielsweise die Grenze zwischen „seltener bis häufiger Aufenthalt“ und „häufiger bis dauernder Aufenthalt“? Die vorgenommenen Einstufungen können hierbei durchaus subjektiv sein und von Bearbeiter zu Bearbeiter unterschiedlich ausfallen. Hier ist es wichtig, den Risikographen zu kalibrieren und Orientierungshilfen zur Durchführung bereit zu stellen, z.B. in Form von genauen

Beschreibungen der einzelnen Parametereinstufungen. Dies ist u.a. beim automotiven Ansatz berücksichtigt worden (s. Abschnitt 3.3).

Hinsichtlich der Sicherheitsintegrität sind nun Ziele zu formulieren. Dies kann nach [SMI 04] auf zwei Arten geschehen: quantitativ und qualitativ. Bei quantitativen Zielen wird die Häufigkeit von zufälligen Hardwareausfällen prognostiziert und mit Grenzwerten für das tolerierbare Risiko verglichen. Wenn die Zielwerte nicht erreicht werden, muss das Design des Betrachtungsgegenstandes so angepasst werden, dass die Zielanforderungen erfüllt werden. Bei qualitativen Zielen wird versucht, das Auftreten von systematischen Ausfällen durch Maßnahmen zu minimieren. Solche Ausfälle können nicht quantifiziert werden.
Die IEC 61508 fordert nach [E+H 04] als erste Norm einen quantitativen Nachweis für das verbleibende Risiko auf Basis der Berechnung von gefährlichen Versagenswahrscheinlichkeiten. Außerdem änderte sich der Betrachtungswinkel. Zuvor wurden die einzelnen Systemkomponenten separat betrachtet und untersucht. Die neue quantitative Berechnung erfolgt für das komplette Sicherheitssystem, von der Messstelle über die Steuerung bis zum Aktor. Die für alle Einzelkomponenten ermittelten Versagenswahrscheinlichkeiten werden addiert und über die sicherheitstechnische Auswahlschaltung berücksichtigt. Es wurden folglich erstmalig probabilistische Grenzwerte in Abhängigkeit des eingestuften Sicherheits-Integritätslevel eingeführt, die es einzuhalten gilt. Dabei werden die sicherheitsbezogenen Systeme hinsichtlich ihrer Betriebsart in zwei Kategorien eingeteilt. Bei einer „Betriebsart mit niedriger Anforderungsrate“ (engl.: low demand mode) wird an ein System per Definition nicht mehr als eine Anforderung pro Jahr gestellt. Die geforderten Ausfallgrenzwerte bei Anforderung für die einzelnen SIL sind in Tabelle 3-2 enthalten. Bei einer „Betriebsart mit hoher Anforderungsrate oder mit kontinuierlicher Anforderung“ (engl.: high demand or continous mode) werden an das System mehr als eine Anforderung pro Jahr gestellt bzw. das System ist dauernd im Einsatz, um die Sicherheitsfunktion aufrecht zu erhalten. Die geforderten Ausfallgrenzwerte der Wahrscheinlichkeiten eines gefahrbringenden Ausfalls pro Stunde (engl.: Probability of Dangerous Failure per Hour, PFH_D) können ebenfalls Tabelle 3-2 entnommen werden.
Die Begründung für die Unterscheidung in die zwei Betriebsarten lässt sich nach [SMI 04] am besten durch zwei Beispiele erklären. Zunächst soll die Fahrzeugbremse betrachtet werden. Hier ist die Ausfallrate von Interesse, da es eine große Wahrscheinlichkeit gibt, eine Gefährdung zu erleiden, wenn der Ausfall eintritt. Dementsprechend muss hierbei die Betriebsart mit hoher Anforderungsrate gewählt werden. Wenn nun allerdings der Airbag in

einem Fahrzeug betrachtet wird, wird schnell deutlich, dass dieses System eine sehr geringe Anforderungsrate hat. Die Ausfallrate scheint für die Beschreibung der Sicherheitsintegrität nicht das geeignete Maß zu sein. Zweckdienlicher ist hier die Kombination der Ausfallrate und der Ausfallzeit durch die mittlere Ausfallwahrscheinlichkeit bei Anforderung (engl.: Probability of Failure on Demand, PFD).

Tabelle 3-2: Ausfallgrenzwerte für eine Sicherheitsfunktion in Abhängigkeit der Betriebsart nach [DIN 02a]

Sicherheits-Integritätslevel	**Betriebsart mit niedriger Anforderungsrate** (mittlere Ausfallwahrscheinlichkeit der entworfenen Funktion bei Anforderung)	**Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung** (Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde)
4	$\geq 10^{-5} bis < 10^{-4}$	$\geq 10^{-9} bis < 10^{-8}$
3	$\geq 10^{-4} bis < 10^{-3}$	$\geq 10^{-8} bis < 10^{-7}$
2	$\geq 10^{-3} bis < 10^{-2}$	$\geq 10^{-7} bis < 10^{-6}$
1	$\geq 10^{-2} bis < 10^{-1}$	$\geq 10^{-6} bis < 10^{-5}$

Zu den Werten in obiger Tabelle 3-2 ist anzumerken, dass bei der Betriebsart mit hoher oder kontinuierlicher Anforderung mit der Angabe „Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde“ in Wirklichkeit die durchschnittliche Häufigkeit des gefahrbringenden Ausfalls in $[h^{-1}]$ gemeint ist. Diese Inkonsistenz in der Semantik einiger Basisbegrifflichkeiten sowie missverständliche Hinweise zur Interpretation dieser Begriffe können als mögliche Gründe dafür angesehen werden, dass bezüglich der Interpretation dieser Grenzwerte in der Praxis lange Unklarheit herrschte und teilweise immer noch vorliegt [MAS 12]. [SMI 04] beispielsweise interpretiert den Begriff als Rate des gefahrbringenden Ausfalls in $[h^{-1}]$. In [SCH 07a] werden mehrere Interpretationsmöglichkeiten des Begriffs „Wahrscheinlichkeit pro Stunde“ und dessen Anwendung in sicherheitstechnischen Modellierungen aus dem automotiven Umfeld erläutert. Das dortige Ergebnis ist, dass es sich bei der „Wahrscheinlichkeit pro Stunde“ um keinen Wahrscheinlichkeitsbegriff im Sinne von Ausfallwahrscheinlichkeit oder Unverfügbarkeit handelt, sondern um einen Häufigkeitsbegriff. Dafür eignet sich nach [SCH 07a] insbesondere die Ausfalldichte im Gegensatz zur Ausfallrate.

Aber nicht nur hinsichtlich der PFH_D-Werte herrscht Unsicherheit, auch bei dem Verständnis des PFD-Wertes gibt es nach [LAN 07] mehrere Interpretationen, auf die an dieser Stelle aber nicht näher eingegangen werden soll. Des Weiteren ist unklar, warum die Zielwerte in Tabelle 3-2 die gegebenen Größenordnungen haben. Eine Diskussion zu den Größenordnungen der normativ geforderten quantitativen Zielwerte ist in Abschnitt 4.4.4 zu finden. Weitere Hinweise zu Stärken und Schwächen der Norm können [SCH 04] und [MAS 12] entnommen werden.

Ungeachtet der Schwierigkeiten haben sich künftige Standards an den Sicherheits-Integritätsleveln der IEC 61508, deren Einteilung und den gegebenen probabilistischen Zielwerten orientiert und sie teilweise übernommen. Hierauf wird im nächsten Abschnitt eingegangen.

3.2.5 Derivate

Eines der vorrangigen Ziele des applikationsunabhängigen Sicherheitsstandards IEC 61508 ist die Ableitung sektorspezifischer Normen zu ermöglichen, wodurch die wichtigsten Einflussgrößen des jeweiligen Anwendungsgebietes vollständig berücksichtigt sowie dessen besonderen Erfordernissen nachgekommen werden soll. In einigen Anwendungsgebieten sind in den vergangenen Jahren bereits „praxisgerechte“ Ableitungen der IEC 61508 entwickelt worden, wie nachfolgende Abbildung zeigt.

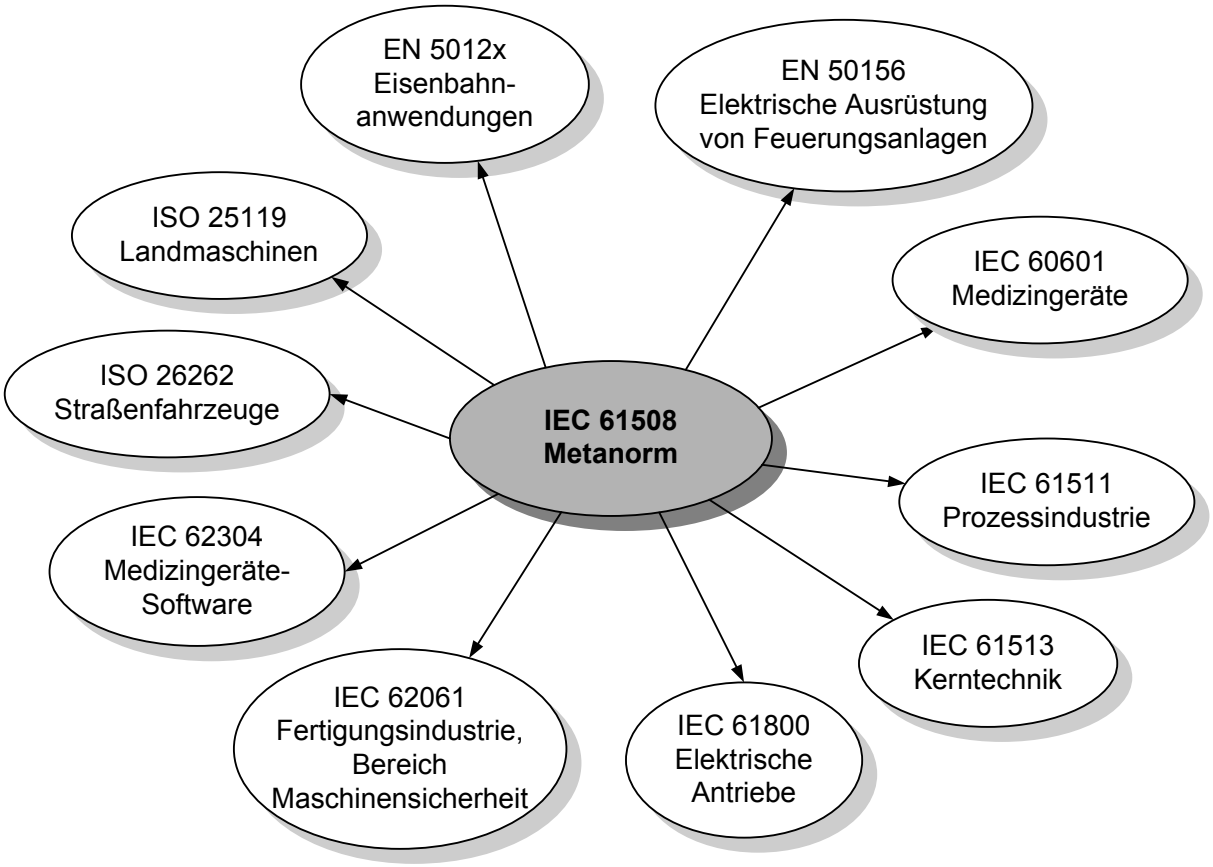


Bild 3-4: Derivate der IEC 61508

Wie in obigem Bild 3-4 zu erkennen, sind schon für einige Industrie- und Anwendungszweige, wie die Medizintechnik, die Fertigungsindustrie, die Kerntechnik oder den Eisenbahnbereich, Ableitungen ausgehend von der generischen Norm entwickelt worden. Obige Abbildung ist nicht vollständig, da es für weitere Bereiche Derivate aus der IEC 61508 gibt, die aus Gründen der Übersichtlichkeit nicht dargestellt wurden. Auch für die Automobilindustrie befindet sich eine sektorspezifische Ableitung in Bearbeitung. Sie ist derzeit als ISO/FDIS 26262 veröffentlicht. Mehr Informationen zu diesem Normenwerk sind in nachfolgendem Abschnitt 3.3 zu finden, der die Funktionale Sicherheit für die Automobilindustrie zum Inhalt hat.

Zuvor sollen allerdings einige der Normen hinsichtlich ihrer Sicherheits-Integritätslevel und der damit zusammenhängenden probabilistischen Zielvorgaben verglichen werden. In Tabelle 3-3 sind hierzu die entsprechenden Werte der folgenden Normen gegenübergestellt:

- IEC 61508,
- IEC 61511: Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie,

- IEC 62061: Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener E/E/PE-Systeme und
- EN 50129: Sicherheitsrelevante elektronische Systeme für Signaltechnik.

Tabelle 3-3: SIL-Gegenüberstellung

SIL	IEC 61508		IEC 61511		IEC 62061	EN 50129
	PFD	PFH_D [1/h]	PFD	PFH_D [1/h]	PFH_D [1/h]	THR [1/h]
1	$10^{-2} \le x < 10^{-1}$	$10^{-6} \le x < 10^{-5}$	$10^{-2} \le x < 10^{-1}$	$10^{-6} \le x < 10^{-5}$	$10^{-6} \le x < 10^{-5}$	$10^{-6} \le x < 10^{-5}$
2	$10^{-3} \le x < 10^{-2}$	$10^{-7} \le x < 10^{-6}$	$10^{-3} \le x < 10^{-2}$	$10^{-7} \le x < 10^{-6}$	$10^{-7} \le x < 10^{-6}$	$10^{-7} \le x < 10^{-6}$
3	$10^{-4} \le x < 10^{-3}$	$10^{-8} \le x < 10^{-7}$	$10^{-4} \le x < 10^{-3}$	$10^{-8} \le x < 10^{-7}$	$10^{-8} \le x < 10^{-7}$	$10^{-8} \le x < 10^{-7}$
4	$10^{-5} \le x < 10^{-4}$	$10^{-9} \le x < 10^{-8}$	$10^{-5} \le x < 10^{-4}$	$10^{-9} \le x < 10^{-8}$	-	$10^{-9} \le x < 10^{-8}$

Wie in obiger Tabelle 3-3 zu erkennen, benutzen alle vier Normen den Terminus Sicherheits-Integritätslevel (SIL) für die Einstufung der Risikobewertung. Darüber hinaus wird deutlich, dass sich einige Anwendungsgebiete, wie die Prozessindustrie, vollständig auf die IEC 61508 beziehen und die quantitativen Werte komplett übernehmen. Andere Branchen, wie die Fertigungsindustrie, nutzen nur einen Teil der Vorgaben der Sicherheitsgrundnorm und/oder haben andere Risikoeinstufungen definiert. Wiederum andere Bereiche, wie die Eisenbahnanwendung, übernehmen zwar das Grundgerüst der Einstufungen, weisen diesen aber ein anderen Begriff zu, der allerdings die gleichen probabilistischen Werte umfasst, wie z.B. die tolerierbare Gefährdungsrate (engl.: Tolerable Hazard Rate, THR) im Gegensatz zu PFH_D.

Andere Derivate definieren mehr als die in de3r IEC 61508 gegebenen Klassifizierungen. Die ISO 25119 für die Sicherheit von Landmaschinen verwendet den Begriff „Agricultural Perfomance Level (AgPL)“. Hier werden fünf solcher Level definiert (von AgPL a bis AgPL e). Diesen werden jedoch keine probabilistischen Grenzwerte im Sinne der IEC 61508 zugeordnet.

Es gibt auch Sicherheitsstandards, die unabhängig von der IEC 61508 entwickelt worden sind. Hierzu zählt z.B die ISO 13849 als zentrale Norm für die Auslegung sicherheitsgerichteter Steuerungen im Bereich Maschinensicherheit, welche die EN 954-1 ersetzen wird. Die ISO 13849 stellt alternativ zur IEC 62061 Vorgaben zur Risikoeinschätzung von E/E/PE-Systemen sowie hydraulischen, pneumatischen und mechanischen Systemen. Sie verwendet

dabei den Begriff „Perfomance Level (PL)“ und weist im Gegensatz zu den vier Sicherheits-Integritätsleveln der IEC 61508 fünf Abstufungen (PL a bis PL e) auf, denen ebenfalls Vorgaben für die PFH_D-Werte zugeordnet werden.
Eine Vorreiterrolle im Bereich der Sicherheitsstandards kommt der Luftfahrtbranche zu. Diese verfügt über keinen eigenen generischen Standard, besitzt allerdings eine Vielzahl von spezifischen Standards und Richtlinien, die unterschiedlichste Aspekte (Entwicklungsprozesse, Betriebskonzepte, Systemdesign, Designanforderungen an Hardware und Software etc.) bzgl. der Sicherheit von Flugzeugen zum Gegenstand haben. Viele dieser Standards wurden weit vor der IEC 61508 verfasst, so dass einige der Luftfahrtnormen teilweise in den Entwicklungsprozess der IEC 61508 einfließen konnten [STÄ 06].

Abschließend bleibt zur IEC 61508 festzuhalten, dass es sich dabei um eine applikationsneutrale generische Richtlinie handelt, welche sehr allgemein gehaltene Anforderungen formuliert und nicht alle Fragen klärt. Sie definiert den zurzeit der Entwicklung bzw. der Aktualisierung gültigen Stand der Technik für Betrachtungen der Funktionalen Sicherheit bei E/E/PE-Systemen. Neu gegenüber früheren Normenwerken ist die Forderung, quantitative Ausfallwahrscheinlichkeiten hinsichtlich der Hardware zu bestimmen und somit den geforderten Sicherheits-Integritätslevel nachzuweisen.

3.3 ISO 26262

Die ISO 26262 stellt die Formulierung eines für die Automobilindustrie tauglichen, handhabbaren und international abgestimmten Sicherheitsstandards als anwendungsspezifische Ableitung der IEC 61508 dar. Nachfolgend werden das Normenwerk vorgestellt sowie wichtige Inhalte und Anforderungen erläutert. Alle Verweise in der vorliegenden Arbeit beziehen sich auf den Stand der ISO/FDIS 26262. Die Norm liegt derzeit nicht in deutscher Sprache vor, so dass eventuelle Übersetzungen in dieser Arbeit als nicht bindend anzusehen sind, da sie vom Autor stammen, wobei diese sich an existierenden Publikationen zu diesem Themenkomplex orientieren. Wichtige Begriffe werden deshalb auch im englischen Original angegeben.

3.3.1 Historie

An der Erstellung des Normenwerks waren weltweit zehn Nationen (u.a. Deutschland, USA, Japan, Großbritannien, Frankreich und Italien) und mehr als 80 Unternehmen aus der Automobil- und der Zulieferindustrie sowie Prüf- und Forschungseinrichtungen beteiligt, wobei europäische und insbesondere deutsche Unternehmen stark vertreten waren. Diese hohe Beteiligung an der Entwicklung der ISO 26262 spiegelt nach [VDA 08] das rege Interesse der internationalen und nationalen Automobilindustrie am Thema Sicherheit von Elektronik wider.

Die ersten Überlegungen bezüglich eines Standards wie der ISO 26262 stammen nach [elp 04] von BMW aus dem Jahre 2002. Im Jahr 2003 haben deutsche Fahrzeughersteller, Lieferanten und Prüforganisationen zusammen die Arbeiten an einem automobilspezifischen Standard zur Funktionalen Sicherheit in einem Arbeitsgremium des FAKRA (Fach-Normenausschuss Kraftfahrzeuge im DIN) aufgenommen. Diese wurden 2005 im Normenausschuss Automobiltechnik unter Führung des Verbandes des Automobilindustrie (VDA) weiterentwickelt. Deutschland war hier folglich federführend, wobei Frankreich kurz darauf hinzugezogen wurde. Diese Arbeiten sind 2005 in die ISO überführt worden. Im Frühjahr 2007 erreichte der Standard die erste weltweite ISO-interne Abstimmung (CD-Umfrage, Committed Draft). Seit Sommer 2009 war die Norm als ISO/DIS 26262 veröffentlicht und damit allgemein zugänglich. Sie war damit aber noch keine verabschiedete ISO-Norm. Vielmehr wurde mit dem Entwurfsstadium eine Umfrage zu den Inhalten der Norm eingeleitet. Die entsprechenden ISO-Mitglieder hatten daher fünf Monate die Möglichkeit, Stellungnahmen abzugeben. Auf Basis dieser wurde im Herbst 2010 von der zuständigen Arbeitsgruppe ein internationaler Schlussentwurf (FDIS, Final Draft International Standard) erstellt, dessen Inhalt durchaus von dem der DIS abweichen kann. Über die Annahme des FDIS entschieden die ISO-Mitglieder in einer Schlussabstimmung im Sommer 2011. Damit waren die inhaltlichen Arbeiten an der Norm abgeschlossen. Die Veröffentlichung der ISO 26262 soll im Herbst 2011 stattfinden.

Aufwandsschätzungen zufolge waren nach Aussagen von Jürgen Sauler, ISO-Experte der Robert Bosch GmbH und Mitglied im zuständigen Normungsgremium, gut 200 Mannjahre für die konkrete Ausgestaltung der Automobilnorm erforderlich [elp 04]. Unter Berücksichtigung der Tatsache, dass in dieser Zahl lediglich der Arbeitsaufwand des

Normungsgremiums enthalten ist und nicht der Aufwand der entsprechenden Zuarbeiten durch weitere Personen, wird deutlich, was für einen Umfang dieses Normenwerk hat.

Der Weg der Entstehung der Norm war mit vielen Kontroversen versehen. Nach [LÖW 10] stieß die ISO/DIS 26262 u.a. in der US-amerikanischen Automobilindustrie auf sehr große Skepsis. Dort gingen firmeninterne Juristen davon aus, dass die Norm bei einem amerikanischen Gerichtsverfahren als nicht zwingend für die Fahrzeugentwicklung angesehen werden könnte. Gleiche Vorbehalte gab und gibt es immer noch hinsichtlich der IEC 61508. Bei dieser ablehnenden Haltung der USA spielten auch firmenpolitische Beweggründe mit. Insbesondere die US-Automobilhersteller kämpften zu der Zeit mit starken Absatzeinbrüchen, so dass sie wenig Interesse zeigten, sich durch ein neues Regelwerk zusätzliche Kostentreiber zu generieren. Darüber hinaus ist die US-Automobilindustrie nicht durch einen starken Export geprägt. Nur verhältnismäßig geringe Stückzahlen der in den USA entwickelten Fahrzeuge wird in den Rest der Welt verkauft. Dadurch reduziert sich nach [LÖW 10] das Risiko der US-Hersteller, z.B. vor einem deutschen Gericht mit der ISO 26262 konfrontiert zu werden.

3.3.2 Rechtliche Stellung

Mit dem Zeitpunkt ihrer Veröffentlichung löst die ISO 26262 als branchenspezifische Ableitung die IEC 61508 als formaljuristisch gültigen Standard für Straßenfahrzeuge ab.

Es kann nach Expertenmeinungen davon ausgegangen werden, dass die ISO 26262 nach ihrer Publizierung mindestens als Stand der Technik anzusehen ist (s. [LÖW 10]), manche gehen sogar vom Stand der Wissenschaft und Technik aus [elp 03]. Somit wird die Norm Relevanz bei Produkthaftungsfragen erlangen. Damit ergibt sich nach [elp 03] für den Hersteller von Verbraucherprodukten (hierzu zählen auch Straßenfahrzeuge) eine Verkehrssicherungspflicht. Danach dürfen nur solche Produkte in Verkehr gebracht werden, welche Sicherheiterwartungen erfüllen, die ein Verbraucher nach dem Stand von Wissenschaft und Technik zum Zeitpunkt des In-Verkehr-Bringens erwarten darf. Zu ihrem Veröffentlichungszeitpunkt trägt eine Norm zum vorhandenen Stand von Wissenschaft und Technik bei. [DIN 07] sagt weiterhin aus, dass ein normatives Dokument zu einem technischen Gegenstand zum Zeitpunkt seiner Annahme als der Ausdruck einer anerkannten Regel der Technik anzusehen sein wird, wenn es in Zusammenarbeit der betroffenen Interessen durch Umfrage- und Konsensverfahren erzielt wurde.

Hierbei ist allerdings festzuhalten, dass die Erfüllung der Norm zwar zwingend notwendig, aber nicht hinreichend ist, um den Stand von Wissenschaft und Technik zu erreichen [elp 03]. Das liegt daran, dass eine Norm ab dem Zeitpunkt ihrer Veröffentlichung ständig veraltet. Schon mit ihrer Veröffentlichung kann sie keinen aktuellen Stand der Technik mehr darstellen, da ihre Inhalte bereits weit vor dem Veröffentlichungstermin festgeschrieben worden sind. Die ISO 26262 stellt folglich einen Mindeststand der Wissenschaft und Technik dar. Es muss daneben weiterhin intensiv der Markt (Veröffentlichungen von Wettbewerbern oder Universitäten, Beiträge auf Tagungen und Kongressen etc.) beobachtet werden hinsichtlich relevanter Entwicklungen beispielsweise bei Methoden.
Eine Nichtbeachtung der normativen Vorgaben und Anforderungen ist allerdings in keinem Fall zu empfehlen. Es könnte beispielsweise bei einem Produkthaftungsfall zu dem Vorwurf kommen, der aufgetretene Schaden sei entstanden, weil das Produkt nicht dem Stand von Wissenschaft und Technik entsprochen hat. Im Rahmen der so genannten Beweislastumkehr ist der Produkthersteller nun gezwungen, das Gegenteil zu beweisen. Bei einer Nichterfüllung der Norm wird dies schwierig bis unmöglich sein.

3.3.3 Motivation und Hintergrund

Die genauen Gründe für die Notwendigkeit der Entwicklung des Standards sind mannigfaltig und können u.a. [ISO 10f], [JUN 08] und [LÖW 10] entnommen werden. An dieser Stelle sollen daher nur einige der Gründe vorgestellt werden.
Da die IEC 61508 aus dem Bereich der Anlagentechnik stammt und u.a. ein eigenes Lebenszyklusmodell verwendet (s. Abschnitt 3.2.4), herrschte große Unsicherheit in der Automobilbranche, wie diese Norm für den Automobilbereich zu interpretieren sei. Das Modell musste zunächst den typischen Phasen der automotiven Entwicklung und des Betriebs angepasst werden. Gleiches galt für einige der in dem Sicherheitslebenszyklus enthaltenen Kernprozesse, wie z.B. die Gefährdungsanalyse und Risikobewertung, welche an die Gegebenheiten des Automobilsektors angeglichen werden mussten. Ohne die ISO 26262 wäre der Stand der Technik in der Automobilbranche unklar geblieben.
Der Grundgedanke der IEC 61508 besteht darin, dass sich die normative Anwendung auf die Entwicklung, Inbetriebnahme und Nutzung eines EUC richtet, also z.B. einer chemischen Anlage. Die Norm geht nach [elp 02] also implizit davon aus, dass diese Anlagen Einzelstücke oder Miniserien sind. In der Automobilindustrie ist hingegen die Massenfertigung der Standard. Speziell Personenkraftwagen werden nicht nur einmal

installiert und betrieben, sondern in sehr großer Stückzahl produziert. Dies erfordert andere Anforderungen an die Produktion als in der IEC 61508 vorgegeben.
Beim oben angesprochenen EUC wird in der IEC 61508 von einem separaten Steuerungs- und Kontrollsystem ausgegangen. Dabei sind enthaltene Sicherheitsfunktionen entweder im Steuerungssystem integriert oder separat umgesetzt. Die potenziellen sicherheitskritischen Fehlfunktionen einer chemischen Anlage werden durch externe Sicherheitsmechanismen, wie z.B. Überdruckventile, reduziert. Die Sicherheit eines Straßenfahrzeugs hängt dagegen von der korrekten Ausführung der E/E-Systeme selbst ab. Die Sicherheit muss folglich in das System hineinentwickelt werden.
Weiterhin wird in der Sicherheitsgrundnorm implizit davon ausgegangen, dass das betrachtete System von einer Organisation entworfen und implementiert wird. Im Automobilbereich herrscht oftmals eine verteilte Entwicklung und Konstruktion von Systemen, bei der teilweise mehrere Zulieferer mit einem Hersteller (OEM, Original Equipment Manufacturer) zusammenarbeiten. Die ISO 26262 enthält folglich spezifische Anforderungen, um solche Entwicklungsprozesse zwischen multiplen Unternehmen zu managen und bei solchen Entwicklungspartnerschaften Hilfestellung zu leisten.

Anhand dieser wenigen Beispiele wird nochmals deutlich, dass nur ein eigener, den speziellen Bedürfnissen und spezifischen Anforderungen der Automobilindustrie angepasster Standard eine angemessene Beachtung der besonderen Bedingungen des Einsatzfeldes von Fahrzeugen gewährleisten kann.

3.3.4 Geltungsbereich

Der Standard ist für die Anwendung bei sicherheitsrelevanten E/E-Systemen in serienproduzierten Personenkraftwagen mit einem Gesamtgewicht von bis zu 3.500 kg vorgesehen. Unter Personenkraftwagen versteht die Norm Fahrzeuge, welche primär zum Transport von Personen einschließlich ihres Gepäcks und ihrer Waren konstruiert worden sind und neben dem Fahrersitz nicht mehr als acht Sitzplätze und keine Stehplätze haben. Ursprünglich sollte die Norm für alle Straßenfahrzeuge gelten, ihr Anwendungsbereich wurde allerdings eingeengt. Daraus resultiert, dass die ISO 26262 beispielsweise Nutzfahrzeuge, Lastkraftwagen, Busse oder Motorräder nicht explizit adressiert, so dass die hierfür formal gültige Norm weiterhin der generische Standard IEC 61508 ist. Bei fahrzeugübergreifenden Entwicklungen hat dies nach [elp 03] zur Folge, dass diese Anforderungen aus mehreren Sicherheitsstandards erfüllen müssen. Allerdings verbietet die Norm an keiner Stelle, dass der

Geltungsbereich nicht auf weitere Fahrzeugklassen erweitert werden darf. Somit ist folglich eine grundsätzliche Anwendung der Norm für alle Straßenfahrzeuge möglich [KLA 11]. Nach [REI 11b] ist für das Jahr 2014 eine Erweiterung der ISO 26262 für die Anwendung bei Lastkraftwagen geplant.

3.3.5 Struktur

Die ISO 26262 besteht aus insgesamt zehn Bänden, welche die Funktionale Sicherheit von elektrischen und elektronischen Systemen beschreibt. Band 10 hat lediglich informativen Charakter und enthält somit keine normativen Vorgaben. In den Bänden 2 bis 9 werden Anforderungen sowohl an den Entwicklungsprozess als auch an das eigentliche Produkt gestellt. Die dabei verwendeten Begriffe werden in Band 1 definiert. Im zehnten Teil der Norm wird ein informativer Leitfaden für die Anwendung der Richtlinie präsentiert. Der Aufbau der Bände gliedert sich wie folgt:

- Band 1: Begriffe,
- Band 2: Management der Funktionalen Sicherheit,
- Band 3: Konzeptphase,
- Band 4: Produktentwicklung – Systemebene,
- Band 5: Produktentwicklung – Hardware-Ebene,
- Band 6: Produktentwicklung – Software-Ebene,
- Band 7: Produktion und Betrieb,
- Band 8: Unterstützende Prozesse,
- Band 9: ASIL- und sicherheitsorientierte Analysen,
- Band 10: Leitfaden zur ISO 26262.

In nachfolgendem Bild 3-5 ist die gesamte Struktur des automotiven Normenwerkes dargestellt. Darin ist zu erkennen, dass der Standard auf dem bekannten V-Modell basiert, welches ein Referenzprozessmodell der verschiedenen Phasen der Produktentwicklung ist. Die schattiert dargestellten „V“s in Bild 3-5 repräsentieren die entsprechenden Querverbindungen zwischen den Teilen 3 bis 7 sowie innerhalb der Bände 5 und 6 der Norm. Diese fünf Phasen umfassen die Kernprozesse des Standards. Bei den angegebenen Nummern in Bild 3-5 steht die erste für den jeweiligen Band und die zweite für den entsprechenden Paragraphen.

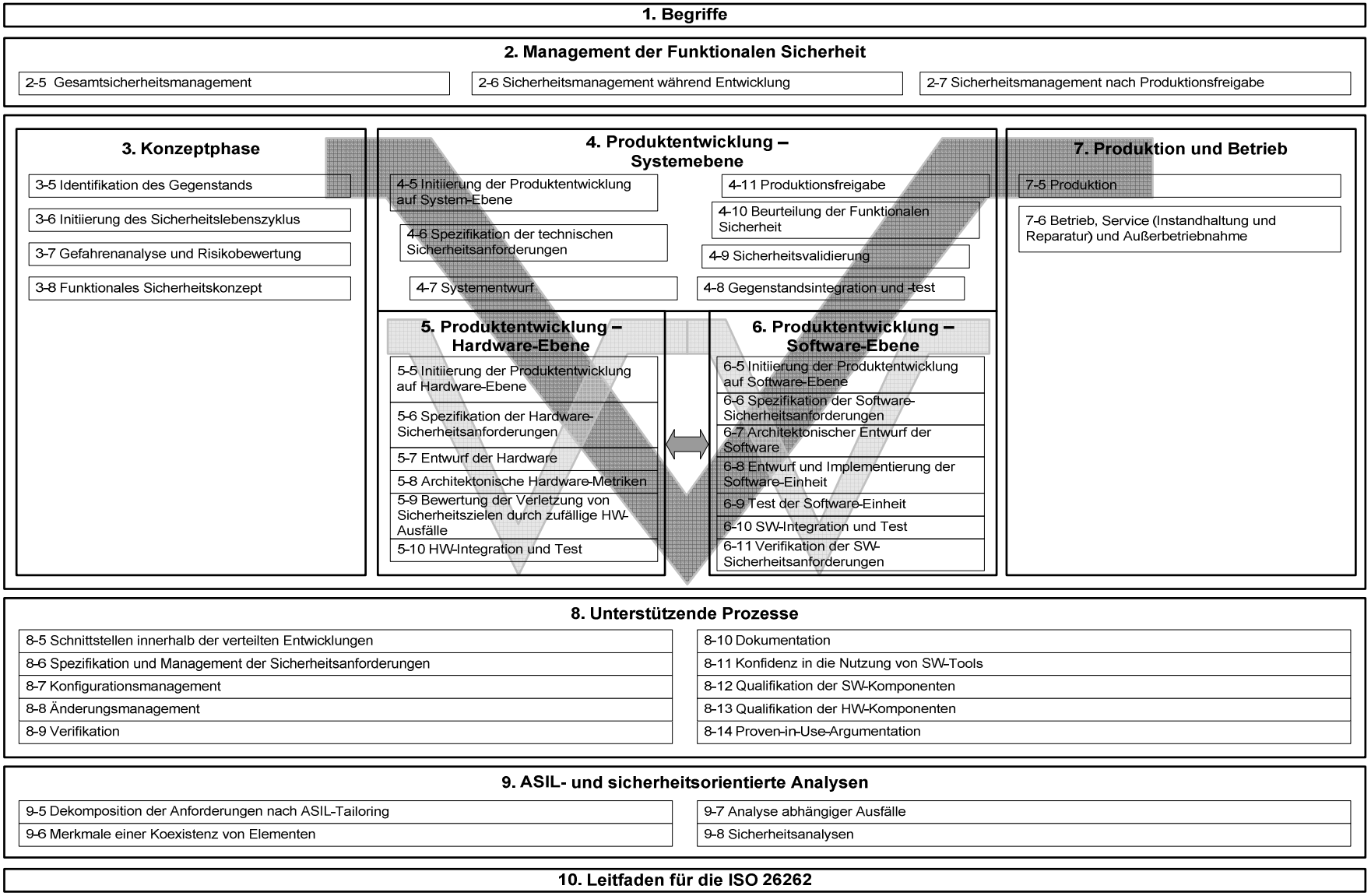


Bild 3-5: Überblick über ISO 26262 nach [ISO 10a]

Der Band 2 befasst sich mit dem Management der Funktionalen Sicherheit, wobei u.a. Anforderungen an die Organisation des Projektmanagements und an die Absicherungsmaßnahmen (Functional Safety Audit und Functional Safety Assessment) zum Nachweis der Normenkonformität gestellt werden.

In den Bänden 3 bis 7 wird der eigentliche Produktlebenszyklus behandelt, der durch einen Sicherheitslebenszyklus in verschiedene Phasen von der Produktentwicklung auf System-, Hardware- und Softwareebene bis hin zur Produktion, Betrieb und Außerbetriebnahme aufgeteilt und strukturiert wird (s. auch folgendes Bild 3-6). Die einzelnen Phasen der Entwicklung sind dabei nach [LÖW 10] grundsätzlich in drei Abschnitte aufgeteilt:

- Planung der Aktivitäten,
- Durchführung der Aktivitäten und
- Verifikation bzw. Validation der Arbeitsprodukte.

Die ISO 26262 verwendet, genau wie der generische Sicherheitsstandard IEC 61508, ein Lebenszyklusmodell als Rahmen, um diejenigen Tätigkeiten auf systematische Art und Weise zu erfassen, die notwendig sind, um die Funktionale Sicherheit von sicherheitsbezogenen E/E-Systemen zu gewährleisten. Dieser automotive Sicherheitslebenszyklus begleitet das System sozusagen von der ersten Idee bis hin zu seiner Entsorgung (siehe Bild 3-6).

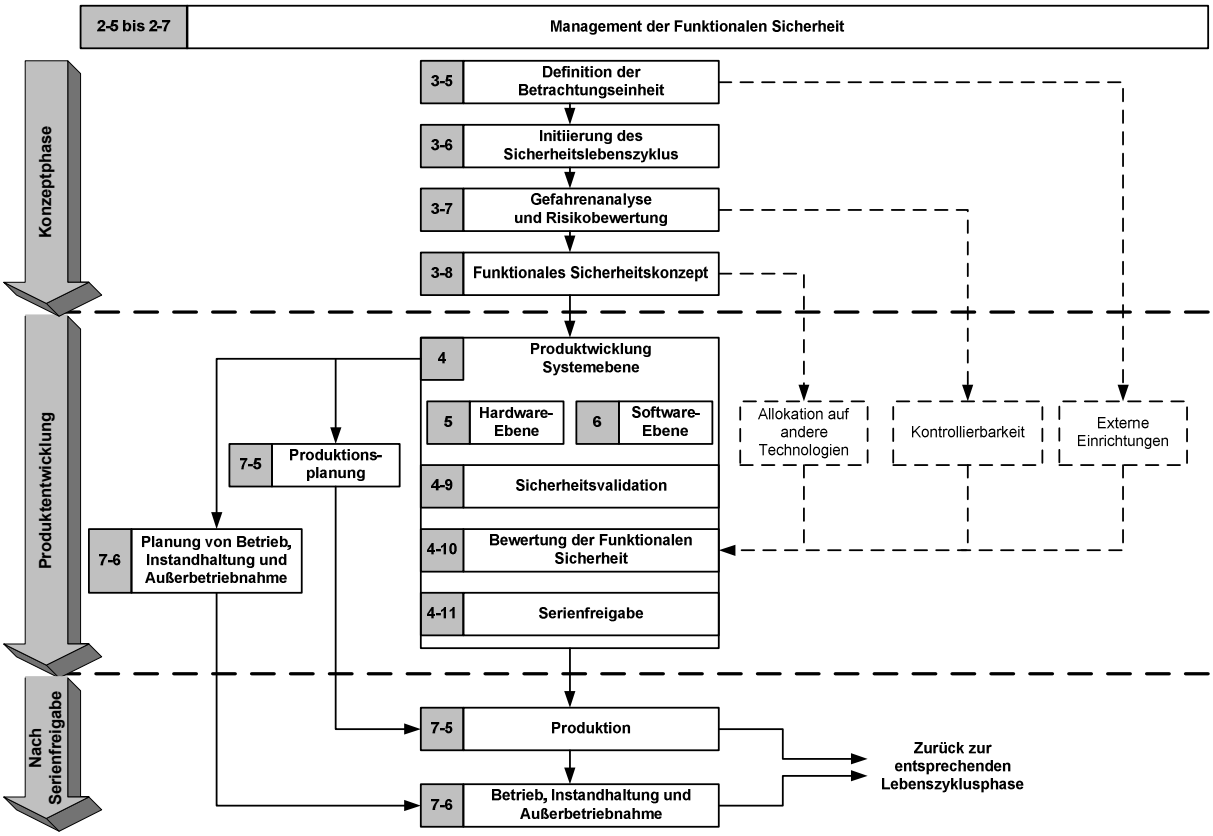


Bild 3-6: Automotiver Sicherheitslebenszyklus nach [ISO 10b]

Der oben dargestellte Sicherheitslebenszyklus ist aufgeteilt in die erforderlichen Aktivitäten während der Konzeptphase, während der Produktentwicklung und nach der Serienfreigabe. Tätigkeiten des Managements der Funktionalen Sicherheit sind während aller Phasen des Zyklus erforderlich. Bei den angegebenen Nummern in Bild 3-6 steht die erste wiederum für den jeweiligen Band und die zweite für den entsprechenden Paragraphen.

Band 3 der ISO 26262 umschreibt die Konzeptphase mit der initialen Definition des Betrachtungsgegenstands (Item; meist ein System) und dessen anschließender Gefahrenanalyse und Risikobewertung. Als Ergebnis dieser werden Sicherheitsziele abgeleitet, denen jeweils ein automotiver Sicherheits-Integritätlevel zugeordnet wird. Die Konzeptphase wird mit der Erstellung des Funktionalen Sicherheitskonzepts (FSK) beendet.
Das FSK wird während der Systementwicklung (Band 4) zum Technischen Sicherheitskonzept (TSK) verfeinert. Vereinfacht kann nach [LÖW 10] das FSK als eine Sicht von außen auf das System und das TSK als eine Innensicht des Systems angesehen werden. Das Technische Sicherheitskonzept wird anschließend noch genauer betrachtet, indem Anforderungen sowohl an den Bereich der Hardware (Band 5) als auch an die Software (Band 6) abgeleitet und spezifiziert werden. Die notwendige Systemintegration sowie die

Phasen bis zur Produktfreigabe sind wiederum in Band 4 beschrieben. Der Band 7 der Norm umfasst Anforderungen an die Produktion, den Betrieb, den Service sowie die Außerbetriebnahme.
In Band 8 werden neben den unterstützenden Prozessen (hierzu zählen u.a. das Konfigurations- und das Anforderungsmanagement) auch Anforderungen an die Dokumentation, neue Methoden wie die Qualifizierung von Tools und eine Möglichkeit des Betriebsbewährtheitsnachweises beschrieben.
Band 9 beinhaltet Angaben zu speziellen sicherheitsorientierten Methoden, wie beispielsweise der Dekomposition der Sicherheits-Integritätslevel oder der Analyse von abhängigen Ausfällen, sowie Anforderungen an Sicherheitsanalysen.

Ziel des Standards ist nach [VDA 08] die Gewährleistung des bisherigen hohen Sicherheitsniveaus von Straßenfahrzeugen für den Endkunden, auch wenn es zu einem verstärkten Einsatz von Elektronik in den Fahrzeugen kommt.

Nachfolgend wird auf einige wichtige Phasen des Sicherheitslebenszyklus und die damit zusammenhängenden Tätigkeiten insbesondere aus der Konzeptentwicklung eingegangen.

3.3.6 Die Gefahrenanalyse und Risikobewertung

Die Durchführung einer Gefahrenanalyse und Risikobewertung (G+R, original: Hazard Analysis and Risk Assessment) - manche Autoren sprechen hierbei auch von einer „Gefährdungsanalyse und Risikoeinschätzung“ oder schlicht „Risikoanalyse“ - wird in der ISO 26262 gefordert und ist ein wesentlicher Schritt des automotiven Sicherheitslebenszyklus. Die dabei vorgeschlagene Vorgehensweise baut auf den Prinzipien der qualitativen Methode des Risikographen auf, der auch in der IEC 61508 beschrieben wird (s. Abschnitt 3.2.4). Im Gegensatz zur Sicherheitsgrundnorm wird in der Automobilnorm allerdings eine Methode spezifiziert, die für die Analyse benutzt werden soll. Die G+R ist deswegen so wichtig, da auf den darin erzielten Ergebnissen und Erkenntnissen alle weiteren sicherheitsbezogenen Aktivitäten basieren. Am Ende muss nach [LÖW 10] feststehen, welche Risiken vom Betrachtungsgegenstand ausgehen werden. Ein solcher kann hierbei ein einzelnes System, ein Systemverbund oder auch eine oder mehrere Funktionen sein. Nachfolgend wird, sofern nicht anders angegeben, der Einfachheit halber angenommen, dass es sich bei dem Betrachtungsgegenstand um ein System handelt. In [SCH 06], [SCH 07b], [LÖW 10] und [STÄ 10] sind weiterführende Informationen zur Risikoanalyse zu finden.

Bei der in der ISO 26262 vorgeschlagenen Vorgehensweise zur G+R handelt es sich um eine qualitative Analysemethode, die auf die Bedürfnisse des Automobilbereichs zugeschnitten ist. Nach [LÖW 10] umfasst der prinzipielle Ablauf der Gefahrenanalyse und Risikobewertung sechs Schritte, die in nachfolgender Abbildung dargestellt sind.

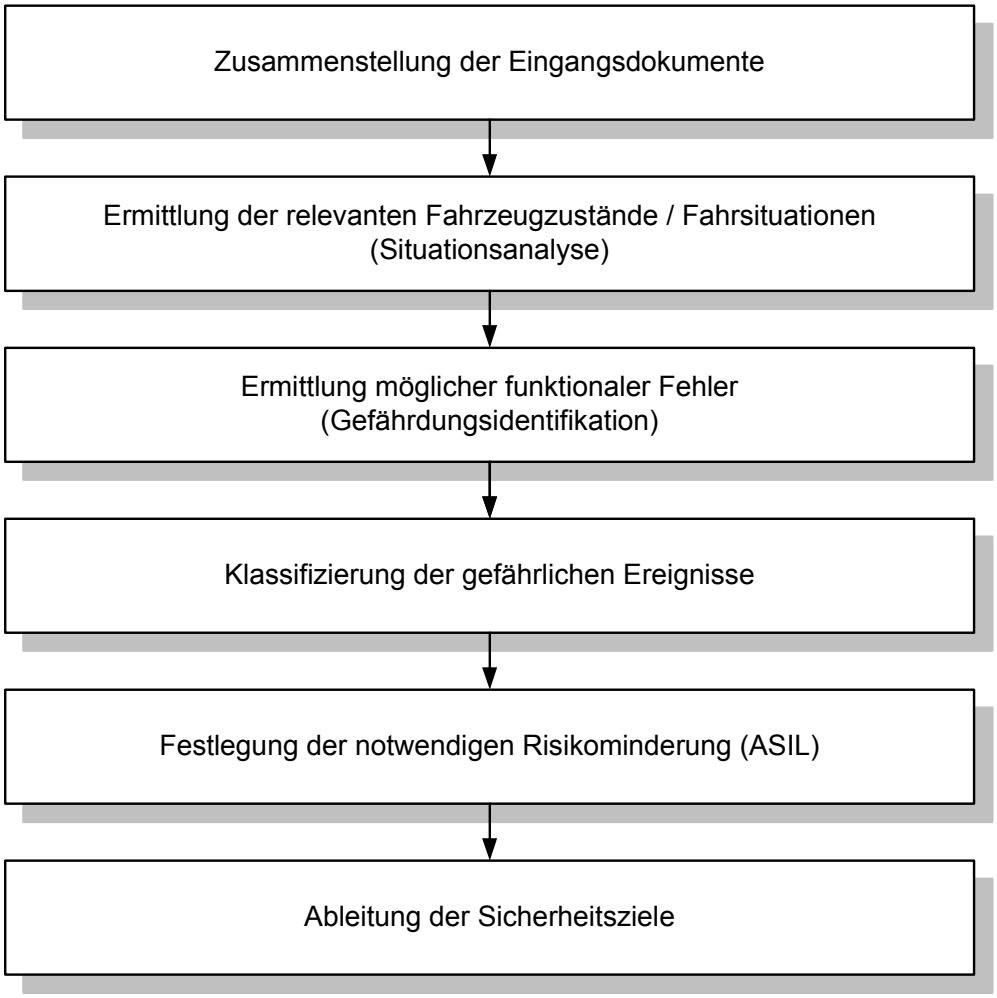


Bild 3-7: Prinzipieller Ablauf einer G+R nach [LÖW 10]

Bevor das betrachtete technische System analysiert werden kann, ist in einem ersten Schritt das System zu definieren und zu beschreiben. Es sind u.a. die Systemgrenzen, die Schnittstellen sowie die relevanten sicherheitsbezogenen Funktionen aufzuzeigen. Zu den benötigten **Eingangsdokumenten** zählen nach [LÖW 10] weiterhin:

- Definition des gesamten Anwendungsbereichs (relevante Fahrzeuge, Varianten, Länder etc.),
- Verzeichnis der bereits bekannten Gefährdungen (z.B. aus Vorgängerprodukten oder -serien),

- Liste der Einsatzarten (z.B. Normalbetrieb),
- Katalog möglicher Fehlfunktionen und
- Verzeichnis möglicher Fehlbedienungen (beabsichtigt und unbeabsichtigt).

In einem zweiten Schritt erfolgt die **Situationsanalyse**. Dabei gilt es, alle relevanten Fahrsituationen und Fahrzeugzustände zu erfassen. Dabei sollen insbesondere solche Situationen berücksichtigt werden, denen ein Gefährdungspotential zugeordnet werden kann. Diese Fahrsituationen sind anschließend Untersuchungsgegenstand in der G+R. Bei der Beschreibung sollte darauf geachtet werden, dass sie u.a. solche Kriterien wie

- den Fahrzeug- und Betriebszustand (z.B. Fahrzeuggeschwindigkeit, Fahrmanöver),
- die Straßenbeschaffenheit (z.B. Art der Straße wie Landstraße oder Autobahn, Nässe oder Dreck durch vorhandene Straßenbaustelle) und
- die Umgebungsbedingungen (z.B. andere Verkehrsteilnehmer, vorhandene Infrastruktur wie Bäume oder Häuser, Sichtverhältnisse durch Nebel, Tunnelfahrt) umfasst.

Darüber hinaus sollte eine Sammlung möglicher Unfallszenarien erstellt werden, wobei u.a. auf die Art des Unfalls (z.B. Auffahrunfall, Frontalcrash, Seitencrash, Fußgängerunfall, Unfall mit Infrastruktur) und auf die dabei auftretenden Geschwindigkeiten eingegangen wird. Alle oben genannten Beschreibungen sollen so genau wie möglich und so umfassend wie nötig verfasst werden, so dass die Darlegungen nicht mit unnötigen Informationen belastet werden.

Im nächsten Schritt folgt die **Gefährdungsidentifikation**, in welcher mögliche funktionale Fehler des betrachteten Systems in Verbindung mit den relevanten Betriebssituationen ermittelt werden. Hierbei können bekannte Techniken und Methoden wie Brainstorming, Checklisten oder auch Fehler-Möglichkeits- und Einflussanalysen (FMEA) zum Einsatz kommen. Dabei erfolgt keine Analyse der Ursachen für diese Fehler. Beispiele für den Inhalt eines solchen Katalogs in Bezug auf ein Abblendlicht sind

- Abblendlicht schaltet ungewollt ein,
- Abblendlicht schaltet ungewollt ab,
- Abblendlicht flackert,
- Abblendlicht leuchtet zu schwach,
- Abblendlicht leuchtet zu stark,
- Abblendlicht schaltet auf Anforderung nicht ein oder

- Abblendlicht schaltet auf Anforderung nicht ab.

Das Ziel der Situationsanalyse und der Gefährdungsidentifikation besteht in der Ermittlung des unerwünschten Verhaltens des Betrachtungsgegenstands, welches zu einem gefährlichen Ereignis führen kann.

In Schritt 4 folgt die **Klassifizierung der gefährlichen Ereignisse** bzw. die Bewertung der Risiken jeder Gefährdungssituation. Die Risikobewertung basiert wiederum auf der allgemeinen Risikodefinition (s. Formel 3-1). Der automotive Ansatz definiert in [ISO 10c] das Risiko als eine Funktion F der Auftretenshäufigkeit eines gefährlichen Ereignisses, der Fähigkeit der Abwehr eines spezifischen Schadens oder einer Gefahr durch rechtzeitige Reaktionen der involvierten Personen und des potentiellen Schweregrades des resultierenden Schadens oder der Gefahr:

$$R = F(f, C, S) \tag{3-2}$$

mit R: Risiko,

f: Auftretenshäufigkeit eines gefährlichen Ereignisses (original: Frequency of Occurrence),

C: Möglichkeit der Gefahrenabwehr (original: Controllability) und

S: Schadensausmaß (original: Severity).

Die Auftretenshäufigkeit eines gefährlichen Ereignisses wird wiederum von mehreren Faktoren beeinflusst. Ein Faktor ist die Berücksichtigung wie oft und wie lange sich Personen in einer Situation befinden und ihr ausgesetzt sind, in der ein zuvor beschriebenes gefährliches Ereignis eintreten kann. Die ISO 26262 vereinfacht diese Fragestellungen zu einem Maß für die Wahrscheinlichkeit einer Fahrsituation, in der das gefährliche Ereignis eintreten kann. Ein weiterer Faktor stellt die Ausfallrate des Systems selbst dar, dessen Fehler/Ausfall zu dem gefährlichen Ereignis führen kann. Dies führt zu folgendem Zusammenhang nach [ISO 10c]:

$$f = E \times \lambda \tag{3-3}$$

mit f: Auftretenshäufigkeit eines gefährlichen Ereignisses (original: Frequency of Occurrence),

E: Wahrscheinlichkeit der Exposition (original: Exposure) und

λ: Ausfallrate des Betrachtungsgegenstands

(bei dem Operator $\times$ handelt es sich um ein Multiplikationszeichen und nicht – wie üblich – um ein Kreuzprodukt).

Die Ausfallrate des Betrachtungsgegenstands wird jedoch bei der Risikobewertung apriorisch nicht berücksichtigt, da ein unzumutbares verbleibendes Risiko durch die Implementierung der Sicherheitsanforderungen vermieden wird, die als Konsequenz der Ergebnisse der Risikobewertung abgeleitet werden.

Den zuvor genannten Risikoparametern S, C und E werden in der Norm jeweils Parametereinstufungen zugeordnet, die eine Festlegung erleichtern sollen. Nachfolgend wird auf diese Parameterklassifizierung genauer eingegangen.

Die Risikobeurteilung legt ihren Fokus auf den möglichen Personenschaden. Um eine Vergleichbarkeit der zu bewertenden Risiken zu gewährleisten, muss in der Beschreibung der potentiellen Schäden eine Kategorisierung vorgenommen werden. Die Bewertung des potentiellen Schadensausmaßes *S* erfolgt anhand von vier Kategorien, die in folgender Tabelle aufgelistet sind.

Tabelle 3-4: Einstufung des Schadensausmaßes (S) nach [ISO 10c]

Stufe	Beschreibung	Referenz für Einzelverletzungen
S0	Keine Verletzungen	AIS 0 und weniger als 10% Wahrscheinlichkeit für AIS 1-6
S1	Leichte und mäßige Verletzungen	Mehr als 10% Wahrscheinlichkeit für AIS 1-6 (und nicht S2 oder S3)
S2	Schwere bis lebensgefährliche Verletzungen (Überleben wahrscheinlich)	Mehr als 10% Wahrscheinlichkeit für AIS 3-6 (und nicht S3)
S3	Lebensgefährliche Verletzungen (Überleben ungewiss)	Mehr als 10% Wahrscheinlichkeit für AIS 5-6

Die in obiger Tabelle 3-4 zu erkennende Einteilung wird durch die Referenz der Abbreviated Injury Scale (AIS) unterstützt. Diese Bewertungsskala wurde Ende der 1960er Jahre von der amerikanischen automobilen Unfallforschung eingeführt, um die Schwere von Einzelverletzungen am menschlichen Körper standardisiert beurteilen zu können. Die

Einstufung erfolgt dabei in mehrere Verletzungsschweregrade (z.B. AIS 0 bis AIS 6). Beispielhafte Verletzungen für die Kategorien S1 bis S3 sind Muskelschmerzen oder Schleudertrauma für S1, Schädelfrakturen ohne Gehirnverletzungen für S2 sowie ein Darm- oder Herzriss für S3. Weiterführende Informationen zur AIS können u.a. [HAA 10] oder [wik 01] entnommen werden.

Bei der Zuordnung der Personenschäden zu den drei Einstufungen S1 bis S3 des Schadensausmaßes wird nicht unterschieden, ob es sich dabei um Verletzungen an dem Fahrer, möglichen Beifahrern oder anderen Verkehrsteilnehmern wie Fahrradfahrern, Fußgängern oder Insassen anderer Fahrzeuge handelt. Kann ausgeschlossen werden, dass es zu einem Personschaden kommt, findet eine Einstufung in die Kategorie S0 statt. Dort werden Schäden aufgenommen, die als nicht sicherheitskritisch anzusehen sind wie etwa Sachschäden durch Rempler mit der Infrastruktur wie Zäune oder Begrenzungspfähle oder auch das Abkommen von der Fahrbahn ohne Kollision oder Überschlag. Bei einer Zuweisung zu der Schadensklasse S0 muss keine weitere Risikobeurteilung durchgeführt werden.

Die in Tabelle 3-4 angegebenen Referenzen sind als mögliche Kriterien anzusehen, da die Norm die Verwendung anderer Kategorisierungen für die Verletzungsschwere nicht untersagt.

In einem weiteren Schritt wird die Einstufung der Beherrschbarkeit (Parameter C) mit Hilfe von vier Kategorien durchgeführt (siehe Tabelle 3-5).

Tabelle 3-5: Einstufung der Beherrschbarkeit (C)

Stufe	Beschreibung	Definition
C0	Im Allgemeinen beherrschbar	-
C1	Einfach beherrschbar	99% oder mehr aller Fahrer oder anderer Verkehrsteilnehmer sind normalerweise imstande, den Schaden abzuwenden.
C2	Normalerweise beherrschbar	90% oder mehr aller Fahrer oder anderer Verkehrsteilnehmer sind normalerweise imstande, den Schaden abzuwenden.
C3	Schwer oder nicht beherrschbar	Weniger als 90% aller Fahrer oder anderer Verkehrsteilnehmer sind normalerweise imstande, den Schaden abzuwenden.

Die Beurteilung einer möglichen Gefahrenabwehr ist eng verbunden mit der Abschätzung der Wahrscheinlichkeit, dass der Fahrzeugführer oder andere Verkehrsteilnehmer die zu entstehen drohende Gefährdungssituation beherrschen und abwenden können. Ein in vernünftiger Weise vorhersehbarer Missbrauch durch den Fahrer muss bei der Einstufung berücksichtigt werden. Außerdem muss dabei beachtet werden, dass die involvierte Person sich nicht mit der Funktionsweise des Betrachtungsgegenstandes auskennt.
Dabei wird der Fahrer dadurch charakterisiert, dass er

- in einer geeigneten Verfassung zum Fahren ist (also z.B. nicht übermüdet ist),
- eine gültige Fahrerlaubnis besitzt und
- die gesetzlichen Vorschriften befolgt.

Einstufungsbeispiele für C0 sind nach der Norm Situationen, die als ablenkend eingestuft werden, wie das Erschrecken durch ein plötzlich lautes Radio oder die Reserve-Warnleuchte für den Kraftstoffvorrat. Weiterhin wird auch die Unverfügbarkeit eines Fahrerassistenzsystems mit C0 bewertet, sofern davon die weitere sichere Fahrzeugnutzung nicht beeinträchtigt wird. Als „einfach beherrschbar“ wird z.B. die Sitzverstellung während der Fahrt oder ein blockiertes Lenkrad beim Fahrzeugstart angesehen. Der Ausfall des ABS während einer ABS-geregelten Bremsung oder ein Motorausfall bei einer hohen Lateralbeschleunigung wird als C2 angesehen. Schwer bis gar nicht beherrschbar ist ein vollständiges Bremsversagen oder eine fehlerhafte Airbag-Auslösung bei hohen Geschwindigkeiten.

Die Ermittlung der Kontrollierbarkeitsklassen erfordert eine Wahrscheinlichkeitsabschätzung, dass ein repräsentativer Fahrer in der Lage ist, die Kontrolle über sein Fahrzeug beizubehalten oder wiederzuerlangen, wenn eine Gefährdung eintritt. Diese Ermittlung kann über Fahrtests durchgeführt werden, wobei beachtet werden sollte, dass eine sehr große Anzahl an Testpersonen benötigt wird, um eine Quote von 99% an bestehenden Testfahrern zu erreichen. Für die Klasse C3 ist kein angemessener Beweis notwendig, da sie als „nicht beherrschbar“ eingestuft ist. Bei einer Zuweisung zu der Kontrollierbarkeitsklasse C0 muss keine weitere Risikobeurteilung durchgeführt werden.

Weiterhin erfolgt die Einstufung des Parameters *E*, also der Wahrscheinlichkeit der Exposition. Eine Bestimmung dieser Expositionswahrscheinlichkeit erfordert eine Auswertung verschiedener Szenarien, in denen die relevanten Umgebungsbedingungen

auftreten, die zum Gefährdungseintritt beitragen. Diese Szenarien umfassen eine Vielzahl von Fahr- und Betriebssituationen. Die Einstufung erfolgt anhand der folgenden fünf Kategorien (s. Tabelle 3-6):

Tabelle 3-6: Einstufung der Wahrscheinlichkeit der Exposition (E)

Stufe	Beschreibung	Definition der Dauer der Situation	Definition der Häufigkeit der Situation
E0	Unvorstellbar	-	-
E1	Sehr geringe Wahrscheinlichkeit	Nicht spezifiziert	Weniger als einmal pro Jahr für den Großteil der Fahrer
E2	Geringe Wahrscheinlichkeit	Weniger als 1% der Betriebszeit	Ein paar Mal im Jahr für den Großteil der Fahrer
E3	Mittlere Wahrscheinlichkeit	1% bis 10% der Betriebszeit	Einmal pro Monat oder öfter für den Durchschnittsfahrer
E4	Hohe Wahrscheinlichkeit	Mehr als 10% der Betriebszeit	Fast bei jeder Fahrt im Durchschnitt

Wie in obiger Tabelle 3-6 zu erkennen, kann die Zuordnung zu den Kategorien auf zwei unterschiedliche Arten geschehen. Das begründet sich in der Tatsache, dass die Situationen in Abhängigkeit der Dauer der Situation oder der Eintrittshäufigkeit der Situation gefährlich werden können. Auf der einen Seite wird die Expositionswahrscheinlichkeit über das Verhältnis der Dauer zur Gesamtbetriebszeit bestimmt. Hierbei kann es in Ausnahmen notwendig sein, die gesamte Fahrzeuglebensdauer zu verwenden. Auch für diese Einstufung gibt die Norm Beispiele vor, wie z.B. die Bergabfahrt mit ausgeschaltetem Motor für E1, verschneite/vereiste Straßen oder Fahrten mit Anhänger für E2, Tunnelfahrten oder Verkehrsstaus für E3 und Beschleunigen, Parken oder Spurwechsel für E4.

Auf der anderen Seite kann es geeigneter sein, für die Bestimmung der Expositionswahrscheinlichkeit die Eintrittshäufigkeit einer Situation zu verwenden. Beispiele für diese Einstufung sind das Abschleppen des Fahrzeugs für E1, Fahren mit Dachgepäckträger für E2, Überholmanöver für E3 und Anfahren, Bremsen oder Rückwärtsfahren für E4.

Bei dieser Unterscheidung zwischen Dauer und Häufigkeit einer Situation ist es möglich, dass eine Einstufung in beiden Fällen denkbar ist, wobei unterschiedliche Expositionseinstufungen herauskommen. Als Beispiel für eine solche Situation nennt die Norm die Waschanlage,

welche mit E2 bei der Dauer und mit E3 bei der Häufigkeit verschieden eingestuft wird. Dann gilt es, die Einstufung zu identifizieren, die am besten für die betrachtete Fahrsituation geeignet ist.

Sind alle Risikoparameter eingestuft worden, erfolgt in Schritt 5 der G+R die **Festlegung der notwendigen Risikominderung**. Nachdem die Einzelbewertungen der Parameter, die den Charakter einer Gefährdungssituation beschreiben, durchgeführt worden sind, ergibt sich der entsprechende automotive Sicherheitsintegritätslevel (ASIL) über die Kombination der ermittelten Tripel von Attributen. Mittels der Angaben in Bild 3-8 wird die notwendige Risikominderung in Form des ASIL festgelegt. Die abzuleitende Sicherheitsintegritätsstufe wird dabei durch einfache Zuordnung auf einer Skala von A bis D bestimmt.

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Bild 3-8: ASIL-Matrix

Die ASIL-Matrix in obiger Darstellung ist wie folgt zu interpretieren: Die Parametereinstufungen $E3$ (mittlere Expositionswahrscheinlichkeit), $C2$ (normale Beherrschbarkeit) und $S2$ (schwere bis lebensgefährliche Verletzungen) ergeben

beispielsweise einen ASIL A. In Bild 3-8 ist neben diesen Sicherheitsanforderungsklassen die Zuordnung mit der Bezeichnung QM (Qualitätsmanagement) vorgenommen worden. Eine mit QM bewertete Funktion ist explizit nicht als sicherheitsrelevant anzusehen.
Ein ASIL A stellt die niedrigste und ein ASIL D die höchste Einstufung dar. Die dabei herrschenden Zusammenhänge zwischen der ASIL-Einstufung und der Risikoreduzierung werden in nächstem Bild 3-9 dargestellt.

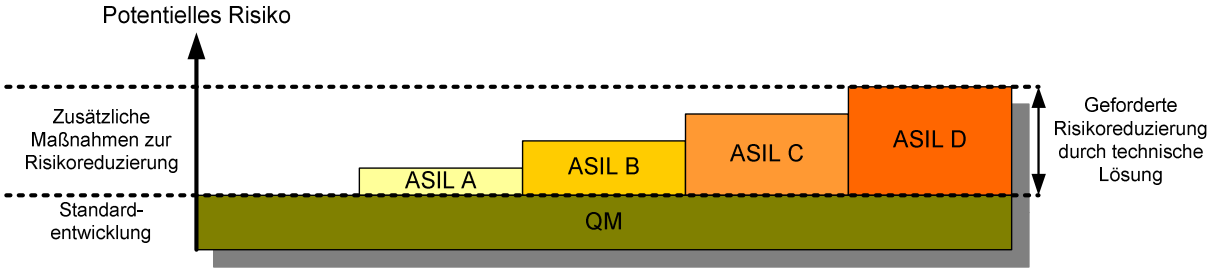


Bild 3-9: Zusammenhang ASIL und Risikoreduzierung nach [DOL 08]

Der ASIL ist nach [LÖW 10] eine von vier Klassen zur Spezifizierung der notwendigen Sicherheitsanforderungen des Systems, um ein akzeptables Risiko zu erreichen. Mittels dieser Klassen können über Tabellenwerke in der ISO 26262 die entsprechenden Maßnahmen und Techniken zur Risikoreduzierung bestimmt werden. Eine höhere Klasse fordert immer anspruchsvollere bzw. effektivere Maßnahmen. QM bedeutet hierbei, dass keine besonderen Maßnahmen zur Risikoreduzierung erforderlich sind, sondern die Schritte der Standardentwicklung als ausreichend angesehen werden. In [KLA 11] können einige ASIL-Einstufungen beispielhaft eingesehen werden.

Der automotive Sicherheits-Integritätslevel, der im Rahmen der Gefahrenanalyse und Risikobewertung für die betrachtete Funktion und das entsprechende System bestimmt wird, gibt nach [VDA 08] an, mit welcher Güte systematische Fehler während der Entwicklung vermieden und zufällige Fehler während des Betriebs beherrscht werden müssen. Für jede in der G+R betrachtete Gefährdung wird in einem letzten Schritt ein **Sicherheitsziel** bestimmt. Diese Sicherheitsziele werden im anschließenden Funktionalen Sicherheitskonzept benötigt, um die funktionalen Sicherheitsanforderungen abzuleiten. Ein Sicherheitsziel stellt somit die Top-Level-Sicherheitsanforderung dar. Hierbei kann sowohl ein Sicherheitsziel mehreren Gefährdungen zugeordnet sein als auch mehrere Sicherheitsziele einer Gefährdung. Die Sicherheitsanforderungen werden nach dem FSK während des Technischen

Sicherheitskonzepts in technische Sicherheitsanforderungen überführt, die dann in die Hard- und Softwareblöcke umgesetzt werden (s. hierzu auch Anmerkungen in Abschnitt 3.3.5).

Für die Mitarbeit bei einer G+R sollten Experten aus unterschiedlichen Themengebieten hinzugezogen werden, so dass die notwendige Kompetenz vorliegt. Folgendes Know-How sollte in einem G+R-Team möglichst vorhanden sein, um eine sorgfältige und verantwortungsvolle Durchführung zu gewährleisten:

- Fachkenntnisse zur Betrachtungseinheit,
- Wissen zum Komplex der Funktionalen Sicherheit,
- Einschätzung des Verhaltens vom Fahrer,
- Einschätzung des Verhaltens vom Fahrzeug,
- Einschätzung der Auswirkungen einer Fehlfunktion und
- Methodenkompetenz für die Durchführung einer G+R.

Zusammenfassend kann festgehalten werden, dass die ASIL-Einstufungen bestimmen, welche Schritte in der Entwicklung durchlaufen werden müssen und welche Anforderungen an das E/E-System zu stellen sind, um eine entsprechende Absicherung des Systems zu gewährleisten. In Abhängigkeit der ermittelten ASIL-Einstufung sind in der ISO 26262 Anforderungen an die unterschiedlichen Phasen des Sicherheitslebenszyklus zu finden, welche es zu beachten gilt. Hierzu zählen u.a.

- die Durchführung von induktiven und deduktiven Sicherheitsanalysen,
- die Einhaltung von Hardware-Metriken hinsichtlich Einfachfehler (Single Point Fault Metric) und schlafender Mehrfachfehler (Latent Point Fault Metric),
- die Anwendung von bestimmten Methoden bei der Softwareentwicklung,
- die Qualifizierung von Softwarewerkzeugen,
- die Erstellung von Fertigungs- und Produktionslenkungsplänen und
- die Spezifizierung und Umsetzung eines Feldbeobachtungsprozesses.

Ein weiterer wichtiger Aspekt ist die Forderung der ISO 26262 nach der Festschreibung von probabilistischen Zielwerten für die Verletzung von Sicherheitszielen aufgrund von zufälligen Hardwareausfällen in Abhängigkeit der ASIL-Einstufung. Für die Zielwerte lässt die Norm drei mögliche Quellen zu:

- aus Felddaten von ähnlichen, hochzuverlässigen Konstruktionsprinzipien ermittelt,

- aus den Ergebnissen von quantitativen Analysen zu früheren Entwürfen abgeleitet oder
- aus den Angaben aus folgender Tabelle 3-7 entnommen.

Tabelle 3-7: Quelle für die Ableitung der Zielwerte für zufällige Hardwareausfälle nach [ISO 10d]

ASIL	Zielwerte für zufällige Hardwareausfälle	Art
A	-	-
B	$< 10^{-7} \frac{1}{h}$	Empfehlung
C	$< 10^{-7} \frac{1}{h}$	Anforderung
D	$< 10^{-8} \frac{1}{h}$	Anforderung

Die quantitativen Zielwerte stellen nach [ISO 10d] durchschnittliche Wahrscheinlichkeiten pro Stunde (original: Average Probability Per Hour) über die Lebensdauer des Betrachtungsgegenstandes dar. Obige Tabelle 3-7 zeigt zunächst, dass für das automotive Sicherheits-Integritätslevel A kein normativer, quantitativer Zielwert für die Verletzung eines Sicherheitsziels aufgrund von Hardwareausfällen vorgesehen ist. Eine Begründung hierfür findet sich in der Norm nicht. [LÖW 10] gibt für ein ASIL A den informativen Wert von $< 10^{-6} \frac{1}{h}$ an. Weiterhin ist in Tabelle 3-7 zu erkennen, dass die Zielwerte für ASIL B und ASIL C gleich groß sind (vgl. hierfür auch Bild 3-10). Der gegebene Wert für ein ASIL B stellt darüber hinaus lediglich eine Empfehlung dar, und keine normative Anforderung. Auch hierfür sind in der Norm keine Begründungen vorhanden. Zwar soll nach [KRI 11] durch die Angaben keine absolute Relevanz im Hinblick auf real im Feld aufgetretenen Ausfallraten hergestellt werden. Hierzu muss angemerkt werden, dass es sich zum Einen nicht um Raten, sondern laut Norm um durchschnittliche Wahrscheinlichkeiten handelt. Zum Anderen kann nicht ausgeschlossen werden, dass solche normativen Angaben nicht dazu verwendet werden, um das Ausfallverhalten im Feld zu bewerten.

Eine Diskussion zu den Größenordnungen der normativ geforderten quantitativen Zielwerte ist in Abschnitt 4.4.4 zu finden.

Die Angaben der ISO 26262 (Tabelle 3-7) sind mit den Angaben der IEC 61508 (Tabelle 3-2) vergleichbar. Fahrzeugsysteme werden mehr als einmal im Jahr beansprucht, so dass nach der Einteilung in der IEC 61508 die „Betriebsart mit hoher Anforderungsrate oder mit kontinuierlicher Anforderung“ gewählt werden müsste und dementsprechend die PFH_D-Werte mit den Angaben der ISO 26262 verglichen werden müssten. Allerdings ist es bei einem Vergleich der Sicherheitsintegritätslevel nicht so, dass diese „eins zu eins“ übertragbar sind, wie folgendes Bild 3-10 zeigt, das an [lin 01] angelehnt ist.

IEC 61508		**ISO 26262**	
SIL	**Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde**	**ASIL**	**Durchschnittliche Wahrscheinlichkeit pro Stunde**
-		QM	-
1	$10^{-6} \leq x < 10^{-5}$ 1/h	A	-
2	$10^{-7} \leq x < 10^{-6}$ 1/h	B	$< 10^{-7}$ 1/h
		C	$< 10^{-7}$ 1/h
3	$10^{-8} \leq x < 10^{-7}$ 1/h	D	$< 10^{-8}$ 1/h
4	$10^{-9} \leq x < 10^{-8}$ 1/h	-	

Bild 3-10: Vergleich SIL/ASIL

In Bild 3-10 ist zu erkennen, dass die automotiven Sicherheits-Integritätslevel anders definiert und abgestuft sind als die SIL der IEC 61508. So gibt es zu einem SIL 4 kein entsprechendes Pendant in der Automobilnorm. Dies begründet sich damit, dass davon ausgegangen wird, dass von fehlerhaften Fahrzeugfunktionen keine katastrophalen Auswirkungen mit vielen Toten ausgehen können, wie es bei einer SIL 4-Einstufung der Fall ist. Ein SIL 1 ist

vergleichbar mit einem ASIL A. Die Level 2 und 3 der IEC 61508 werden im automobilen Umfeld größtenteils durch die Level B, C und D dargestellt, da die Gegebenheiten im Automobilbereich hier eine feinere Abstufung erfordern. Ein ASIL D ist hierbei ein SIL 3, aber nicht umgekehrt. Außerdem gibt die ISO 26262 keine Intervallgrenzen für die ASIL-Einstufungen an, wodurch ein direkter Vergleich von SIL 2 und ASIL B bzw. C nicht möglich ist. Die Untergrenze für SIL 2 von $10^{-7}\frac{1}{h}$ stellt die Obergrenze für ein ASIL B bzw C dar.

3.3.7 Abschließende Anmerkungen

Der Grundgedanke der ISO 26262 besteht darin, Lösungsvorschläge aufzuzeigen und nicht vorzuschreiben. Es wird grundsätzlich beschrieben, was bei der Entwicklung im Automobilbereich berücksichtigt werden sollte. Wie diese Vorgaben letztendlich umgesetzt werden, bleibt dem verantwortlichen Entwickler in den meisten Fällen frei gestellt. Ziel der Norm ist es folglich, Anforderungen vorzugeben ohne den Lösungsraum für die Umsetzung zu sehr einzuschränken. Nach [KRI 11] wurde die Norm bewusst auf einem Abstraktionslevel formuliert, der in der Produktumsetzung keine technischen Lösungen vorgeben, sondern Innovationsfähigkeit und Wettbewerbsdifferenzierung ermöglichen soll.

Aus diesen Freiräumen ergeben sich für den Anwender durchaus weite Interpretationsspielräume, die durchaus nach [KRI 11] durchaus gewollt sind. Dadurch kann es aber wiederum zu Schwierigkeiten kommen. Diese finden sich nach [elp 03] z.B. bei der Durchführung der G+R wieder. Zwar bietet die ISO 26262 genauere und umfangreichere Parametersätze als die IEC 61508, jedoch gibt die Automobilnorm nur wenige Hinweise, wie diese drei Risikoparameter konkret festzulegen sind, so dass die Parameter-Einstufungen subjektiv bleiben. Hier liegen die Herausforderungen u.a. darin, zu einem „konsistenten ASIL-Gefüge“ der Fehlfunktionen zu kommen – und zwar innerhalb der gesamten Automobilindustrie. Dieses muss dann von allen Unternehmen berücksichtigt werden.

Dem Automobilstandard mangelt es an einigen Stellen allerdings auch an klaren Definitionen und Erläuterungen, so beispielsweise hinsichtlich der angesprochenen Hardware-Metriken, bei denen nach [MAS 12] klare Definitionen und Abgrenzungen bei den zu verwendenden Größen fehlen. Weiterhin werden Grenzwerte für zufällige Hardwareausfälle vorgegeben. Der entsprechende Parameter wird jedoch nicht deutlich definiert.

Auch für die Thematik des Betriebsbewährtheitsnachweises liefert die Norm zwar Vorgaben in Abhängigkeit des eingestuften ASIL, jedoch werfen diese durchaus Fragen auf und bieten

ebenfalls einen gewissen Interpretationsspielraum. Hierauf wird im folgenden Kapitel eingegangen.

Nach [elp 01] gehen Abschätzungen davon aus, dass durch die Umsetzung der ISO 26262 der Entwicklungsaufwand um 3% bis 10% ansteigen wird. Dies ist natürlich abhängig vom Anteil der sicherheitsrelevanten Elemente der gefertigten Produkte. Es ist aber davon auszugehen, dass der Mehraufwand nach einem initialen Anstieg, in dem neue Dinge implementiert und Prozesse angepasst werden müssen, über die Jahre hinweg wieder abnehmen wird.

4 Proven in Use

Die bisherigen Ausführungen behandelten die notwendigen Schritte bei der Neuentwicklung von elektrischen/elektronischen Komponenten und Systemen, um deren Funktionale Sicherheit zu gewährleisten. Allerdings haben die Hersteller - unabhängig von der Branche - seit Jahren bereits entwickelte Produkte sehr erfolgreich auf dem Markt, die sich im täglichen Einsatz bewährt haben. Insbesondere die Automobilindustrie kann Systeme in ihren Fahrzeugen nachweisen, bei denen es im Einsatz über Tausende von Kilometern zu keinen sicherheitskritischen Fehlern oder Ausfällen gekommen ist und die nicht nach den Vorgaben der ISO 26262 entwickelt worden sind. Um solche Produkte hinsichtlich der Normenkonformität bewerten zu können, bietet die ISO 26262 die Möglichkeit, einen Betriebsbewährtheitsnachweis durchzuführen. Diese Vorgehensweise beruht auf der Auswertung von Felddaten, um dadurch nachträglich den Beweis zu erbringen, dass das Produkt mindestens eine genauso große Sicherheit bietet, als wenn es nach Normvorgaben entwickelt worden wäre. Die normativen Vorgaben zum automotiven Betriebsbewährtheitsnachweis und der damit zusammenhängenden Vorgehensweise werden nachfolgend vorgestellt. Darin erfolgt auch eine kritische Auseinandersetzung und Interpretation dieser Vorgaben. Zuvor soll der Begriff Betriebsbewährtheit oder auch Betriebsbewährung (Proven in Use) näher erläutert werden und der heutige Stand im Umgang mit diesem Nachweis aufgezeigt werden.

4.1 Allgemeines

Unter „Proven in Use“ wird die Möglichkeit verstanden, die Betriebsbewährtheit einer Komponente über die Auswertung von Betriebsinformationen nachzuweisen. In [GAL 00] wird beschrieben, dass Rechner- bzw. programmierbare Systeme in vielen unterschiedlichen Anwendungsgebieten für sicherheitsrelevante Aufgaben eingesetzt werden. Häufig werden Systeme eingesetzt, die entweder bereits für bestimmte Anwendungen qualifiziert sind oder in nicht sicherheitsrelevanten Anwendungen zum Einsatz kamen. Für solche Produkte kann der Nachweis der Betriebsbewährung ein wirtschaftlicher Weg zur Erlangung eines Sicherheitsnachweises sein, der entsprechend nationaler und internationaler Normung erforderlich ist.

Eine generelle Definition der Betriebsbewährtheit liefert eine der Vornormen zur DIN EN 61508, die DIN V VDE 0801, welche im Jahr 2004 jedoch zurückgezogen worden ist. Darin wird eine Betrachtungseinheit als betriebsbewährt angesehen, wenn sie im Wesentlichen unverändert über einen ausreichenden Zeitraum in zahlreichen verschiedenen Anwendungen betrieben wurde und dabei keine oder nur unwesentliche Fehler festgestellt wurden [DIN 90].
Nach DIN EN 61511-1 ist eine Komponente betriebsbewährt, wenn eine entsprechend dokumentierte Untersuchung ergeben hat, dass Nachweise aus früheren Einsätzen belegen, dass die Komponente für den Einsatz in einem sicherheitstechnischen System geeignet ist [DIN 05].
Aktueller ist die Definition im Norm-Entwurf [DIN 06], welche besagt, dass „Proven in Use“ ein auf einer Analyse der betrieblichen Erfahrung für eine spezielle Konfiguration eines Elements basierender Nachweis ist. Die Wahrscheinlichkeit eines gefahrbringenden systematischen Fehlers muss dabei niedrig genug sein, damit jede Sicherheitsfunktion, die das Element verwendet, ihren erforderlichen Sicherheits-Integritätslevel erreicht.

Die Idee, auf langjährige Erfahrungen und somit erfolgreiche und bewährte Produkte zu setzen, stammt nicht allein von der Automobilindustrie. In vielen Bereichen, sei es in der Prozessindustrie oder im Bereich Werkzeugmaschinenbau, ist der Nachweis der Betriebsbewährtheit ein Thema. Die Anforderungen an einen Betriebsbewährtheitsnachweis werden in den Normen verschieden dargestellt und darüber hinaus gehen die normativen Standards teils von sehr unterschiedlichen Voraussetzungen aus. Die Normen bieten weiterhin nur unzureichend konkrete Hinweise oder Anleitungen, wie ein solcher Nachweis erbracht werden sollte. Das liegt nach [GAL 00] u.a. an einer nicht eindeutigen Definition der für die Bewährung tatsächlich notwendigen Betriebszeit. So gibt es heutzutage einige Ansätze von Verbänden, Forschungseinrichtungen oder Beratungsunternehmen, die sich mit der Nachweisführung der Betriebsbewährung beschäftigen. Auf diese soll im Folgenden kurz eingegangen werden.

4.2 Bisherige Ansätze für Proven in Use

Die IEC 61508 beschreibt in [DIN 02d] unter dem Aspekt der „Felderfahrung“ die Maßnahme der Betriebsbewährtheit für den Einsatz einer Betrachtungseinheit, die im Wesentlichen unverändert über einen ausreichend langen Zeitraum in zahlreichen verschiedenen Anwendungen betrieben wurde und bei der es zu keinen oder nur unbedeutenden Fehlern

gekommen ist. Um als „felderfahren“ angesehen zu werden, müssen folgende Bedingungen erfüllt sein:

- unveränderte Spezifikation,
- zehn Systeme in verschiedenen Anwendungen und
- 10^5 Betriebsstunden und mindestens ein Jahr Betriebsaufzeichnung.

Hierbei wird die Felderfahrung über die Dokumentation des Herstellers und/oder des betreibenden Unternehmens nachgewiesen.

Die IEC 61511 beschreibt in [DIN 05] mit dem Stichwort „frühere Nutzung“ (original: Prior Use) die Betriebsbewährtheit auf Basis einer früheren Verwendung. Dieser Nachweis muss Folgendes beinhalten:

- Berücksichtigung des Qualitäts- und Konfigurationsmanagements beim Hersteller,
- geeignete Identifizierung und Spezifikation der Komponenten oder Teilsysteme,
- Nachweis der Leistungsfähigkeit der Komponenten oder Teilsysteme bei vergleichbaren Betriebsanforderungen in einer ähnlichen Betriebsumgebung und
- Umfang der Betriebserfahrung (z.B. in Form von Standardgerätelisten).

Auch für den Bereich der Kernkraftwerke hat sich der zuständige kerntechnische Ausschuss (KTA) bereits Ende der 1980er Jahre Gedanken zu PiU gemacht. In der sicherheitstechnischen Regel 3507 des KTA [KTA 02] wird zum Nachweis der Betriebsbewährung ohne Typprüfnachweis die Auswertung von Aufzeichnungen über die Betrachtungseinheit oder vergleichbaren Betrachtungseinheiten auf der Grundlage der für diese Einheit spezifizierten Eigenschaften und Umgebungsbedingungen gefordert. Für vergleichbare Einheiten ist hierbei nachzuweisen, dass vergleichbare elektrische Bauteile, Konstruktionselemente und Auslegungsgrundsätze verwendet und gleiche Umgebungs- und Betriebsbedingungen spezifiziert wurden. Die Aufzeichnungen sind nach statistischen Methoden auszuwerten, wobei folgende Bedingungen erfüllt sein müssen:

- Wahl eines Kollektivs, von dem mindestens zehn Stück über einen Zeitraum von zwei Jahren in Betrieb waren,
- Kollektiv muss mindestens eine Betriebsstundenzahl von 10^7 h erreicht haben und
- Angabe der mittleren Ausfallrate und des Vertrauensbereichs mit einer Sicherheit von 95% nach der Chi-Quadrat-Verteilung.

Auf der Hauptversammlung 2010 der NAMUR[11], einer Interessensgemeinschaft der Automatisierungstechnik der Prozessindustrie, wurde in [NET 11] u.a. die NAMUR-Empfehlung NE 130 vorgestellt, die sich mit betriebsbewährten Geräten für Schutzeinrichtungen in der Prozessleittechnik (PLT) und einer vereinfachten SIL-Berechnung beschäftigt. In dieser Empfehlung wird ein Konzept der Betriebsbewährung für PLT-Schutzeinrichtungen in vier Schritten vorgestellt. Es sind dort Richtwerte für sicherheitstechnische Kennzahlen von betriebsbewährten Geräten angegeben. Dabei handelt es sich um konstante Ausfallraten, die für bestimmte Gerätegruppen aus dem praktischen Einsatz anhand einer seit 2002 bestehenden Datenbank von Störfällen ermittelt worden sind. Die Datenbasis beruht auf einer langjährigen Beobachtung des Fehlerverhaltens von circa 40.000 Schutzeinrichtungen in rund 40 sich beteiligenden Unternehmen. Anhand der ermittelten Ausfallwerte wurden Musterrechnungen für verschiedene Redundanzkonzepte durchgeführt, so dass Unternehmen aus der Prozessindustrie mit Hilfe dieser Angaben bei Verwendung der genannten betriebsbewährten Geräte auf einen Einzelnachweis verzichten können, da er bereits vorliegt.

Die zuvor genannten Ansätze für den Nachweis der Betriebsbewährtheit einer Komponente bieten mögliche Anregungen für einen Ansatz in der Automobilindustrie, sind allerdings nicht spezifisch genug und lediglich allgemein gehalten. Darüber hinaus kann keine Konsistenz im Vorgehen festgestellt werden. Sie bieten entweder sehr generelle Vorgaben (IEC 61511) oder fordern den Nachweis einer pauschal festgelegten Mindestbetriebszeit (IEC 61508 oder KTA). In keinem der Ansätze wird die konkrete Auswertung von realen Felddaten explizit gefordert oder gar eine Vorgehensweise für den Nachweis geliefert. Dies wurde auch in [GAL 00] erkannt, wo neue Interpretationsansätze hinsichtlich der Betriebsbewährung zur Verfügung gestellt werden. Darin wird ein standardisiertes Verfahren präsentiert, welches dem in der ISO 26262 vorgeschlagenen (s. Abschnitt 4.3) ähnlich ist.

Von den zuvor vorgestellten Ansätzen ist besonders der von NAMUR interessant, da er die Auswertung von Felddaten in den Mittelpunkt stellt. Die Automobilindustrie und insbesondere die OEM verfügen über sehr umfangreiche und strukturierte Datenbanken, in denen u.a. Informationen zu aufgetretenen Garantie- und Kulanzfällen enthalten sind. Diese bieten eine mögliche Basis für den Einsatz in einer PiU-Untersuchung.

[11] Die NAMUR ist ein internationaler Verband der Anwender von Automatisierungstechnik der Prozessindustrie. Ihr ursprünglicher voller Name „Normenarbeitsgemeinschaft für Meß- und Regeltechnik in der chemischen Industrie“ wird heute nicht mehr verwendet.

4.3 Automotive Normvorgaben für Proven in Use

Nachfolgend werden die in der Automobilnorm ISO 26262 in [ISO 10e] gegebenen Vorgaben hinsichtlich eines Betriebsbewährtheitsnachweises oder auch PiU-Argumentation (original: Proven in Use Argument) dargestellt und erläutert. Eine Interpretation und Bewertung dieser wird in Abschnitt 4.4 vorgenommen.

Der Begriff „Proven in Use“ bezeichnet und beschreibt eine alternative Vorgehensweise zum Standardvorgehen der ISO 26262, um die Funktionale Sicherheit eines sicherheitsbezogenen E/E-Systems in Konformität zu der Norm nachzuweisen. Dies kann zum Beispiel bei der Wiederverwendung von Komponenten/Systemen der Fall sein, wenn entsprechende Informationen aus dem Feldeinsatz vorliegen. Es werden also keine Anforderungen an die Entwicklung eines E/E-Systems gestellt - es soll vielmehr nachträglich anhand von Analysen der Felddaten gezeigt werden, dass das System mindestens eine genau so große Sicherheit bietet, als wenn es komplett nach den Anforderungen der ISO 26262 entwickelt worden wäre. Die Sicherheit des E/E-Systems wird folglich durch die Betriebsbewährtheit im Feld nachgewiesen. Zusammengefasst hebt PiU nach [LÖW 10] die Bedeutung der Wiederverwendung von Elementen oder ganzen Systemen als eine sehr gute Alternative im Gegensatz zur Anwendung des gesamten Entwicklungslebenszyklus hervor.
Durch den Einsatz des Betriebsbewährtheitsnachweises kann es u.U. möglich sein, einen gewissen Umfang an Entwicklungsaufwand einzusparen. Der Aufwand einer PiU-Argumentation muss hierfür allerdings mit dem Aufwand einer Komplettentwicklung nach ISO 26262 verglichen werden, um eine individuelle Aussage zu ermöglichen.

4.3.1 Einsatzmöglichkeiten

Eine PiU-Argumentation kann prinzipiell auf alle Elemente des zu entwickelnden Produkts angewendet werden, deren Definition und Bedingungen identisch sind zu oder einen hohen Grad an Übereinstimmung haben mit einem bereits freigegebenen und im Einsatz befindlichen Element. Es kann sowohl auf ein Gesamtsystem oder eine Gesamtfunktion als auch auf ein Teilsystem bzw. einen Betrachtungsgegenstand angewendet werden. Betrachtungsgegenstand im Sinne der Norm kann ein System, eine Funktion, eine HW-Komponente, eine SW-Komponente oder auch einzelne Arbeitsergebnisse aus den Teilen der ISO 26262 sein, wie z.B. ein TSK, Testspezifikationen, ein Algorithmus oder ein Quellcode. Der jeweilige Umfang bzw. die Betrachtungseinheit wird „Kandidat“ genannt.

Die Motivation für einen Betriebsbewährtheitsnachweis beinhaltet

- die teilweise oder komplette Übertragung einer automotiven Applikation in kommerzieller Verwendung in ein anderes Objekt oder
- die Implementierung einer zusätzlichen Funktion in ein ECU[12] oder
- einen Kandidaten im Feldeinsatz, der vor der Veröffentlichung der ISO 26262 entwickelt worden ist oder
- einen Kandidaten im Einsatz in anderen sicherheitsbezogenen Industrien oder
- einen Kandidaten, der ein weit verbreitetes COTS[13]-Produkt ist, das nicht notwendigerweise für den Einsatz im Automobil vorgesehen ist.

An dieser Stelle widerspricht sich die Norm selbst. In [ISO 10e] wird bei den Angaben zum Geltungsbereich nämlich festgelegt, welche Systeme und Produkte aus dem Betrachtungsumfang ausgeschlossen werden. Hierzu zählen solche Systeme und Komponenten, die

- vor dem Veröffentlichungsdatum der ISO 26262 bereits zur Produktion freigegeben sind oder
- sich vor dem Veröffentlichungsdatum der ISO 26262 bereits in der Entwicklung befinden.

Manche Experten, wie beispielsweise in [KRI 11] zu sehen, sehen aufgrund der Angaben zum Geltungsbereich der Norm grundsätzlich keinen möglichen Anwendungsfall für eine PiU-Argumentation. Der Autor der vorliegenden Arbeit kann einen solchen Fall nicht ausschließen, vor allem, da in dem entsprechenden Kapitel der ISO 26262, wie zuvor gezeigt, mögliche Szenarien für einen Betriebsbewährtheitsnachweis aufgezeigt werden.

4.3.2 Voraussetzungen

Die Durchführung einer PiU-Argumentation ist an eine Reihe von Voraussetzungen gebunden, ohne deren Erfüllung die Methode nicht ausgeführt werden darf. Hierbei sind zwei Szenarien für die Verwendung des Kandidaten zu beachten:

[12] Der Begriff Electronic Control Unit (ECU) beschreibt Steuergeräte und Mikrocontroller.
[13] Der Begriff Component-off-the-Shelf (COTS) bezeichnet in der Wirtschaft ein seriengefertigtes Produkt aus dem Elektronik- oder Softwarebereich, das in großer Stückzahl völlig gleichartig aufgebaut („von der Stange“) gefertigt und vertrieben wird [wik 02].

- Betrachtung des Kandidaten in seiner geplanten neuen Verwendung und
- Betrachtung des Kandidaten in seiner bisherigen Verwendung.

Zur Erstellung eines Betriebsbewährtheitsnachweises für einen Kandidaten in seiner bisherigen Verwendung sind folgende Informationen notwendig:

- Spezifikation des Kandidaten,
- zutreffende(s) Sicherheitsziel(e) oder Sicherheitsanforderung(en) mit den zugehörigen ASIL-Einstufungen und
- vorhersehbare Betriebssituationen sowie geplante Betriebsarten und Schnittstellen.

Hinsichtlich der bisherigen Verwendung des Kandidaten sind Felddaten aus der Betriebszeit erforderlich.
Zum Kandidaten und seiner bisherigen Verwendung sind weiterhin Beschreibungen notwendig, aus denen hervorgeht, welche Elemente und Komponenten der Kandidat umfasst. Außerdem müssen Informationen zu Umgebungs-, Schnittstellen, physikalischen, funktionalen und Leistungseigenschaften des Kandidaten enthalten sein. Sofern verfügbar sind auch die Sicherheitsanforderungen der bisherigen Verwendung mit den entsprechenden ASIL anzugeben.

4.3.3 Änderungsanalyse

Während einer Änderungsanalyse werden Änderungen am Kandidaten (am Design durch z.B. Anforderungsmodifikationen oder funktionale Erweiterungen bzw. bei der Implementierung durch z.B. Softwarekorrekturen oder neue Entwicklungswerkzeuge) sowie an dessen Umgebung identifiziert und zu bewertet. Änderungen an Konfigurations- oder Kalibrierungsdaten sind als Änderungen am Kandidaten anzusehen, wenn sie einen Einfluss auf dessen Verhalten haben im Hinblick auf eine mögliche Verletzung der Sicherheitsziele. Änderungen an der Umgebung des Kandidaten (z.B. durch einen neuen Einbauort oder Updates von Komponenten, die mit dem Kandidaten interagieren) sind ebenfalls zu berücksichtigen. Wird gezeigt, dass die geplanten Änderungen definitiv keinen Einfluss auf die Sicherheit des Gesamtsystems haben, kann die Änderung als unkritisch angesehen werden.

4.3.4 Quantitative Zielwerte

Für die Analyse der Felddaten eines Kandidaten gibt die Norm Grenz- bzw. Zielwerte vor, die für den normativen Nachweis in Abhängigkeit der ASIL-Einstufung einzuhalten sind. Liegt für den Kandidaten noch keine ASIL-Bewertung vor, wird konservativ ein ASIL D festgelegt.
Hierzu ist die Ermittlung der gesamten Betriebszeit des Kandidaten erforderlich. Da ein Kandidat (z.B ein Steuergerät) in unterschiedlichen Fahrzeugtypen einer Baureihe (z.B. Fahrzeuge mit Otto- oder Dieselmotor, Allradfahrzeuge, Limousinen, Kombifahrzeuge, Sportwagen usw.) oder sogar in verschiedenen Baureihen verbaut sein kann, müssen alle Betriebszeiten der relevanten Fahrzeuge ermittelt und summiert werden. Der Beobachtungszeitraum jedes Prüflings muss sich hierfür über eine Betriebszeit von mindestens einem Jahr erstrecken.

Für jedes Sicherheitsziel (als Ergebnis der durchgeführten G+R) des Kandidaten muss die Rate für die Verletzung dieses Sicherheitsziels bestimmt werden. Ist die aus den Felddaten ermittelte Rate - die Norm spricht hier von einer „beobachtbaren Ereignisrate“ (original: Observable Incident Rate) - größer als die entsprechende Vorgabe der Norm, so ist die Verwendung der PiU-Argumentation nicht erfolgreich. Hierbei geht es um vom Hersteller beobachtbare Ereignisse. Diese müssen vom Kandidaten ausgehen und das Potential besitzen, ein Sicherheitsziel zu verletzen.
In den beiden nachfolgenden Tabellen sind die normativen Grenzwerte der beobachtbaren Ereignisrate zu finden, einmal für den Fall, dass Ereignisse eingetreten sind (Tabelle 4-1), und einmal für den Fall, dass noch keine Ereignisse beobachtet werden konnten (Tabelle 4-2). Die darin enthaltenen Angaben beziehen sich auf die Betriebszeit des Kandidaten. Zugrunde gelegt ist ein einseitiges unteres Konfidenz- oder auch Vertrauenslevel von 70%.

Tabelle 4-1: Grenzwerte bei beobachtbaren Ereignissen nach [ISO 10e]

ASIL	Beobachtbare Ereignisrate für die Verletzung des Sicherheitsziels bei beobachtbaren Ereignissen
A	$< 10^{-7} \frac{1}{h}$
B	$< 10^{-8} \frac{1}{h}$
C	$< 10^{-8} \frac{1}{h}$
D	$< 10^{-9} \frac{1}{h}$

Tabelle 4-2: Grenzwerte ohne beobachtbare Ereignisse nach [ISO 10e]

ASIL	Beobachtbare Ereignisrate für die Verletzung des Sicherheitsziels ohne beobachtbare Ereignisse
A	$< 3 \cdot 10^{-7} \frac{1}{h}$
B	$< 3 \cdot 10^{-8} \frac{1}{h}$
C	$< 3 \cdot 10^{-8} \frac{1}{h}$
D	$< 3 \cdot 10^{-9} \frac{1}{h}$

Die Norm unterscheidet hierbei, wie aus den obigen Tabellen hervorgeht, ob es in dem Betrachtungszeitraum bereits relevante Ereignisse gegeben hat, die beobachtet wurden, oder nicht. Findet eine PiU-Untersuchung zu einem frühen Zeitpunkt nach der Serienfreigabe statt, kann es sein, dass noch keine Ereignisse eingetreten sind, die vom Kandidaten verursacht worden sind und zu einer Verletzung des Sicherheitsziels geführt hätten. Es soll zu diesem Zeitpunkt aber trotzdem ein PiU-Nachweis erbracht werden (die Norm spricht hierbei von einer Interimsperiode (original: Interim Period)). Um dies zu ermöglichen, wurden die Angaben mit beobachtbaren Ereignissen (s. Tabelle 4-1) mit einem Sicherheitsfaktor mit dem Wert 3 versehen (s. Tabelle 4-2). Die Wahl des Wertes 3 ist in der Norm allerdings nicht begründet.

In nachfolgender Tabelle 4-3 sind Beispiele für die minimale Betriebszeit des Kandidaten in Abhängigkeit des jeweiligen ASIL gegeben für den Fall, dass kein durch den Kandidaten verursachtes beobachtbares Ereignis vorgelegen hat, welches das Potential hatte, das Sicherheitsziel zu verletzen.

Tabelle 4-3: Zielwerte der minimalen Betriebszeit ohne beobachtbares Ereignis nach [ISO 10e]

ASIL	Minimale Betriebszeit des Kandidaten ohne beobachtbares Ereignis
A	$1{,}2 \cdot 10^7\, h$
B	$1{,}2 \cdot 10^8\, h$
C	$1{,}2 \cdot 10^8\, h$
D	$1{,}2 \cdot 10^9\, h$

Die Werte in oben stehender Tabelle lassen sich nach [ISO 10e] aus folgender Gleichung bestimmen:

$$T = MTTF \cdot \frac{\chi^2_{KL;2f+2}}{2} \tag{4-1}$$

mit T: Kumulative Betriebszeit (summiert über alle betrachteten Fahrzeuge), auch akkumulierte Lebensdauer genannt,

$MTTF$: Mean Time To Failure $\left(= \frac{1}{Ausfallrate}\right)$,

KL: Konfidenzlevel als absolute Zahl (z.B 0,7 bei einem Konfidenzlevel von 70%),

f: Anzahl der sicherheitsrelevanten Ereignisse,

$\chi^2_{\alpha;\nu}$: Chi-Quadrat-Verteilung mit der Irrtumswahrscheinlichkeit α und ν Freiheitsgraden.

Wichtig anzumerken ist an dieser Stelle, dass die Norm dabei voraussetzt, dass die sicherheitsrelevanten Ereignisse (bei denen es sich um Fehler oder Ausfälle an E/E-Komponenten handelt) exponentiell verteilt und deren Ausfallraten dementsprechend konstant sind. Dies ist in der Praxis eine gängige Vereinfachung. Dementsprechend kann die MTTF über den Kehrwert der Ausfallrate λ der Exponentialverteilung berechnet werden. Bei den Erläuterungen in der ISO 26262 zu obiger Formel wird von der „Ausfallrate“ gesprochen,

gemeint ist allerdings die „Beobachtbare Ereignisrate“. Bei diesen Ereignissen muss es sich nicht zwingend um Ausfälle handeln. Es können auch beispielsweise Fehler am Kandidaten zu einer Verletzung eines Sicherheitsziels führen. Es herrscht folglich keine einheitliche Nomenklatur in diesem Teil der Norm. Weitere Anmerkungen zum gegebenen Formalismus sowie anderen normativen Vorgaben zum PiU-Nachweis folgen im nächsten Abschnitt.

Es ergibt sich beispielsweise für ein ASIL D bei keinem beobachteten Ereignis und einem Konfidenzlevel von 70% folgende minimale Betriebszeit, wobei die Grundausfallrate aus Tabelle 4-1 verwendet wird:

$$T = \frac{1}{10^{-9}\frac{1}{h}} \cdot \frac{\chi^2_{0,7;2\cdot 0+2}}{2} = 10^9 h \cdot \frac{\chi^2_{0,7;2}}{2} = 1{,}204 \cdot 10^9 h\,.$$

Dieser und die entsprechend ermittelbaren Werte für die weiteren ASIL-Einstufungen ohne beobachtbare Ereignisse sind in Tabelle 4-3 zu finden.

Es wird deutlich, dass Faktoren in Abhängigkeit der Fehleranzahl bestimmt werden können, mit denen die Vorgaben der Norm multipliziert werden müssen, um die minimale Betriebszeit zu bestimmen, die erreicht werden muss. Die angesprochenen Vorgaben, die in Tabelle 4-4 zu finden sind, berechnen sich aus den Kehrwerten der beobachtbaren Ereignisraten über

$$Vorgabe = \frac{1}{Beobachtbare\ Ereignisrate}\,. \tag{4-2}$$

Als Werte für die beobachtbare Ereignisrate werden wiederum die Grundwerte aus Tabelle 4-1 verwendet.

Tabelle 4-4: Vorgaben aus ISO 26262 für die minimale Betriebszeit ohne Faktoren

ASIL	Vorgaben für die minimale Betriebszeit ohne Faktoren
A	$10^7 h$
B	$10^8 h$
C	$10^8 h$
D	$10^9 h$

In nachfolgender Tabelle 4-5 sind die Faktoren für eine Auswahl an Fehleranzahlen bis $f = 200$ exemplarisch aufgelistet. Für andere Fehleranzahlen lassen sich die Faktoren, wie zuvor gezeigt, leicht bestimmen.

Tabelle 4-5: Faktoren in Abhängigkeit der Fehleranzahl

Anzahl der Fehler	Faktor	Anzahl der Fehler	Faktor	Anzahl der Fehler	Faktor
0	1,204	10	12,470	20	23,141
1	2,439	11	13,548	30	33,661
2	3,616	12	14,623	40	44,101
3	4,762	13	15,695	50	54,490
4	5,890	14	16,765	60	64,842
5	7,006	15	17,832	70	75,166
6	8,111	16	18,898	80	84,467
7	9,209	17	19,961	90	95,751
8	10,301	18	21,023	100	106,019
9	11,387	19	22,082	200	208,186

Die Werte in den zuvor stehenden Tabellen sind folgendermaßen zu interpretieren:
Ausgehend von beispielsweise vier beobachteten Ereignissen, die das Potential haben, das dem Kandidaten zugeordnete Sicherheitsziel (bewertet mit einem ASIL C) zu verletzen, muss für einen PiU-Nachweis eine Gesamtbetriebszeit des Kandidaten von $5{,}890 \cdot 10^8 h$ nachgewiesen werden. Es wird hierfür also der Faktor in Abhängigkeit der Fehleranzahl (Tabelle 4-5) mit der Vorgabe in Abhängigkeit des ASIL (Tabelle 4-4) multipliziert, um die nachzuweisende Betriebszeit des Kandidaten zu ermitteln:

$$Betriebszeit = Faktor \cdot Vorgabe . \quad (4\text{-}3)$$

4.4 Interpretation und Bewertung der automotiven Vorgaben für Proven in Use

Nachfolgend werden die Vorgaben der ISO 26262 bezüglich einer PiU-Argumentation kritisch betrachtet und bewertet.

4.4.1 Konstantes Ereignisverhalten

Zunächst muss festgehalten werden, dass alle Vorgaben der Norm hinsichtlich einer PiU-Argumentation ein konstantes Ausfallverhalten und somit exponentiell verteilte sicherheitsrelevante Ereignisse voraussetzen. Dies ist eine gängige Annahme in der Praxis, da davon ausgegangen wird, dass ein mögliches Frühausfallverhalten bei elektronischen Komponenten durch gezielte Präventivmaßnahmen, wie vorab durchgeführte Belastungstests für künstliche Alterungseffekte (Burn-In), nicht mehr auftritt und somit ein konstantes Ausfallverhalten vorliegt (siehe Bild 4-1). Aufgrund zahlreicher praktischer Untersuchungen (siehe u.a. [MEY 10]) wurde allerdings gezeigt, dass insbesondere komplexe E/E-Komponenten ein ausgeprägtes Frühausfallverhalten besitzen können.
In Bild 4-1 ist das generelle zeitliche Verhalten der Ausfallrate zu erkennen, welches sich aus Lebensdauertests und Feldausfällen ermitteln lässt.

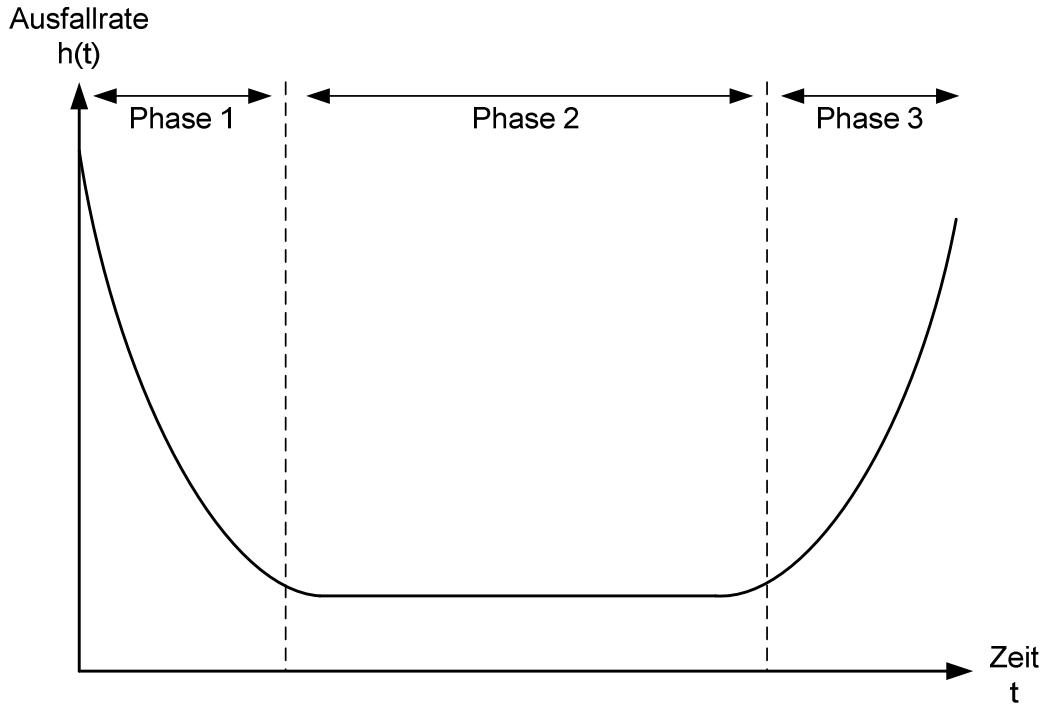


Bild 4-1: Zeitliches Verhalten der Ausfallrate („Badewannenkurve“)

Die dargestellte „Badewannenkurve“ stellt das hierzu grundlegende Schema dar. Es lassen sich nach [MEY 10] drei Bereiche einteilen, die jeweils durch eine Weibull-Verteilung oder eine andere Verteilungsfunktion beschrieben werden können:

- Phase 1: Frühausfälle
  Die in dieser Phase auftretenden Frühausfälle sind meist auf Materialschwächen und Qualitätsschwankungen in der Fertigung oder Anwenderfehler zurückzuführen. Kennzeichnend ist die mit zunehmender Lebensdauer t stetig fallende Ausfallrate.
- Phase 2: Zufallsausfälle
  Die Ausfälle im Zeitbereich der so genannten nützlichen Lebensdauer zeichnen sich durch eine konstante Ausfallrate aus. In der Phase kommt es zu zufälligen Ausfällen. Das Ziel der Hersteller liegt darin, diese Phase so lang wie möglich zu gestalten.
- Phase 3: Verschleißausfälle
  Die hier auftretenden Ausfälle sind auf Verschleiß-, Alterungs- und Ermüdungseffekte zurückzuführen. Sie zeichnen sich durch eine steigende Ausfallrate aus.

Die Vorgaben der ISO 26262 hinsichtlich der Bewertung eines möglichen Betriebsbewährtheitsnachweises durch die Annahme eines konstanten Verhaltens sind nicht universell gültig. Die Analyse von Felddaten ist einer der Hauptbestandteile des PiU-Nachweises nach Norm. Es stellt sich die Frage, warum nicht auch das tatsächliche zeitliche Verhalten der Ausfall- oder Ereignisrate aus eben diesen Daten ermittelt wird, anstatt von einer konstanten Rate auszugehen.
Darüber hinaus ist die normative Angabe, dass die beobachtbaren Ereignisse nicht das Potential besitzen dürfen, ein Sicherheitsziel zu verletzen, unpräzise. Zu einen ist unklar, was mit Potential gemeint ist, denn grundsätzlich kann jedem Fehler ein gewisses Potential zugeordnet werden. Zum anderen sind Fälle denkbar, in denen ein solcher Nachweis schwierig ist, da nicht ausgeschlossen werden kann, welche Fehler ein solches Potential besitzen oder nicht.

4.4.2 Qualitativer Nachweis

Ein weiterer Kritikpunkt an den Normvorgaben besteht darin, dass keine genauen Handlungsanweisungen gemacht werden, was bei einem nicht-konstanten Ausfallverhalten zu unternehmen ist. Wie soll beispielsweise der Vergleich einer aus den Felddaten ermittelten nicht-konstanten Ereignisrate mit einer normativ geforderten konstanten Rate erfolgen?

Hierzu finden sich in der Norm keinerlei Hinweise. Im Falle einer nicht konstanten Ausfallrate und somit einer nicht-exponentiellen Verteilungsfunktion der sicherheitsrelevanten Ereignisse gibt die Norm zwar an, dass zusätzliche Maßnahmen für eine PiU-Argumentation angewandt werden müssen, um beispielsweise Defekte zu berücksichtigen, welche mit Ermüdung verbunden sind. Detaillierte Vorgaben, was unter diesen zusätzlichen Maßnahmen zu verstehen ist und wie mögliche Arbeitsschritte aussehen, sind in der Norm aber nicht enthalten. Die entsprechende Interpretation bleibt den verantwortlichen Personen in den Unternehmen überlassen, die sich mit diesen Fragestellungen beschäftigen. Es verwundert darüber hinaus, dass die Norm Ausfälle aufgrund von Alterung des Kandidaten aus der Betrachtung ausschließt. Es sind bislang keine Untersuchungen bekannt, deren Ergebnisse belegen, dass E/E-Komponenten keinem Alterungsprozess unterliegen.

Die vorstehend angesprochene Problematik wird in nachfolgendem Bild 4-2 verdeutlicht. Darin dargestellt ist in blauer Farbe eine fiktive Ereignisrate $h_E(t)$ (wird in Abschnitt 5.4.3.1 erläutert), welche aus Felddaten ermittelt wird, mit einem charakteristischen Frühausfallverhalten. In roter Farbe ist der normative Grenzwert für eine ASIL D-Einstufung abgebildet, wobei der normative Wert mit der Einheit $\frac{1}{h}$ unter Verwendung von 400 Betriebsstunden pro Jahr[14] in die Einheit $\frac{1}{a}$ umgerechnet worden ist.

[14] Der Wert von 400 Betriebsstunden pro Jahr stellt einen in der Automobilindustrie üblicherweise verwendeten Wert dar, wenn keine genaueren Kenntnisse über die tatsächliche jährliche Betriebszeit vorhanden sind.

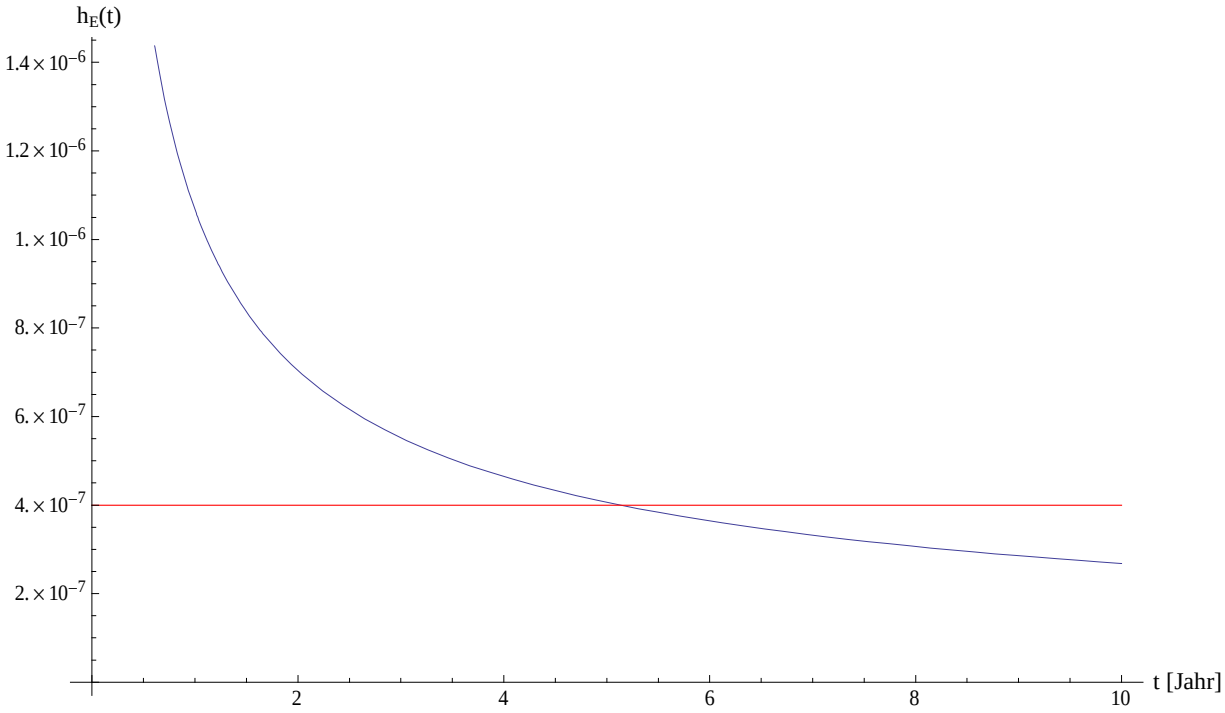


Bild 4-2: Qualitative Problematik beim PiU-Nachweis

In obigem Bild 4-2 ist zu erkennen, dass die fiktive Ereignisrate (blau) den Normgrenzwert (rot) schneidet. Das bedeutet, dass für dieses Beispiel keine positive PiU-Argumentation ausgesprochen werden könnte, da das tatsächliche Verhalten schlechter als die Normvorgabe ist. Ein positiver PiU-Nachweis kann folglich nur erbracht werden, wenn der gesamte Verlauf der tatsächlichen Ereignisrate unterhalb des normativen Grenzwertes liegt. Dieser Nachweis ist bei Kandidaten mit einem Frühausfallverhalten oder auch einem Spätausfallverhalten praktisch nicht zu erfüllen, da die Kurven den Grenzwert zu einem bestimmten Zeitpunkt immer schneiden würden. Nur ein rein konstanter Verlauf einer Ereignisrate lässt sich sinnvoll mit der Normvorgabe vergleichen und bewerten. Ein solches Ereignisverhalten ist allerdings in der Realität nicht zu erwarten.

Auch die Ermittlung des Durchschnittswertes der aus den Felddaten bestimmten Ereignisrate und dessen Vergleich mit dem Normgrenzwert ist nicht zielführend, da das Zeitintervall für die Bestimmung des Durchschnitts unbekannt ist.

4.4.3 Formalismus für die Betriebszeit

Zu dem in der ISO 26262 gegebenen Formalismus zur rechnerischen Bestimmung der Betriebszeit (siehe Gleichung (4-1)) gibt es einige Anmerkungen zu treffen. Neben der uneinheitlichen Nomenklatur der Norm, auf die in Abschnitt 4.3.4 bereits eingegangen wurde

(Ausfallrate vs. Beobachtbare Ereignisrate), gibt es weitere Inkonsistenzen bei der rechnerischen Angabe. Um diese zu erläutern, bedarf es einiger theoretischer Erklärungen, welche nachfolgend in Anlehnung an [HÄR 83] und [MEY 10] vorgenommen werden.

Wenn im Rahmen einer statistischen Untersuchung die Parameter einer Grundgesamtheit genau bestimmt werden sollen, muss eigentlich jede Einheit der Grundgesamtheit bei der Berechnung erfasst werden. Da dies in der Regel unpraktisch bis unmöglich ist, werden bei Tests statistische Verfahren auf der Basis von Stichproben verwendet. Dadurch können geschätzte oder Näherungswerte der entsprechenden Parameter angegeben werden, so genannte Punktschätzer. Im Gegensatz dazu kann eine Intervallschätzung durchgeführt werden. Dabei wird um den relevanten Messwert einer Stichprobe ein Intervall gelegt, für das gilt, dass sich der tatsächliche Parameterwert zu einem vorher festgelegten Konfidenzniveau in dem Intervall befindet. Die zugrunde liegende Stichprobe ist in der Regel unvollständig, d.h. $n << N$, wobei n die Stichprobengröße und N die Grundgesamtheit ist.

Bei solchen Zuverlässigkeitsuntersuchungen wird zwischen zwei Arten der Zensierung unterschieden:

- Typ-I-Zensierung und
- Typ-II-Zensierung.

Bei einer Typ-I-Zensierung liegt eine gestutzte Stichprobe vor. Dies ist der Fall, wenn der Test nach einer vorher definierten Zeit t_k (Beobachtungs- oder Testdauer) abgebrochen wird. Die Anzahl der Ausfälle k ist zufällig.
Wenn der Test nach einer vorher festgelegten Anzahl von Ausfällen k abgebrochen wird, liegt eine zensierte Stichprobe vor und somit eine Typ-II-Zensierung. Die Beobachtungsdauer t_k ist dabei zufällig, wohingegen $k \leq n$ ist.
Bei beiden Zensierungsarten können wiederum die Möglichkeiten

- mit Ersatz und
- ohne Ersatz

unterschieden werden.
„Mit Ersatz“ bedeutet in diesem Zusammenhang, dass die ausgefallenen Einheiten sofort wieder ersetzt werden und somit die Grundgesamtheit immer gleich groß bleibt (Modell „Ziehen mit Zurücklegen“). Werden die ausgefallenen Einheiten nicht wieder ersetzt („ohne Ersatz“), wird auch vom Modell „Ziehen ohne Zurücklegen“ gesprochen.

Für die vorliegenden Betrachtungen ist das Modell „Ziehen mit Zurücklegen“ relevant, da im Automobilbereich davon ausgegangen werden kann, dass ausgefallene Komponenten während eines Werkstattbesuches repariert bzw. ausgetauscht und durch identische Komponenten ersetzt werden.

Mit Hilfe von Vertrauensbereichen oder -intervallen können, wie bereits erwähnt, statistische Unsicherheiten, die mit einem einzigen Schätzwert auf Basis der Stichprobe verbunden sind, quantitativ zum Ausdruck gebracht werden. Diese statistische Unsicherheit α (auch Irrtumswahrscheinlichkeit genannt) bezeichnet die Wahrscheinlichkeit dafür, dass ein Wert x nicht im Intervall $[x_u, x_o]$ liegt. Dieses Intervall wird Konfidenz- oder auch Vertrauensintervall zum Konfidenzniveau $1-\alpha$ genannt. Übliche Werte aus der Praxis für $1-\alpha$ (auch statistische Sicherheit genannt) sind 90% bzw. 0,90, 95% bzw. 0,95 oder 99% bzw. 0,99. Die Abweichungen eines bestimmten Stichprobenparameters lassen sich über speziell entwickelte Prüfverteilungen bestimmen. Für die Exponentialverteilung (relevant für den Formalismus in der ISO 26262) haben sich für die Schätzung des Parameters λ die Chi-Quadrat-Verteilung und der Einsatz der Maximum-Likelihood-Methode bewährt. Bei den Vertrauensgrenzen wird dabei zwischen der

- einseitigen oberen Vertrauensgrenze $\lambda_{1-\alpha}$,
- einseitigen unteren Vertrauensgrenze λ_{α},
- zweiseitigen oberen Vertrauensgrenze $\lambda_{1-\frac{\alpha}{2}}$ und
- zweiseitigen unteren Vertrauensgrenzen $\lambda_{\frac{\alpha}{2}}$ unterschieden.

In nachfolgender tabellarischer Übersicht sind die wichtigsten Formeln für beide Zensierungsarten für den Vertrauensbereich des Schätzwertes $\hat{\lambda}$ gegenübergestellt, wobei nur die Möglichkeit „Mit Ersatz“ dargestellt ist.

Tabelle 4-6: Wichtige Formelzusammenhänge für zensierte und gestutzte Stichproben

Art	Funktion	Typ-I-Zensierung (t_k wird vorgegeben)	Typ-II-Zensierung (k wird vorgegeben)
Schätzwert	$\hat{\lambda}$	$\frac{k}{T_k}$	$\frac{k}{T_k}$
Einseitige untere Vertrauensgrenze	λ_{α}	$\frac{\chi^2_{\alpha}(2\cdot k)}{2\cdot T_k}$	$\frac{\chi^2_{\alpha}(2\cdot k)}{2\cdot T_k}$
Einseitige obere Vertrauensgrenze	$\lambda_{1-\alpha}$	$\frac{\chi^2_{1-\alpha}(2\cdot k+2)}{2\cdot T_k}$	$\frac{\chi^2_{1-\alpha}(2\cdot k)}{2\cdot T_k}$
Zweiseitige untere Vertrauensgrenze	$\lambda_{\frac{\alpha}{2}}$	$\frac{\chi^2_{\frac{\alpha}{2}}(2\cdot k)}{2\cdot T_k}$	$\frac{\chi^2_{\frac{\alpha}{2}}(2\cdot k)}{2\cdot T_k}$
Zweiseitige obere Vertrauensgrenze	$\lambda_{1-\frac{\alpha}{2}}$	$\frac{\chi^2_{1-\frac{\alpha}{2}}(2\cdot k+2)}{2\cdot T_k}$	$\frac{\chi^2_{1-\frac{\alpha}{2}}(2\cdot k)}{2\cdot T_k}$

Der normative Formalismus in Gleichung (4-1) beruht auf der Likelihoodfunktion der Maximum-Likelihood-Methode (siehe [MEY 10]), für die im Falle der einparametrigen Exponentialverteilung folgt:

$$L(\lambda|k)=\frac{n!}{(n-k)!}\cdot\left(\prod_{i=1}^{k}\lambda\cdot e^{-\lambda\cdot t_i}\right)\cdot e^{-\lambda\cdot(n-k)\cdot t_k}. \tag{4-4}$$

Durch Logarithmierung und Bestimmung des Maximums der Likelihoodfunktion ergibt sich für den Schätzer $\hat{\lambda}$ des unbekannten Parameters λ der Exponentialverteilung

$$\hat{\lambda}=\frac{k}{\sum_{i=1}^{k}t_i+(n-k)\cdot t_k}. \tag{4-5}$$

In obiger Tabelle 4-6 ist die summierte Lebensdauer T_k aller Einheiten ein zentraler Bestandteil. Sie wird auch akkumulierte Lebensdauer oder kumulative Betriebszeit genannt und bestimmt über

$$T_k=\sum_{i=1}^{k}t_i+(n-k)\cdot t_k \tag{4-6}$$

mit n: Stichprobenumfang,

k: Anzahl der Ausfälle,

t_k: Testdauer und

t_i: Ausfallzeitpunkt der i-ten Einheit.

Da es in der Praxis häufig der Fall ist, dass $k << n$ ist, kann der Term $k \cdot t_k$ vernachlässigt werden. Außerdem gilt

$$\sum_{i=1}^{k} t_i << k \cdot t_k , \tag{4-7}$$

so dass die Schätzung in guter Näherung auch über

$$\hat{\lambda} \approx \frac{k}{n \cdot t_k} \approx \frac{k}{T_k} , \tag{4-8}$$

erfolgen kann. Die Gleichung (4-8) gilt unabhängig davon, um welches Modell oder um welche Zensierung es sich handelt. Für den Fall, dass die ausgefallenen Einheiten wieder ersetzt werden, ist der Schätzer ohne Näherung durch

$$\hat{\lambda} = \frac{k}{n \cdot t_k} \tag{4-9}$$

gegeben.

Wird nun der Formalismus der ISO 26262 (s. Gleichung (4-1)) nach der Ausfallrate hin umgestellt ergibt sich

$$\lambda = \frac{\chi^2_{KL;2f+2}}{2 \cdot T} \tag{4-10}$$

mit T: Kumulative Betriebszeit (summiert über alle betrachteten Fahrzeuge),

λ Ausfallrate der Exponentialverteilung,

KL: Konfidenzlevel als absolute Zahl und

f: Anzahl der sicherheitsrelevanten Ereignisse

oder in anderer Schreibweise

$$\lambda = \frac{\chi^2_{1-\alpha}(2 \cdot k + 2)}{2 \cdot T_k} . \tag{4-11}$$

Das Konfidenzlevel entspricht dem Komplement zur Irrtumswahrscheinlichkeit, also $1-\alpha$. Die Anzahl der sicherheitsrelevanten Ereignisse f ist dabei gleich der Anzahl der Ausfälle k in den Ausführungen dieses Abschnitts und die kumulative Betriebszeit wird hier über T_k ausgedrückt. Wird die Gleichung (4-10) mit den Formeln aus Tabelle 4-6 verglichen, fällt auf, dass es sich dabei offensichtlich um den Formalismus für die Bestimmung der einseitigen

oberen Vertrauensgrenze für den Fall einer gestutzten Stichprobe (Typ-I-Zensierung) handelt, bei welcher die Beobachtungszeit stets vorgegeben wird.

Dies ist insofern verwunderlich, da durch die ISO 26262 die einseitige untere Vertrauensgrenze (original: Single Sided Lower Confidence Level) bei der Ermittlung der minimalen Betriebszeit eines PiU-Kandidaten vorgegeben wird.

Sowohl an Gleichung (4-10) als auch an Gleichung (4-11) fällt auf, dass die Ausfallrate λ und die Betriebs- oder Beobachtungszeit T umgekehrt proportional zueinander sind. Es gilt folglich

$$\lambda \sim P \cdot \frac{1}{T} \Leftrightarrow T \sim P \cdot \frac{1}{\lambda} \tag{4-12}$$

mit P: Proportionalitätsfaktor (z.B. $P = \frac{\chi^2_{1-\alpha}(2 \cdot k + 2)}{2}$).

D.h. da die Ausfallrate vorgegeben ist, wird die Betriebszeit minimal, wenn der Proportionalitätsfaktor minimal ist. Durch Verwendung des reinen normativen Formalismus mit der einseitigen oberen Vertrauensgrenze wird P allerdings maximal und dementsprechend auch T. Diese offensichtliche Diskrepanz zwischen dem gegebenen Formalismus und den Inhalten in den textlichen Beschreibungen der ISO 26262 sind an dieser Stelle für den ungeschulten Anwender allerdings kaum zu erkennen. An anderen Stellen in der Norm wird beispielsweise unabhängig von der zu wählenden Vertrauensgrenze lediglich allgemein von einer Konfidenz von 70% gesprochen, so dass unklar ist, welche in der Praxis gängigen Formalismen (s. Tabelle 4-6) verwendet werden müssen.

Wie bereits erwähnt, weicht die normativ vorgegebene Irrtumswahrscheinlichkeit von 30% deutlich von den in der Praxis verwendeten Werten ab. Für praxisnahe α-Werte von 0,1, 0,05 oder 0,01 im Gegensatz zum normativen α-Wert von 0,3 sind in nachfolgender

Tabelle 4-7 die Ergebnisse für die Berechnung der minimalen Betriebszeit für den Formalismus der ISO 26262 (verwendet werden die in der Norm gegebene Ausfallrate für ASIL D sowie kein bzw. ein beobachtbares sicherheitsrelevantes Ereignis) dargestellt.

Tabelle 4-7: Ergebnisse für praxisnahe Irrtumswahrscheinlichkeiten

Konfidenzniveau	α **-Wert**	$T = MTTF \cdot \frac{\chi^2_{KL;2f+2}}{2}$	
		$f = 0$	$f = 1$
70%	0,3	$1{,}204 \cdot 10^9\, h$	$2{,}439 \cdot 10^9\, h$
90%	0,1	$2{,}303 \cdot 10^9\, h$	$3{,}890 \cdot 10^9\, h$
95%	0,05	$2{,}996 \cdot 10^9\, h$	$4{,}744 \cdot 10^9\, h$
99%	0,01	$4{,}605 \cdot 10^9\, h$	$6{,}638 \cdot 10^9\, h$

Tabelle 4-7 zeigt, dass die Verwendung praxisnaher Werte für die Irrtumswahrscheinlichkeit zu einer deutlichen Erhöhung der minimalen Betriebszeit führt.
Die Verwendung der Näherungsformel aus Gleichung (4-8) führt unabhängig vom Konfidenzniveau zu dem Ergebnis, dass bei einer Ausfallrate von $\lambda = 1 \cdot 10^{-9} \frac{1}{h}$ und einem beobachtbaren Ereignis die minimale Betriebszeit $1 \cdot 10^{9} h$ betragen muss. Der Einsatz der Näherung kann dem Anwender eine Tendenz vermitteln, in welcher Größenordnung sich die Betriebszeit bei einer gegebenen Ereignisanzahl (exklusive einer Betrachtung von keinem beobachteten Ereignis) und einer normativ vorgegebenen Ausfallrate bewegen wird. Allerdings ist das Näherungsergebnis in jedem Fall niedriger als das Resultat ohne Näherung.

4.4.4 Quantitative Vorgaben

Nachfolgend werden die Vorgaben der ISO 26262 bezüglich der probabilistischen Werte für die beobachtbaren Ereignisraten (s. Angaben in Tabelle 4-1 bzw. in Tabelle 4-2) erörtert. Zunächst ist in beiden Tabellen zu erkennen, dass die numerischen Werte der Grenzwerte für ein ASIL B und ASIL C gleich groß sind und somit in dieser Hinsicht kein Unterschied zwischen den beiden Einstufungen gemacht wird. Eine Begründung hierfür findet sich in der Norm nicht.

An dieser Stelle sei zunächst erwähnt, dass es in den vergangenen Jahrzehnten in der Normungslandschaft, insbesondere bei Fragestellungen hinsichtlich Sicherheitsbeurteilungen und Risikoanalysen, ein gewisses Umdenken weg vom reinen Determinismus[15] hin zum Probabilismus[16] gegeben hat. Damit ist gemeint, dass insbesondere bei der Entwicklung von Sicherheitskonzepten und der dabei erforderlichen Nachweisführung neben deterministischen Ansätzen, die ohne Unsicherheiten operieren, vermehrt probabilistische Ansätze, welche Wahrscheinlichkeiten berücksichtigen, Einzug gefunden haben und immer noch finden.

[15] Unter dem Begriff Determinismus wird nach [BRO 06a] die Lehre von der kausalen Bestimmtheit allen Geschehens (auch des menschlichen Handelns) durch Naturgesetze verstanden. Der Determinismus geht davon aus, dass physikalische Zustände von Systemen dem Kausalprinzip insofern unterliegen, als dass die Zukunft durch die Gegenwart eindeutig bestimmt ist. Der mechanistisch-metaphysische Determinismus verkennt dadurch allerdings die Vielfalt der Form der Determination in der objektiven Realität, reduziert diese Vielfalt auf eine mechanistisch interpretierbare Kausalität und leugnet somit die Objektivität des Zufalls.

[16] Unter dem Begriff Probabilismus wird nach [BRO 06b] in der Erkenntnis- und der Wissenschaftstheorie die Auffassung verstanden, dass die menschliche Erkenntnis zu keiner absoluten Gewissheit, sondern nur einer mehr oder weniger großen Wahrscheinlichkeit fähig ist. Ein Probabilismus prägt auch Lehren, die von einer gewissen Indeterminiertheit der Natur ausgehen. In manchen Theorien (z.B. Kernphysik) wird er häufig zur Bezeichnung der Tatsache gebraucht, dass das Eintreten bestimmter Ereignisse mit einer gewissen Wahrscheinlichkeit prognostiziert werden kann.

Nachfolgend sollen nur einige wichtige Punkte hinsichtlich des Streitfalls zwischen Determinismus und Indeterminismus beleuchtet werden, da eine ausführliche Auseinandersetzung mit diesem Thema nicht Gegenstand der vorliegenden Arbeit ist. Hierfür wird auf die entsprechende Literatur, wie z.B. [PRO 08], verwiesen.

Im Rahmen von Risikoanalysen kann nach [KRÖ 10] noch feiner unterschieden zwischen

- deterministischen (postulierend),
- statistischen (rückschauend) und
- probabilistischen (prognostisch) Betrachtungsweisen.

Beim deterministischen Ansatz wird davon ausgegangen, dass Ereignisse durch Wirkungsketten durchgängig vorbestimmt sind. Es wird die Wirkung der angenommenen Ursachen analysiert. Die statistische Betrachtungsweise stützt sich auf Erfahrungsgesetze, welche aus einer großen Anzahl von gleichen Ergebnissen ableitbar sind. Die Beobachtungen richten sich dabei auf die System- bzw. Ereignisebene. Beim probabilistischen Ansatz werden Ereignisse und Ereignisketten im Voraus identifizierbar und durch Eintrittswahrscheinlichkeiten bestimmbar. Dabei werden Beobachtungen auf der Ebene von Komponenten genutzt.

Der Einzug probabilistischer Werte in die entsprechenden Regelwerke hat sowohl Vor- als auch Nachteile. Zunächst kann die Wirklichkeit durch probabilistische Betrachtungsweisen besser abgebildet werden. Nicht alle Sachverhalte lassen sich aufgrund von definierten Anfangs- und Randbedingungen wirklich vorherbestimmen und wenn doch, dann oftmals nur unter Idealbedingungen. Durch den Probabilismus können denkbare Zufälle sowie vorhandene Unsicherheiten berücksichtigt werden. Dadurch ist es möglich, über eine Vielzahl von Methoden wichtige Erkenntnisse über ein betrachtetes System zu erlangen, die über rein deterministische Untersuchungen nicht erkannt worden wären. So können über eine Fehlerbaumanalyse (FBA) beispielsweise mögliche Ausfallkombinationen identifiziert und somit Schwachstellen in einem System entdeckt werden. Über die Implementierung der Fuzzy-Logik[17] in eine solche FBA kann darüber hinaus z.B. die Tatsache berücksichtigt werden, dass die quantitativen Eingangsgrößen mit einer gewissen Unsicherheit behaftet sind. Weiterhin können probabilistische Ergebnisse miteinander verglichen und bewertet werden.

[17] Die Fuzzy-Logik (fuzzy = unscharf) bietet nach [Mey 10] die Möglichkeit der Verarbeitung von ungenauen oder unscharfen Informationen, wodurch beispielsweise Expertenwissen nutzbar gemacht und in bestehende Ansätze der Sicherheits- und Zuverlässigkeitsbewertung integriert werden kann.

Eine Schwierigkeit bei probabilistischen Angaben liegt in der oftmals unpräzisen oder schlicht nicht vorhandenen Definition der betrachteten Kenngrößen (vgl. Ausführungen zu Tabelle 3-2 und in [SCH 07a]), so dass eine Interpretation der Vorgaben schwierig wird. Weiterhin ist es möglich, dass allein aufgrund von Zahlenwerten ein Vertrauen in diese quantitativen Werte suggeriert wird. Hierzu sei folgendes Beispiel betrachtet: für eine chemische Anlage ist als normativer Grenzwert eine Störfallhäufigkeit von $4 \cdot 10^{-5} \frac{1}{a}$ festgelegt. Im Rahmen einer Risikoanalyse wurde ermittelt, dass die Anlage diesem Normwert genügt und ihn erfüllt. Nun kann obiger Wert als durchaus unwahrscheinlich eingeordnet werden – er drückt aus, dass wenn die Anlage das gesamte Jahr in Betrieb ist, es in ca. 25.000 Jahren zu einem ungewollten Ereignis, also zu einem Störfall kommt. Allerdings besagt dieser Wert nicht, wann es zu diesem Ereignis kommen wird. Der Störfall kann heute, morgen oder erst in 100 Jahren eintreten. Durch kleine quantitative Werte bei Risikofragen wird dem ungeschulten Betrachter immer eine gewisse „Scheinsicherheit“ vermittelt, die es eigentlich nicht gibt.

Hinsichtlich der Werte aus Tabelle 4-1 und Tabelle 4-2 mit den Größenordnungen 10^{-7} bis 10^{-9} für die beobachtbare Rate je Stunde ist auffällig, dass sie sehr strenge Vorgaben darstellen. Werden sie mit ähnlichen Parametern aus anderen Branchen und Industriezweigen verglichen, so fällt auf, dass sie das Niveau der Luftfahrtindustrie erreichen. In [SAE 96], einer systembezogenen Sicherheitsnorm für die zivile Luftfahrt, werden beispielsweise Angaben zu der Auswirkungsschwere von Fehlerzuständen in Bezug zu ihrer Auftretenswahrscheinlichkeit gemacht. Die SAE (Society of Automotive Engineers) ist eine globale Organisation aus Ingenieuren und Technikexperten aus den Bereichen Luftfahrt und Automobil, die in ihrer Geschichte eine Vielzahl von anerkannten Richtlinien herausgebracht hat. Für kritische Fehler mit katastrophalen Auswirkungen (Verlust des Flugzeugs mit vielen Toten) wird in [SAE 96] eine Ausfallwahrscheinlichkeit von 10^{-9} pro Flugstunde gefordert. Ein solcher Fehler darf folglich nur einmal innerhalb von einer Milliarde Flugstunden auftreten. Solche Fehler werden als sehr unwahrscheinlich bezeichnet. Ein gefährlicher Fehler hingegen (Unfall mit einigen Toten und Verletzten) darf mit einer maximalen Wahrscheinlichkeit von 10^{-7} pro Flugstunde auftreten. Diese Fehler werden als unwahrscheinlich beschrieben.

Dass die quantitativen Werte für den Automobilbereich in der gleichen Größenordnung liegen, ist nicht nachvollziehbar, vor allem unter dem Gesichtspunkt, dass die

Luftfahrtindustrie die geforderten Betriebsstunden aufgrund der dort herrschenden Flottenstärke mit entsprechenden Flugstunden durchaus nachweisen kann. Dies ist, wie im nächsten Abschnitt noch aufgezeigt wird, im Automobilbereich jedoch nicht möglich.

Um die in der ISO 26262 angegebenen Werte größenmäßig einordnen zu können, bietet sich ein Vergleich mit probabilistischen Risikoangaben aus anderen Bereichen an. Im Rahmen einer Risikobewertung wird anhand festgelegter Kriterien eine Entscheidung darüber herbeigeführt, ob das in der Risikoanalyse ermittelte vorhandene Risiko eingegangen werden kann oder ob es zu hoch ist. Es muss dabei nach [SFK 04] immer eine Abwägung zwischen dem einzugehenden Risiko und dem damit verbundenen Nutzen vorgenommen werden.
In den USA wird bei Risikobetrachtungen oftmals zwischen „de minimis risk“ und „de manifestis risk“ unterschieden. Das Konzept „de minimis risk“ charakterisiert nach [KOC 96] Risken, die als so gering eingestuft werden, dass weitere Maßnahmen zur Risikoreduzierung als uneffektiv angesehen werden. Solche Risiken sind als trivial und vernachlässigbar einzustufen. Bei der Betrachtung von Umwelt- und Gesundheitsrisiken werden dabei z.B. jährliche krebsinduzierte Todesfallrisiken in der Größenordnung von 10^{-4} bis 10^{-6} angewendet. „De manifestis“-Risiken hingegen sind so hoch, dass sie als offenkundig untragbar charakterisiert werden. Bei solchen Risiken sind Maßnahmen erforderlich und zwar unabhängig von den entstehenden Kosten. Der Schwellenwert hierfür liegt nach [SFK 04] bei $4 \cdot 10^{-4}$ pro Jahr.
Zum Thema Risiko von Kernkraftwerken hat in Großbritannien die Health and Safety Executive (HSE) in [HSE 92] das jährliche Todesfallrisiko (als Individualrisiko) von 10^{-6} (also 1 zu eine Million) als Schwelle festgelegt, bei welcher zusätzliche Kosten zur Risikovorsorge nicht mehr im Verhältnis zum Sicherheitszugewinn stehen. Ein jährliches Todesfallrisiko von 10^{-4} (also 1 zu 10.000) wird als nicht mehr vertretbares Risiko für die Öffentlichkeit definiert. Zwischen diesen beiden Schwellen befindet sich die ALARP[18]-Zone, in der abhängig vom vorliegenden Fall sowie unter Berücksichtigung von Kosten-Nutzen-Abwägungen ein vertretbares Risiko von der Aufsichtsbehörde festgelegt wird.
Auch in Deutschland spielten Fragen rund um die Sicherheit bei Kernkraftwerken seit den 1960er Jahren, als die ersten Kraftwerke entstanden, eine entscheidende Rolle. Im Kontext mit sicherheitstechnischen Überlegungen trat dabei auch das Risiko schwerer Unfälle in den Fokus. In Anlehnung an die Rasmussen-Studie (WASH-1400), die Ende der 1950er Jahre in

[18] As Low As Reasonably Practicable (so niedrig wie vernünftigerweise durchführbar)

den USA durchgeführt und 1975 veröffentlicht worden ist, bestand nach [grs 01] das Ziel der deutschen Risikostudie der Gesellschaft für Reaktorsicherheit (GRS) darin, die Risiken von Unfällen in deutschen Kernkraftwerken zu bewerten. Die Ergebnisse der Rasmussen-Studie sollten folglich auf die deutschen Verhältnisse angepasst werden. Die deutsche Studie war aufgeteilt in zwei Phasen. Die Phase A (die Ergebnisse wurden 1979 veröffentlicht) hatte nach [grs 01] das Ziel, das mit den Unfällen verbundene Risiko abzuschätzen, die Folgen eines Unfalls zu ermitteln und mit naturbedingten und zivilisatorischen Risiken zu vergleichen. Dabei war nicht nur die umfassende Herangehensweise neu, sondern insbesondere die Methode der probabilistischen Sicherheitsanalyse (PSA), welche erstmalig in Deutschland eingesetzt wurde und das Risiko konkret bezifferte. In der Phase B (die Ergebnisse wurden 1989 veröffentlicht) wurde sich der vertieften Untersuchung einzelner Problemstellungen und der methodischen Weiterentwicklung der PSA gewidmet. In [GRS 90] wurde als Ergebnis der Untersuchungen für den Druckwasserreaktor Biblis B, welcher der Studie als Referenzanlage diente, eine Wahrscheinlichkeit für einen Unfall mit Kernschmelze von $3{,}6 \cdot 10^{-6}$ pro Jahr ermittelt, was als sehr gering eingeschätzt wurde. Dies entspricht nach [grs 01] in etwa einem Unfall alle 280.000 Betriebsjahre.
Im Jahr 2001 veröffentlichte die GRS[19] in [GRS 01] eine neue Studie zur Bewertung des Unfallrisikos bei Druckwasserreaktoren. Als Ergebnis wurde die Summenhäufigkeit von Kernschadenszuständen präsentiert, welche deutlich unter 10^{-5} pro Jahr liegt.
Neben aller Kritik, die an den vorgestellten Studien geübt worden ist, stellen die zuvor genannten Werte das von der Politik und der Gesellschaft akzeptierte Risiko hinsichtlich eines Störfalls bei den entsprechenden Kraftwerken dar.

Der Vergleich der schärfsten Vorgaben der ISO 26262 aus den Tabellen 4-1 und 4-2 mit der Größenordnung 10^{-9} pro Stunde bzw. 10^{-7} pro Jahr mit den oben angegebenen Risikowerten erlaubt die Aussage, dass die ISO-Vorgaben als sehr streng und fast schon unverhältnismäßig einzustufen sind.

4.4.5 Quantitativer Nachweis

In Abschnitt 4.4.2 wurden die Schwierigkeiten beim „qualitativen Nachweis“ nach Normvorgaben hinsichtlich der Betriebsbewährtheit dargestellt. Nachfolgend wird auf den „quantitativen Nachweis“ eingegangen. Hierzu soll zunächst ein fiktiver Beispielkandidat

[19] Heutzutage steht GRS für Gesellschaft für Anlagen- und Reaktorsicherheit mbH.

betrachtet werden, dessen sicherheitsrelevante Funktion mit einem ASIL B als Ergebnis einer durchgeführten G+R bewertet worden ist. Anhand von vorhandenen Felddaten für den Kandidaten sind zehn Ereignisse identifiziert worden, welche das Potential zur Verletzung des abgeleiteten Sicherheitsziels haben. Für die minimale Betriebszeit bedeutet dies nach Gleichung (4-1) der ISO 26262:

$$T = \frac{1}{10^{-8}\frac{1}{h}} \cdot \frac{\chi^2_{0,7;2\cdot 10+2}}{2} = 10^8\,h \cdot \frac{\chi^2_{0,7;22}}{2} = 1{,}247 \cdot 10^9\,h\,.$$

Es müssen also knapp 1,25 Milliarden Betriebsstunden nachgewiesen werden, um den Betriebsbewährtheitsnachweis zu erlangen.

Um die Problematik zu verdeutlichen, wird nun ein fiktives elektronisches Beispielsystem betrachtet, dessen sicherheitsrelevante Funktion mit einem ASIL D eingestuft worden ist. Anhand der Felddaten ist ein einziges Ereignis identifiziert worden, welches das Potential zur Verletzung des Sicherheitsziels hat. Für die minimale Betriebszeit bedeutet dies nach Gleichung (4-1) der ISO 26262:

$$T = \frac{1}{10^{-9}\frac{1}{h}} \cdot \frac{\chi^2_{0,7;2\cdot 1+2}}{2} = 10^9\,h \cdot \frac{\chi^2_{0,7;4}}{2} = 2{,}439 \cdot 10^9\,h\,.$$

In diesem Fall müssen sogar fast 2,44 Milliarden Betriebsstunden nachgewiesen werden. Dieses fiktive Beispielsystem, dessen Funktion mit ASIL D bewertet worden ist, möge nun in einer Baureihe verbaut sein, welche ein konstantes monatliches Fertigungsvolumen von 30.000 Fahrzeugen aufweist (es sei darauf hingewiesen, dass diese monatliche Produktionszahl für die Automobilindustrie als utopisch einzustufen ist, da es sehr wenige bis keine Baureihen geben wird, die ein solches Fertigungsvolumen haben). Weiterhin wird berücksichtigt, dass dem Hersteller nur während der Garantiezeit von zwei Jahren Informationen aus dem Feld zu den produzierten Fahrzeugen zur Verfügung stehen. Außerdem wird eine jährliche Betriebszeit von 400 Stunden angenommen. Als Ergebnis dieser Überlegungen stellt sich heraus, dass selbst für eine solche großvolumige Baureihe die normativ geforderte minimale Betriebszeit erst nach 76 Produktionsmonaten, also nach mehr als sechs Produktionsjahren erreicht wird.

Bei Verwendung einer jährlichen Betriebsdauer von 500 Stunden, wie z.B. in dem Zuverlässigkeitsstandard RDF 2000 [UTE 00], einem französischen Zuverlässigkeits-berechnungsstandard für elektronische Systeme, angegeben, und demselben

Fertigungsvolumen wie zuvor würde die geforderte Betriebszeit nach 63 Produktionsmonaten erreicht werden.
Als letztes Extrembeispiel könnte noch die Annahme getroffen werden, dass ein Fahrzeug das komplette Jahr in Betrieb ist, also 8.760 Stunden. Dies ist selbstverständlich eine von der Praxis losgelöste Annahme, da es kein Fahrzeug gibt, welches 24 Stunden am Tag und 365 Tage im Jahr in Betrieb ist. Dies stellt aber den maximal möglichen Betrachtungszeitraum dar. Als Ergebnis hierfür ergibt sich, dass die minimale Betriebszeit bei einem konstanten monatlichen Produktionsvolumen von 30.000 Fahrzeugen nach acht Produktionsmonaten erreicht werden würde.

Als Fazit der zuvor aufgeführten einfachen Beispielbetrachtungen muss festgehalten werden, dass der PiU-Nachweis über die in der Norm angegebenen Grenzwerte für Betrachtungsgegenstände von kleinvolumigen Kollektiven (Baureihen) praktisch nicht zu erfüllen sind. Selbst für großvolumige Baureihen (oder die Summe vieler kleiner Baureihen) kann ein Nachweis für wenige sicherheitskritische Ereignisse des Kandidaten erst nach einer sehr langen Produktionszeit erbracht werden. Dies ist zwar immer abhängig von der ASIL-Einstufung sowie den identifizierten Ereignissen, aber die Schwierigkeiten beim Nachweis bleiben unabhängig davon bestehen. Infolgedessen müssen die in der Norm angegebenen Grenzwerte in Frage gestellt werden. Damit zusammenhängend muss die Vorgehensweise über die Bestimmung der minimalen Betriebszeit als nicht zielführend für den Einsatz in der Praxis angesehen werden.

Zusammenfassend kann anhand der Bewertungen und Interpretationen zum qualitativen und quantitativen Nachweis festgehalten werden, dass die darin gewonnenen Erkenntnisse sowohl aus praxisnaher als auch aus wissenschaftlicher Sicht zu der Notwendigkeit einer alternativen Vorgehensweise für eine PiU-Argumentation (im Gegensatz zur Bestimmung der minimalen Betriebszeit) führen, die das reale Ereignisverhalten im Feld berücksichtigt. Darüber hinaus gilt es, alternative und vor allem realitätsnahe Bewertungskriterien (im Gegensatz zu den konstanten Ereignisraten mit sehr strengen Werten) abzuleiten. Diese Punkte werden im folgenden Kapitel berücksichtigt, in welchem ein alternativer Vorschlag erarbeitet wird.

5 Alternative Vorgehensweise für eine PiU-Argumentation

In den vorherigen Abschnitten wurde die Notwendigkeit für die Entwicklung einer neuen Vorgehensweise bei einem automotiven Betriebsbewährtheitsnachweis aufgezeigt. An den neuen Ansatz, der nachfolgend zunächst allgemein beschrieben und erläutert wird, werden folgende Anforderungen gestellt:

- Einsetzbarkeit in der Praxis,
- konkrete Untersuchung des realen Betriebsverhaltens des Kandidaten im Feld und
- Entwicklung individueller Bewertungskriterien für die neuartige PiU-Argumentation.

Im anschließenden Kapitel 6 wird die neue Vorgehensweise auf ein konkretes Beispiel aus der Automobilindustrie angewendet.

5.1 Generelle Schrittfolge einer PiU-Argumentation

Ein Betriebsbewährtheitsnachweis kann prinzipiell auf alle Elemente eines zu entwickelnden Produkts in der Automobilindustrie angewendet werden. Deren Definition und Betriebsbedingungen müssen jedoch identisch sein zu einem bereits freigegebenen und im Einsatz befindlichen Element oder einen hohen Grad an Übereinstimmung mit diesem haben. Es kann sich dabei sowohl um ein Gesamtsystem oder eine Gesamtfunktion als auch ein Teilsystem bzw. einen Betrachtungsgegenstand handeln. Betrachtungsgegenstand in diesem Kontext kann ein System, eine Funktion, eine HW-Komponente, eine SW-Komponente etc. sein. Der jeweilige Umfang wird wie in der ISO 26262 „Kandidat“ genannt.

Der generelle Ablauf einer PiU-Argumentation ist in nachfolgendem Bild 5-1 dargestellt.

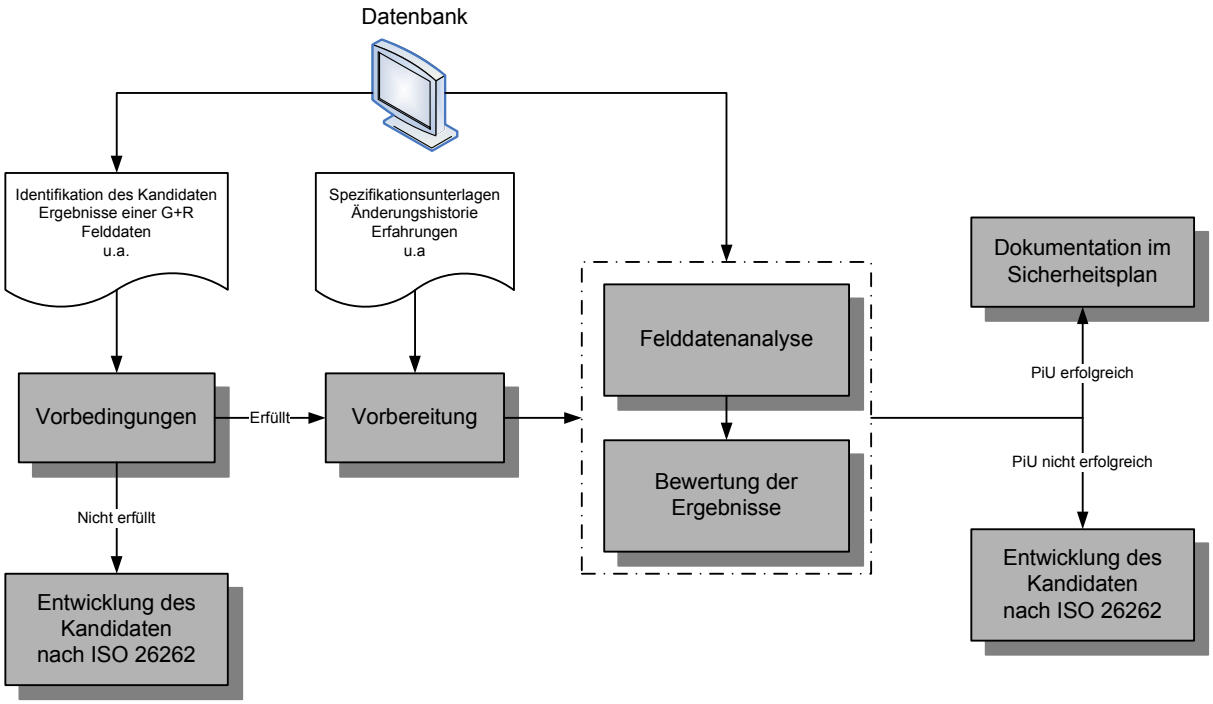


Bild 5-1: Genereller Ablauf einer PiU-Argumentation

Wie in obiger Abbildung 5-1 zu erkennen, müssen zunächst einige Vorbedingungen erfüllt sein. Sind diese nicht alle erfüllt, so kann eine PiU-Argumentation nicht durchgeführt werden, und der Kandidat muss „normal“ nach den Vorgaben der ISO 26262 entwickelt werden. Sind die Vorbedingungen erfüllt, erfolgt der Nachweis der Betriebsbewährtheit in den Schritten

- Vorbereitung,
- Analyse der Felddaten und Bewertung der Ergebnisse und
- Konsequenz aus der Bewertung der Ergebnisse der Felddatenanalyse.

Die Ergebnisse der Felddatenanalyse müssen mit entsprechenden Bewertungskriterien verglichen werden. Werden diese Kriterien eingehalten, so ist die PiU-Argumentation erfolgreich. Dies muss entsprechend im Sicherheitsplan[20] (original: Safety Plan) des Betrachtungsgegenstandes dokumentiert werden. Werden die Kriterien nicht eingehalten, so ist die PiU-Argumentation nicht erfolgreich und der Kandidat muss nach den Vorgaben der ISO 26262 entwickelt werden.

Die zuvor angesprochenen einzelnen Schritte der neuen Vorgehensweise werden in den folgenden Abschnitten detaillierter erläutert.

[20] Der Sicherheitsplan ist eine Informationsquelle nach ISO 26262 zur Steuerung und Unterstützung der Sicherheitsaktivitäten eines Projektes. Seine Zielsetzung besteht in der Sicherstellung, dass der entwickelte Kandidat alle Sicherheitsanforderungen erfüllt [LÖW 10].

5.2 Vorbedingungen

Um einen Kandidaten hinsichtlich seiner Betriebsbewährtheit zu untersuchen, müssen zunächst einige Vorbedingungen erfüllt sein, ohne die eine PiU-Argumentation nicht durchgeführt werden kann. Es handelt sich dabei um

- Identifikation des Kandidaten:

  Um einen Nachweis nach ISO 26262 überhaupt durchführen zu können, muss es sich bei dem Betrachtungsgegenstand um einen Kandidaten handeln, der in einem sicherheitsbezogenen E/E-System implementiert ist. Der Kandidat muss weiterhin klar identifiziert und abgegrenzt sein. Hierzu gehört nicht nur die alleinige Festlegung des Betrachtungsgegenstandes, sondern es müssen auch weitere Punkte berücksichtigt werden, wie eine mögliche Abgrenzung hinsichtlich einer relevanten Version des Kandidaten sowie die Identifikation der relevanten Baureihe(n) und Fahrzeugmodelle. So ist es möglich, dass ein Kandidat unter gleichen Bedingungen und ohne Änderungen in mehreren Modellen der gleichen Baureihe und sogar in unterschiedlichen Baureihen verbaut ist.

- Ergebnisse einer Gefährdungsanalyse und Risikobewertung für den Kandidaten:

  Für den Kandidaten muss eine G+R durchgeführt worden sein, so dass die dabei ermittelten Sicherheitsziele als Ergebnis der Untersuchung vorliegen.

- Felddaten vom Kandidaten:

  Für die PiU-Argumentation sind die Ereignisse relevant, die zu einer Verletzung eines Sicherheitsziels führen können. Diese Ereignisse müssen also für den Kandidaten anhand von Feld- und Einsatzdaten erkannt werden, die eine solche Identifizierung vom Inhalt und Umfang her zulassen. Die Automobilindustrie und insbesondere die Hersteller verfügen, wie bereits erwähnt, über umfangreiche und strukturierte Datenbanksysteme, in denen eine Vielzahl von unterschiedlichen Informationen dargestellt, teilweise gebündelt und sogar ausgewertet werden können. Die Informationen umfassen dabei Daten aus den unterschiedlichsten Bereichen, wie z.B.

  - Garantie- und Kulanz (GuK),
  - Diagnosebewährung,
  - Fahrzeugerprobung und
  - Test- und Prüfdurchführung.

  Insbesondere die Informationen aus dem Bereich der Garantie und Kulanz sowie aus der Diagnosebewährung sind für den Einsatz in einer PiU-Argumentation interessant, da sie das reale Verhalten eines Fahrzeugs und dessen Systeme, Komponenten und

Funktionen im tatsächlichen Betrieb wiedergeben. Manche Hersteller verfügen sogar über Datenbanken, die selektive Fahrzeuginformationen aus dem Zeitraum nach Ende der Garantiezeit beinhalten, die ebenfalls für die Betriebsbewährung relevant sein können. Weiterhin ist es möglich, dass Qualitätsinformationen zu bestimmten Komponenten und Systemen vorliegen, die darüber hinaus in die Untersuchung miteinbezogen werden können. Hiermit sind beispielsweise Datenbanken gemeint, die nur Fehler zu einzelnen Steuergeräten oder Steuergerätegruppen beinhalten.

Auf den Komplex der Datenbanken sowie die damit zusammenhängenden Schwierigkeiten wird in Abschnitt 5.4.1 genauer eingegangen.

Die PiU-relevanten Ereignisse müssen in den entsprechenden Datenbanken herausgefiltert und eventuell miteinander verknüpft werden (s. Abschnitt 5.4.1.4), so dass eine sicherheitstechnische Untersuchung dieser Datensätze möglich ist.

5.3 Vorbereitung

Sind die Vorbedingungen erfüllt, folgt in einem ersten Schritt die Vorbereitung für die PiU-Argumentation. Diese umfasst die Sammlung und Durchsicht erforderlicher Informationen des Kandidaten, anhand derer ein möglichst umfassendes Bild über die Funktionsweise, die Einsatzbedingungen usw. erlangt werden soll. Hierzu zählen u.a. die nachfolgenden Dokumente, sofern sie vorhanden sind:

- Spezifikationsdokumente:

  Hierzu gehören Funktionsdefinitionen, Entwicklungsunterlagen zu den Grenzen, Schnittstellen, Überwachungsmöglichkeiten, Konfigurationsparametern etc.
- Einsatzdefinitionen:

  Hierin sollten Informationen zu Nutzungsprofilen, Umgebungsbedingungen, Einsatzbeschränkungen etc. vorhanden sein.
- Informationen zur Änderungshistorie:

  Eine Grundvoraussetzung für den Betriebsbewährtheitsnachweis ist, dass für den Betrachtungsgegenstand eine gültige Spezifikation vorliegt. Diese darf während des Betrachtungszeitraums nicht verändert werden. An der Betrachtungseinheit selbst dürfen nur geringe bzw. nicht-einflussreiche Änderungen vorgenommen werden. Zu diesen muss eine genaue Dokumentation vorliegen und deren Einfluss muss analysiert werden.

- Erfahrungen zum Kandidaten:

  Zum Betrachtungsgegenstand sollten bereits Erfahrungen hinsichtlich möglicher Fehler und Ausfälle im Feld vorliegen. Er sollte also beispielsweise in einer Baureihe verbaut sein, bei der die Garantiezeit bereits abgelaufen ist, so dass bereits aufgrund von Untersuchungen Kenntnisse zum Ausfallverhalten und dessen Ursachen vorliegen.

5.4 Felddatenanalyse

Nach der PiU-Vorbereitung erfolgt die Analyse der Felddaten, die zuvor aus den Datenbanken gewonnen wurden. Dieser Komplex stellt das Kernstück des Betriebsbewährtheitsnachweises dar. Er ist in nachfolgender Abbildung 5-2 schematisch dargestellt.

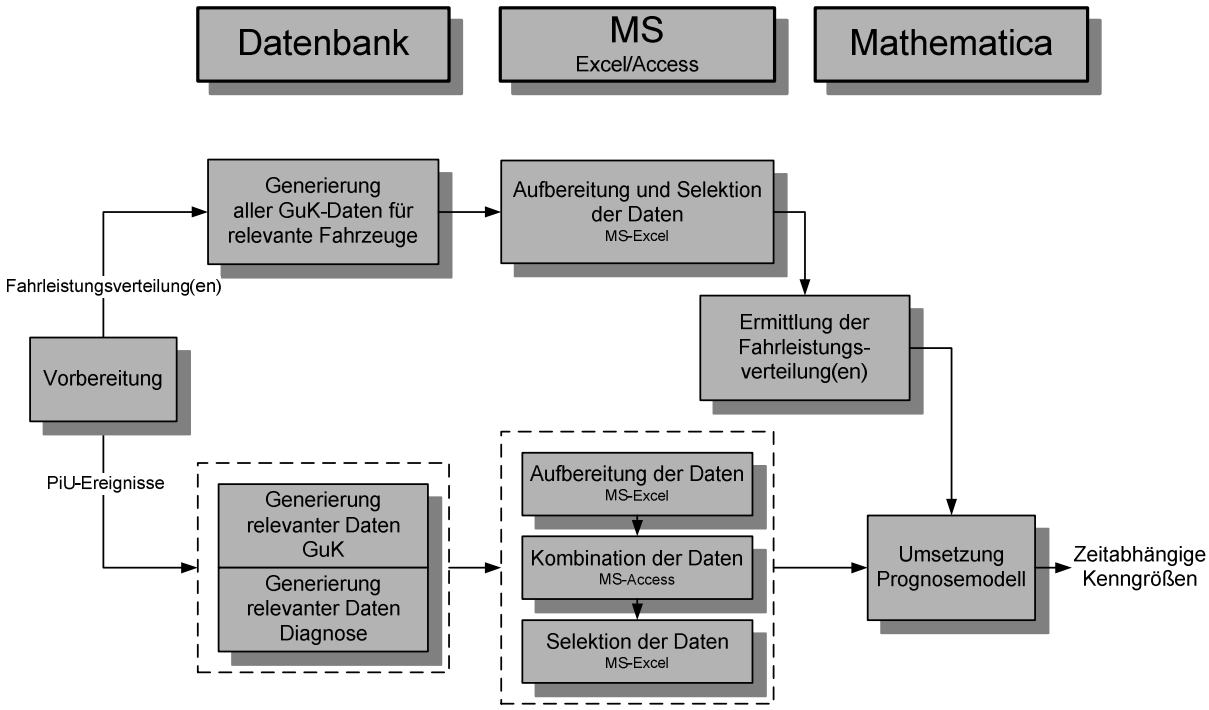


Bild 5-2: Felddatenanalyse bei einer PiU-Argumentation

In Bild 5-2 ist zu erkennen, dass im Anschluss an die bereits beschriebenen, vorbereitenden Schritte die zweigeteilte Datenanalyse erfolgt. Diese umfasst die beiden Pfade

- Fahrleistungsverteilung(en) (oberer Pfad) und
- PiU-Ereignisse (unterer Pfad).

Diese beiden Pfade und die darin erforderlichen Arbeitsschritte werden in den Abschnitten 5.4.2 und 5.4.3 genauer erläutert. An dieser Stelle soll jedoch noch kurz auf die in Bild 5-2 befindlichen Tools eingegangen werden. Hierbei stellen

- Datenbank,
- MS[21] und
- Mathematica®

die in den jeweiligen Arbeitsschritten anzuwendenden Werkzeuge bzw. Hilfsmittel dar. So können die für die PiU-Untersuchung relevanten Daten nur in einer entsprechenden automobilspezifischen Datenbank gefunden werden. Nach einem entsprechenden Export können die Aufbereitung und Selektion dieser Daten in Tools wie MS-Excel® und MS-Access® erfolgen. Für die letztendliche Analyse der Daten ist eine spezielle Software erforderlich, da dort komplexe Berechnungsschritte durchgeführt werden, die in Standard-Softwarewerkzeugen nicht durchführbar sind. Eine solche Spezialsoftware ist Mathematica® von Wolfram Research, welche ein mathematisch-naturwissenschaftliches Softwarepaket darstellt.

Die Angabe der Tools hat keinen Anspruch auf Vollständigkeit – die Tools sind vielmehr als Beispiele anzusehen. Es ist daher möglich, dass z.B. die Kombination der Daten mit anderen Softwareprodukten, wie z.B. MySQL, ebenfalls durchzuführen ist. Im Rahmen der vorliegenden Arbeit wurden allerdings die genannten SW-Werkzeuge verwendet.

5.4.1 Der Komplex Felddaten

Wie zuvor erwähnt, basiert die gesamte PiU-Argumentation auf der Beschaffung und Auswertung von Felddaten zu einem Kandidaten, die das reale Betriebsverhalten widerspiegeln. Nachfolgend werden mögliche Probleme sowie daraus abgeleitete Mindestanforderungen und Empfehlungen an den Komplex der Felddaten gestellt, wobei folgende Merkmale berücksichtigt werden:

- Datenumfang,
- Datenqualität,
- Datenexport und
- Datenkombination.

[21] MS steht für Microsoft®. Einige Office-Produkte, die heutzutage Standard sind, können im Rahmen der Arbeitsschritte verwendet werden, wie z.B. MS-Excel® und MS-Access®.

An dieser Stelle muss zunächst festgehalten werden, dass viele Datenbanken in der Automobilindustrie ihren Fokus nicht auf sicherheits- und zuverlässigkeitstechnischen Gesichtspunkten haben, sondern auf betriebswirtschaftlichen, insbesondere finanziellen Aspekten. So sind Garantiedatenbanken bei den OEM primär darauf ausgerichtet, den Kostenkreislauf zwischen Hersteller und Vertragswerkstatt zu koordinieren. Dennoch enthalten diese Datenbanken auch Informationen zu Garantiefällen, die für Sicherheits- und Zuverlässigkeitsbetrachtungen nützlich sind.

5.4.1.1 Datenumfang

Da im Rahmen der vorliegenden Arbeit das Wuppertaler Prognosemodell verwendet wird, sind einige Daten bzw. Informationen aus einer solchen Garantiedatenbank notwendig bzw. hilfreich. Es handelt sich hierbei um die in nachfolgender Tabelle 5-1 dargestellten Informationen.

Tabelle 5-1: Daten für den Einsatz im Wuppertaler Prognosemodell

Daten
Fertigungsdatum des Fahrzeugs • Berücksichtigung des Zulassungsverzugs
Erstzulassungsdatum des Fahrzeugs
Ausfalldatum der Schadenskomponente
Reparaturdatum des Schadens am Fahrzeug
Erfassungsdatum des Schadens in der Datenbank • Berücksichtigung des Meldeverzugs
Kilometerstand beim Schadenseintritt
Fertigungsmenge für den Betrachtungszeitraum
Verkaufsmenge für den Betrachtungszeitraum
Typteile- bzw. Bauteilnummer der Schadenskomponente
Fehlercode oder Schadensnummer

Weitere Erläuterungen zum Modell selbst und zu den Daten sind in Abschnitt 5.4.3.1 enthalten. Es ist möglich, dass einige der in obiger Tabelle 5-1 enthaltenen Informationen nicht in den Datenbanken vorhanden sind, wie z.B. das konkrete Eintrittsdatum eines Schadens/Fehlers/Ausfalls oder die genaue Verkaufsmenge in einem Betrachtungszeitraum. Auf die unterschiedlichen und vielschichtigen Gründe hierfür soll an dieser Stelle nicht

eingegangen werden. Das Fehlen dieser Informationen muss nicht bedeuten, dass die Daten ungeeignet sind. Vielmehr ist es oftmals möglich, fehlende Angaben durch andere Informationen zu substituieren. Anstelle der Verkaufsmenge kann die Fertigungsmenge für den Betrachtungszeitraum verwendet werden. Anstelle des konkreten Ausfalldatums ist es möglich, das Reparaturdatum am Fahrzeug zu nutzen – gleiches gilt für den Kilometerstand bei Schadenseintritt, der durch den Reparatur-Kilometerstand ersetzt werden kann. Durch solche Substitutionen gelangen in der Regel gewisse Ungenauigkeiten in das Modell, die es individuell abzuschätzen und zu bewerten gilt. So wird z.B. eine Fertigungsmenge in einem bestimmten Zeitraum in der Regel größer sein als die Verkaufsmenge im gleichen Zeitraum. Die Grundgesamtheit, die im Modell verwendet wird, ist folglich immer etwas größer als die eigentlich zu verwendende. Dadurch werden die untersuchten Ereignisse im Regelfall zu positiv bewertet.

5.4.1.2 Datenqualität

Die Qualität der Daten kann sehr unterschiedlich sein. Im Folgenden werden einige häufig beobachtete Fehlertypen exemplarisch dargestellt.

Unvollständige Datensätze

Unter „unvollständigen Datensätzen“ sind solche zu verstehen, in denen eine Information, wie z.B. das Erstzulassungsdatum eines Fahrzeugs, nicht eingetragen ist. Eine Möglichkeit, wie es zum Fehlen solcher Daten kommt, ist, dass einige Informationen manuell während eines Werkstattaufenthaltes eingetragen werden. Das bedeutet, dass ein Mitarbeiter es z.B. unterlässt, eine Information einzutragen und der Datensatz zu der Reparatur somit unvollständig ist. Eine Möglichkeit, das Problem unvollständiger Datensätze zu beheben, besteht in Überprüfungen bei der Eingabe der Daten. Fehlt eine entsprechende Eingabe, so kann beispielsweise eine entsprechende Mitteilung am Eingabegerät erscheinen.

Unplausible Datensätze

„Unplausibel“ sind Datensätze, bei denen eine Fehleingabe vorliegen muss, da die Informationen nicht zueinander passen bzw. eine Angabe nicht schlüssig gegenüber anderen ist oder ein Eintrag des Datensatzes selbst nicht plausibel ist. Beispiele hierfür sind:

- Falscher Kilometerstand:

  Je nachdem, in welchem Land ein Datensatz erhoben wird, herrschen unterschiedliche Schreibweisen für Zahlenangaben. So wird beispielsweise in Nordamerika, Großbritannien sowie großen Teilen Asiens ein Punkt als Dezimaltrennzeichen verwendet, wohingegen im Rest von Europa und Südamerika eine Dezimalzahl mit einem Komma geschrieben wird. Beim Tausendertrennzeichen verhält es sich dagegen genau umgekehrt. So kann es sein, dass die Kilometerangabe 123,456 km in Deutschland eine andere Zahl darstellt als in den USA – der amerikanische Wert ist nämlich genau tausendmal so groß. Werden solche Gegebenheiten nicht beachtet, kann es zu Fehlern kommen, sofern die Eingabe nicht überprüft wird.

  Darüber hinaus ist es denkbar, dass eine Eingabe in Tkm (Tausendkilometer) gefordert wird. Beträgt der Kilometerstand 11.111 km und wird diese Zahl so eingetragen, bedeutet dies, dass fälschlicherweise 11.111.000 km eingegeben wurden. Es hätten 11,111 Tkm verwendet werden müssen, um den Wert 11.111 km korrekt darzustellen.

- Falsche Datumseingabe:

  Auch bei den Angaben eines Datums herrschen in verschiedenen Ländern unterschiedliche Schreibweisen. Einige Beispiele für Datumsformate sind

  - Tag/Monat/Jahr, wie z.B. in Deutschland,
  - Monat/Tag/Jahr, wie z.B. in den USA und
  - Jahr/Monat/Tag, wie z.B. in China.

  In manchen Ländern werden sogar mehrere Datumsformate verwendet. Auch diese Gegebenheiten gilt es zu berücksichtigen, da es ansonsten zu Fehleinträgen oder Fehlinterpretationen und somit zu falschen Datumsangaben für die weitere Analyse kommen kann.

- Unplausible Datumsangaben:

  Zuvor genannte falsche, aber auch vertauschte Datumsangaben können zu unplausiblen Datensätzen führen. Hier ist eine Reihe von Möglichkeiten zu nennen, wie z.B.

  - Erstzulassungsdatum liegt vor dem Produktionsdatum,
  - Reparaturdatum liegt vor dem Produktionsdatum,

- Anerkennungsdatum liegt vor dem Reparaturdatum oder
- Reparaturdatum liegt vor dem Erstzulassungsdatum.

Weiterhin können Datensätze unplausibel sein, wenn eine unglaubhafte Fahrleistung vorliegt. Wenn ein Fahrzeug beispielsweise einen Monat nach der Erstzulassung zu seinem ersten Werkstattbesuch gebracht wird und eine Fahrleistung von 90.000 km aufweist, kann mit der Angabe etwas nicht stimmen. Um eine solche Kilometerleistung zu realisieren, müsste das Fahrzeug jeden Tag 3.000 km gefahren sein. Dies erscheint für den normalen Gebrauch unrealistisch, da dies eine Durchschnittsgeschwindigkeit von $125\frac{km}{h}$ erfordern würde.

Hilfreich wären für die oben aufgeführten Punkte Überprüfungen der Daten auf Plausibilität direkt bei der Eingabe, so dass es zu solchen Fehleinträgen nicht kommen kann. Hierfür gilt allerdings, dass die einzelnen Arbeitsschritte und Prozesse bei der Dateneingabe für die Erarbeitung von konkreten Lösungsvorschlägen genau analysiert werden müssen.

Unplausible Datensätze sind während einer Analyse herauszufiltern und aus den weiteren Betrachtungen auszuschließen, da nicht nachvollzogen werden kann, ob es sich z.B. um vertauschte oder falsch eingetragene Angaben handelt. Aufgrund von Erfahrungswerten kann es nach [ALT 09a] durchaus vorkommen, dass bis zu 20% der eingetragenen Daten infolge von Fehleinträgen nicht verwertbar sind.

5.4.1.3 Datenexport

Je nachdem, in welchem Tool die weiteren Berechnungsschritte durchgeführt werden, muss die Datenbank einen Export in verschiedene Dateiformate zulassen. Die exportierten Dateien sind nach dem Export direkt auf ihre Korrektheit zu überprüfen, da auch während des Exportvorgangs Fehler passieren können und beispielsweise nicht der gesamte gewollte Umfang exportiert wird.

5.4.1.4 Datenkombination

Für den Betriebsbewährtheitsnachweis müssen die Ereignisse eines Kandidaten identifiziert werden, welche das Potential besitzen, ein dem Kandidaten zugeordnetes Sicherheitsziel (als Ergebnis einer G+R) zu verletzen. Um genau diese Ereignisse zu erkennen und zu finden, kann es möglich sein, dass die alleinige Betrachtung der Informationen aus einer einzigen Datenbank (z.B. mit Garantie- und Kulanzdaten) nicht ausreicht. In der Regel werden die Fehlerarten und Fehlerorte von schadhaften Komponenten in einer solchen GuK-Datenbank mit alphanumerischen Zeichenfolgen verschlüsselt dargestellt. Je nachdem, wie spezifisch ein relevantes PiU-Ereignis definiert worden ist, kann es sein, dass die zur Verfügung stehenden Fehlerarten und deren Beschreibungen nicht ausreichend sind, um die Ereignisse klar zu identifizieren. Wenn z.B. nur ein ganz bestimmter Sensorfehler als relevant gilt, anhand der GuK-Daten aber „nur“ zwischen

- elektrischem Fehler,
- Kurzschluss,
- Unterbrechung und
- schadhafter Komponente

unterschieden werden kann, sind diese Fehlerbeschreibungen für eine PiU-Argumentation nicht befriedigend. In einem solchen Fall wird es erforderlich sein, zusätzliche Informationen aus anderen Datenquellen heranzuziehen.

Eine mögliche Quelle ist die Diagnosebewährung. In einer solchen Datenbank sind Ereignisse enthalten, die beim Anschluss des Fahrzeuges an ein Diagnosegerät in einer Vertragswerkstatt aufgenommen werden. Hierbei ist es üblich, dass die Fehlerspeicher der unterschiedlichen Steuergeräte ausgelesen werden. Jedem Steuergerät ist beispielsweise eine Vielzahl von Fehlercodierungen zugeordnet, die Aufschluss über Fehlfunktionen von Fahrzeugkomponenten gibt. Aufgrund der aus dem Fehlerspeicher entnommenen Einträge kann untersucht werden, welche Fehler an dem Fahrzeug vorliegen.

Eine alleinige Auswertung der GuK-Daten kann, wie bereits beschrieben, nicht ausreichen. Eine gesonderte Analyse der Daten aus der Diagnosebewährung kann ebenfalls nicht zielführend sein, da nicht jeder Diagnoseeintrag automatisch einen wirklichen Fehlereintrag repräsentieren muss. Es ist denkbar, dass ein Fahrzeug während eines Werkstattaufenthalts aufgrund von Reparaturarbeiten mehrmals an ein Diagnosegerät angeschlossen wird und dabei Fehlercodierungen mehrfach auftreten. Weiterhin ist es möglich, dass während der

Reparaturarbeiten an einem Fahrzeug Fehler über die Diagnose detektiert werden, die nach Abschluss der Reparatur nicht mehr vorhanden sind.

Es kann somit erforderlich sein, eine Entscheidungsmöglichkeit zu finden, welche der gefundenen Ereignisse wirklich sicherheitsrelevant gewesen sind. In dem Fall müssen beide Datenmengen (GuK und Diagnose) unter Umständen miteinander kombiniert werden, um diejenigen Ereignisse zu identifizieren, die für die PiU-Argumentation relevant sind. Diese Kombination kann in der entsprechenden Datenbank selbst erfolgen, sofern beide Datenmengen in der Datenbank vorhanden sind. Wenn nicht, muss die Kombination in anderen Tools durchgeführt werden.

Um eine eindeutige Zuordnung der Datensätze aus den unterschiedlichen Bereichen zu ermöglichen, müssen Informationen innerhalb der Datensätze gefunden werden, die eindeutig und vor allem in allen Bereichen identisch sind. Dadurch wird bei der Datenkombination gewährleistet, dass es sich bei den Datensätzen aus den Bereichen um Einträge desselben Fahrzeugs handelt. Eine solche Information ist die Fahrzeugidentifizierungsnummer (FIN, früher: Fahrgestellnummer), anhand derer ein Fahrzeug eindeutig identifizierbar ist, da jede FIN weltweit nur ein einziges Mal vorhanden ist. Dabei handelt es sich um einen international genormten, 17-stelligen alphanumerischen Code. Dieser besteht nach [wik 03] aus

- der Herstellererkennung,
- einem herstellerspezifischen Schlüssel und
- einer fortlaufenden Nummerierung.

In Abbildung 5-3 ist der Aufbau der Fahrzeugidentifizierungsnummer dargestellt.

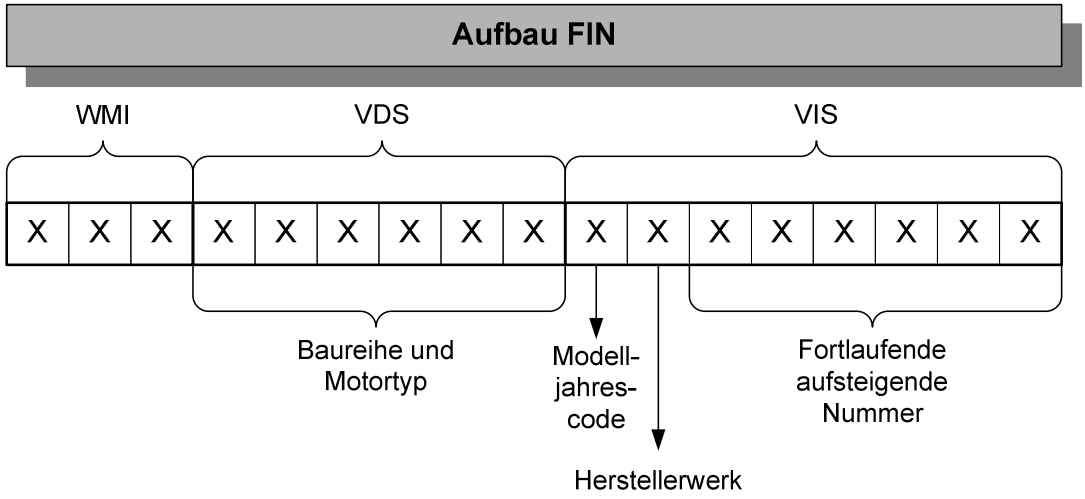


Bild 5-3: Aufbau der Fahrzeugidentifizierungsnummer

Es gibt zwei verschiedene Systeme für die FIN: Hersteller aus der Europäischen Union müssen die Norm ISO 3779 erfüllen, wohingegen Hersteller aus Nordamerika ein anderes, aber der ISO-Norm konformes System verwenden. Bei beiden Systemen ist übrigens die Verwendung der Großbuchstaben I, O und Q verboten, da eine zu große Verwechselungsgefahr mit den Ziffern 0 und 1 besteht. In obigem Bild 5-3 ist der Aufbau der europäischen FIN dargestellt. Wie darin zu erkennen, stellen die ersten drei Stellen den Welt-Hersteller-Code (World Manufacturer Identification, WMI) dar. Die Buchstaben WDB stehen hierbei beispielsweise für die Daimler AG, WOL für Opel und WVW für Volkswagen. Die nächsten sechs Stellen bieten Platz für eine herstellerspezifische Verschlüsselung (Vehicle Description Section, VDS), die vom Hersteller festgelegt werden kann. Darin werden die Baureihe sowie der Motortyp gekennzeichnet. In den Stellen 10 bis 17 (Vehicle Indicator Section, VIS) der FIN sind der Modelljahrescode, das Herstellerwerk und eine fortlaufende Nummerierung enthalten.

Zu den zuvor stehenden Anmerkungen ist festzuhalten, dass die in den Datenbanken enthaltenen GuK- und Diagnoseereignisse unter Umständen nicht vollständig sind. Es werden in den Datenbanken nur solche Fälle hinterlegt, bei denen ein Fahrzeugführer in eine Vertragswerkstatt gefahren ist, um einen Schaden oder Fehler an seinem Fahrzeug beheben zu lassen. Hat ein Kunde einen für die PiU-Argumentation relevanten Fehler erlitten und ist in eine Nicht-Vertragswerkstatt gefahren, so ist dieser Fall nicht in der Datenbank des Herstellers enthalten. Außerdem ist es möglich, dass die enthaltenen Schadensfälle nicht korrekt sind, z.B. wenn in einer Vertragswerkstatt eine Schadenskomponente falsch identifiziert worden ist. Auch diese Fehler sind vom OEM nur schwer zu identifizieren.

Nachfolgend wird nun die zweigeteilte Felddatenanalyse, dargestellt in Bild 5-2, mit den beiden Pfaden Fahrleistungsverteilung(en) und PiU-Ereignisse erläutert.

5.4.2 Pfad Fahrleistungsverteilung(en)

Die Fahrleistungsverteilung (FLV) ist für die weiteren Schritte im Wuppertal Prognosemodell (s. Abschnitt 5.4.3.1) notwendig, da die reine Betriebsdauer von Fahrzeugkomponenten nicht erfasst wird und Ausfälle von elektronischen Komponenten praktisch nicht vom reinen Alter (Kalenderzeit) einer Komponente abhängen. Somit wird die Betriebszeit über die Fahrleistung dargestellt. Diese wird für das jeweilige Fahrzeug bzw. die Fahrzeugklasse gesondert

ermittelt, da sie von Fahrzeugtyp zu Fahrzeugtyp unterschiedlich sein kann. Weiterhin muss beachtet werden, dass die Fahrleistung während der Garantiezeit von Fahrer zu Fahrer sehr unterschiedlich sein kann, wodurch Systeme z.B. bei Wenigfahrern geringer belastet werden als bei Vielfahrern. Dieser Sachverhalt wird dadurch berücksichtigt, dass die Fahrleistungen der Fahrzeuge auf ein Jahr umgerechnet werden. Weiterhin wird die Annahme getroffen, dass das Fahrverhalten eines Fahrzeuges über Jahre im Wesentlichen konstant ist. Besitzerwechsel erfolgen dabei sowohl von Viel- zu Wenigfahrern als auch umgekehrt, so dass sich hierdurch eventuell auftretende Effekte ausgleichen (s. hierzu [PAU 99b], [ALT 09a], [MEY 10] und [BRA 11]).

Aus praktischen Untersuchungen (siehe z.B. [MEY 03a]) hat sich gezeigt, dass die FLV von Personenkraftwagen sehr gut durch die logarithmische Normalverteilung $LN\left(\mu,\sigma^2\right)$, auch Lognormal-Verteilung genannt, beschrieben werden kann. Allerdings kann sich in einigen Fällen auch eine andere Verteilungsfunktion eignen, wie z.B. die Weibull-Verteilung (s. [BRA 07]) oder die Normalverteilung (z.B. für Nutzfahrzeuge). Unter der Annahme eines konstanten Fahrverhaltens ergibt sich die Fahrleistung eines Fahrzeugs in der Garantiezeit zu

$$S_t = S_g \cdot \frac{t}{g} \tag{5-1}$$

mit S_t: Zufallsvariable der Fahrleistung für die Betriebsdauer bis zum Ausfall,

S_g: Zufallsvariable der Fahrleistung für die Garantiezeit,

t: Betriebsdauer bis zum Ausfall und

g: Garantiedauer.

Die Fahrleistungsverteilungsfunktion berechnet sich aufgrund der einfachen linearen Transformation zu

$$L_t(s) = L_g\left(\frac{g}{t} \cdot s\right) \tag{5-2}$$

mit L_t: Verteilungsfunktion der Zufallsvariablen S_t,

L_g: Verteilungsfunktion der Zufallsvariablen S_g und

s: Fahrleistung bis zum Ausfall.

Die theoretische Anpassungsfunktion der Fahrleistungsverteilung ist die logarithmische Normalverteilung der Form

$$L_t(s) = \frac{1}{\sigma \cdot \sqrt{2\pi}} \cdot \int_0^s \frac{1}{\tau} e^{-\frac{(\ln \tau - \mu)^2}{2\sigma^2}} d\tau = \Phi\left(\frac{\ln s - \mu}{\sigma}\right) \quad \forall s > 0,\ \mu \in \Re,\ \sigma > 0\,. \tag{5-3}$$

Die obigen Fahrleistungsparameter μ und σ der Verteilungsfunktion können über die Maximum-Likelihood-Methode (MLM) oder andere Schätzverfahren aus den empirischen Daten bestimmt werden. Die MLM wird allerdings bevorzugt, da sie sehr gute Ergebnisse liefert und einfach in der Anwendung ist. Es ergeben sich die nachfolgenden Gleichungen für die Parameterschätzungen (siehe u.a. [MEY 10]):

$$\hat{\mu} = \frac{1}{n} \cdot \sum_{i=1}^{n} \ln t_i \text{ und} \tag{5-4}$$

$$\hat{\sigma}^2 = \frac{1}{n} \cdot \sum_{i=1}^{n} (\ln t_i - \hat{\mu})^2 \tag{5-5}$$

mit n: Stichprobenumfang und

t_i: Lebensdauer der i-ten Komponente.

Mit Hilfe der ermittelten Parameter kann außerdem der Erwartungswert der Verteilungsfunktion über

$$E(S) = e^{\mu + \frac{\sigma^2}{2}} \tag{5-6}$$

bestimmt werden. Der Erwartungswert eignet sich neben den Verteilungsparametern sehr gut, um die Fahrleistungsverteilungen von Fahrzeugen miteinander vergleichen zu können.

Es ist denkbar, dass die bei einer PiU-Untersuchung zu analysierende Fahrzeugmenge sehr klein ist. Es ist zwar ohne weiteres möglich, auch für eine kleine Anzahl an Datensätzen eine FLV zu ermitteln, die theoretische Fahrleistungsverteilung sollte aber, sofern realisierbar, aus allen möglichen aufgetretenen Schadensfällen aus der GuK-Datenbank bestimmt werden, welche die zu betrachtenden Fahrzeugbaureihen bzw. –modelle betreffen. Die FLV ist unabhängig von einem bestimmten Fehlertyp. Ist der Kandidat nur in einem gewissen Teil einer Baureihe (z.B. Fahrzeuge mit Diesel-Motoren) oder nur in einem bestimmten Fahrzeugtyp (z.B. Cabriolet) verbaut, darf allerdings nur diese Fahrzeugmenge in die Betrachtung einbezogen werden. Da durch diese Vorgehensweise für ein Fahrzeug mehrere Schadensfälle möglich sind (ein Fahrzeug kann in der Garantiezeit öfter als einmal in einer

Vertragswerkstatt gewesen sein), wird für die Fahrleistungsbestimmung der jeweils letzte Eintrag genutzt. Dadurch werden möglichst beständige Werte gewährleistet, da die Laufleistung erst über die Zeit stabil wird. Zu sehr frühen Zeitpunkten können unterschiedliche Faktoren, wie z.B. sehr lange Überführungsfahrten am Tag der Zulassung, die Ergebnisse beeinflussen und sogar verfälschen.

In nachfolgender Abbildung 5-4 wird die einjährige logarithmisch normalverteilte Fahrleistungsverteilung zur Veranschaulichung für einen Beispieldatensatz gezeigt.

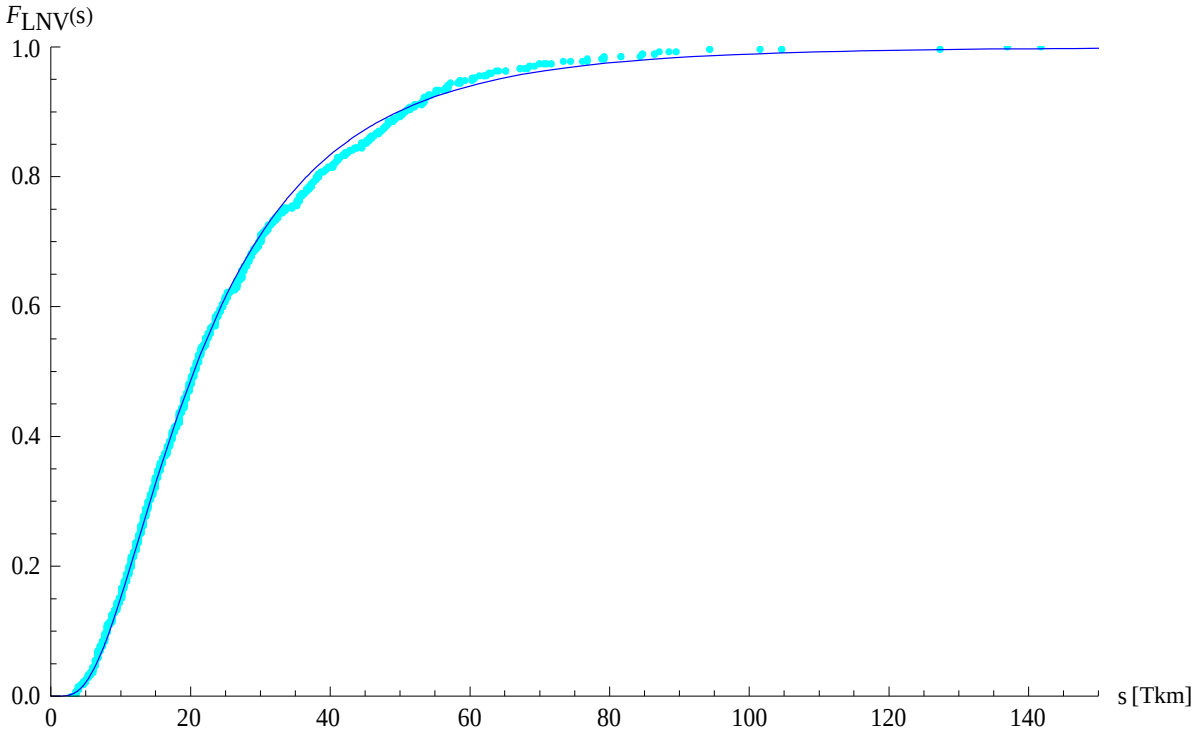


Bild 5-4: Jährliche Fahrleistungsverteilung ($LN\left(\mu,\sigma^2\right)$)

In obigem Bild 5-4 ist neben den empirischen Daten (mintfarbene Punkte) auch die angepasste theoretische Verteilungsfunktion (dünne blaue Linie) dargestellt. Zu erkennen ist weiterhin, dass für den verwendeten Beispieldatensatz die Hälfte aller Fahrzeuge ungefähr 20.000 km in einem Jahr zurücklegt haben und ca. 90% höchstens 50.000 km im Jahr fahren.

Aussagen zur Güte der Anpassung der theoretischen Verteilungsfunktion an die empirischen Werte können mit Hilfe eines Q-Q-Plots (Quantile-Quantile-Plot) und dem daraus resultierenden Bestimmtheitsmaß sowie dem Schätzer der Steigung der linearen Regression getroffen werden (Informationen hierzu können [HAR 05] und [FAH 07] entnommen werden).

Ab einem Wert von $B \geq 0{,}998 = 99{,}8\%$ kann von einer sehr guten Anpassung gesprochen werden. Die Anpassung aus Bild 5-4 erreicht eine Güte von 99,81%.

Eine weitere Überprüfung der Daten sollte dahingehend erfolgen, dass nicht nur unplausible Datensätze (s. Ausführungen in Abschnitt 5.4.1.2) aussortiert werden, sondern auch solche, bei denen eine Fahrleistung von 0 km eingetragen ist oder bei denen eine Angabe des Kilometerstandes komplett fehlt. Außerdem ist es sinnvoll, eine Begrenzung der Daten hinsichtlich der Jahresfahrleistung vorzunehmen. Dies muss individuell für die betrachteten Fahrzeugmodelle vorgenommen werden. So werden z.B. Fahrzeuge, die eine jährliche Fahrleistung von unter 3.000 km oder über 180.000 km aufweisen, aus der weiteren Betrachtung ausgeschlossen, da sie das Ergebnis verfälschen können. Die Grenzwerte stellen hierbei Erfahrungswerte für das jeweilige Betrachtungsland dar, die aus Untersuchungen oder speziellen Fahrleistungsdatenbanken gewonnen werden müssen. Fahrleistungen, die außerhalb des Bereichs liegen, sind normalerweise Ausnahmen (z.B. Taxen) und nicht repräsentativ für die entsprechende Fahrzeuggruppe.

Ist die für die PiU-Untersuchung relevante Analysemenge identifiziert, können hierfür nach den zuvor genannten Schritten die Fahrleistungsverteilungen bestimmt werden. Je nachdem, ob der Kandidat nur in einem Fahrzeugmodell, in mehreren Modellen oder sogar in verschiedenen Baureihen verbaut worden ist, sind dementsprechend mehrere Analysen erforderlich.

Darüber hinaus kann es bei der Fahrleistungsverteilungsbestimmung sinnvoll sein, bestimmte Fahrzeugmodelle in Klassen zusammenzufassen. Dabei sollten sowohl technische als auch statistische Aspekte berücksichtigt werden. Damit ist gemeint, dass Cluster gebildet werden können, in denen z.B.

- Fahrzeuge mit Dieselmotoren,
- Fahrzeuge mit Ottomotoren,
- Fahrzeuge mit Hybridantrieb,
- Fahrzeuge mit Elektroantrieb,
- Fahrzeuge mit Allradantrieb,
- Fahrzeuge mit Motoraufladung oder auch
- Tuningfahrzeuge

zusammengefasst werden. Fahrzeuge dieser Klassen teilen gleiche technische Merkmale, wie den gleichen Antrieb oder die gleiche Verbrennungsmotorart. Weiterhin kann aufgrund der Ermittlung der einzelnen FLV auffallen, dass bestimmte Fahrzeugtypen eine ähnliche Fahrleistungsverteilung aufweisen. Dies lässt sich anhand der Parameter und des Erwartungswerts der Verteilungsfunktion identifizieren (s. hierzu auch Ausführungen in Abschnitt 6.3.1).

Für diese Klassen wird jeweils eine eigene FLV ermittelt. Dies kann wiederum über die zuvor genannten Schritte geschehen. Falls die einzelnen modellbezogenen Fahrleistungsverteilungen bereits vorliegen, können die FLV der Cluster auch durch den Einsatz der Monte-Carlo-Simulation (MCS) bestimmt werden. Die MCS ist eine Simulationsmethode, mit der u.a. Zufallsgrößen und deren Verteilungsfunktionen simuliert werden können (weiterführende Informationen zur Monte-Carlo-Simulation sind u.a. [MAR 02] und [MEY 10] zu entnehmen). Da es sehr aufwendig sein kann, die einzelnen Datensätze der jeweiligen Gruppierungen separat zu analysieren, können die bereits ermittelten Ergebnisse der einzelnen Fahrzeugmodelle genutzt werden. Für jede einzelne FLV der Gruppierungselemente mit den zugehörigen, bereits bestimmten Parametern μ und σ kann eine Reihe von Lognormal-verteilten Zufallszahlen simuliert werden. An diese Werte wird anschließend eine neue logarithmische Normalverteilung angepasst, welche die Fahrleistungsverteilung der Gruppierung darstellt. Die Anzahl der simulierten Zahlen kann hierbei durch Faktorisierung der Originaldatenanzahl bestimmt werden.

Es bietet sich zusammenfassend für die OEM an, Fahrleistungsdatenbanken einzurichten, in welcher die Ergebnisse aller Baureihen, aller Modelltypen und aller Motorisierungsvarianten usw. sowie möglicher Clusterungen vorhanden sind. Sogar regionale und länderspezifische Betrachtungen sind hierbei möglich und auch sinnvoll. Aus den somit gewonnenen Informationen können wichtige Erkenntnisse über die Nutzung der einzelnen Fahrzeugtypen und –klassen gewonnen werden. Sofern möglich, kann die Ermittlung der FLV automatisiert innerhalb des Datenbanktools erfolgen – eine Überprüfung auf Plausibilität und Korrektheit muss allerdings immer noch erfolgen.

Darüber hinaus sind die Fahrleistungsverteilungen, wie bereits erwähnt, ein wichtiger Bestandteil des Wuppertaler Prognosemodells, welches im Pfad PiU-Ereignisse, der im nächsten Abschnitt beschrieben wird, verwendet wird.

In Abschnitt 6.3.1 sind die Ergebnisse der FLV-Ermittlungen (sowohl für einzelne Fahrzeugtypen als auch für verschiedene Klassen) für ein automotives Beispiel dargestellt.

5.4.3 Pfad PiU-Ereignisse

Im zweiten Teil der Felddatenanalyse (Pfad PiU-Ereignisse in Bild 5-2) müssen zunächst die Datensätze für den Kandidaten bestimmt werden, welche die PiU-relevanten Ereignisse darstellen. Um dies erfolgreich durchzuführen, ist eine enge Zusammenarbeit mit den entsprechenden Entwicklern bzw. Experten des Kandidaten notwendig, da diese Personen den diesbezüglich umfangreichsten Wissensstand, vor allem hinsichtlich möglicher Fehler und deren Ursachen, aufweisen.

Es kann darüber hinaus bei der Ereignisidentifizierung erforderlich sein, den Fokus nicht nur ausschließlich auf den Bereich Garantie und Kulanz zu legen, sondern Daten aus anderen Bereichen, wie z.B. der Diagnosebewährung, mit einzubeziehen. Infolgedessen muss die Schnittmenge der beiden Datenmengen anhand der jeweiligen Datumsangaben für z.B. die Reparatur (GuK) und die Diagnose gebildet werden, um die Analysemenge mit den relevanten Datensätzen zu ermitteln (s. hierzu auch Abschnitt 6.3.2). Diese Analysemenge wird anschließend mit Hilfe des Wuppertaler Prognosemodells untersucht, welches nachfolgend beschrieben wird.

5.4.3.1 Das Wuppertaler Prognosemodell

Das Zuverlässigkeitsprognosemodell, das in den 1990er Jahren von der Robert Bosch GmbH in Zusammenarbeit mit dem Fachgebiet Sicherheitstheorie und Verkehrstechnik des Fachbereichs Sicherheitstechnik der Bergischen Universität Wuppertal entwickelt worden ist und seitdem ständig weiterentwickelt wird (siehe u.a. [PAU 98], [PAU 99a], [PAU 00], [MEY 03a], [MEY 03b], [MEY 04], [ALT 09a] und [BRA 11]), kann bei vielen Hersteller- und Zulieferdaten in der Automobilindustrie angewandt werden, sofern die benötigten Informationen vorliegen. Diese Daten werden in der Regel nur während der Garantiezeit aufgenommen und vollständig sowie gut strukturiert dokumentiert. Mit Erreichen des Endes der Garantiezeit (in der Automobilindustrie in Deutschland üblicherweise zwei Jahre) entsteht somit ein abruptes Informationsloch zu den Fahrzeugen. Zwar wird es eventuell noch einige Kulanzfälle geben, die auch nach Ablauf der Garantie vom Hersteller übernommen werden, aber der Großteil der Fahrzeuge verschwindet sozusagen „vom Radar des OEM“. Die Vorteile

des Modells liegen nach [BRA 11] in der Betrachtung der spezifischen Feldbelastung durch Einbeziehung der Fahrleistung sowie in der vielfältigen Anwendbarkeit, die somit Prognose für nahezu alle Varianten von Systemen, Baugruppen und Komponenten bietet. Diesbezüglich sind eine Reihe von Projekten erfolgreich durchgeführt worden, die sich u.a. mit elektronischen Steuergeräten, Telematikeinheiten, Sensoren und Generatoren befassten (vgl. [PAU 98], [MEY 03a], [BRA 07] und [ALT 09a]).
Basis der Untersuchung bilden alle innerhalb der Garantiezeit erfassten Feldausfälle. Folgende Mindestinformationen sind dabei notwendig (s. auch Tabelle 5-1):

- Erstzulassungsdatum des Fahrzeugs,
- Ausfalldatum,
- Kilometerstand beim Ausfall und
- Fertigungsmenge im Betrachtungszeitraum.

Weiterhin sind zusätzliche Informationen hilfreich, um die Prognose präziser zu gestalten. Hierzu zählen:

- Produktionsdatum des Fahrzeugs (Berücksichtigung des Zulassungsverzugs),
- Erfassungsdatum des Ausfalls in der Datenbank (Berücksichtigung des Meldeverzugs),
- Teilmarktfaktor (Berücksichtigung, dass nur ein Teil der Schadensfälle bekannt ist, z.B. nur aus einem Land, wobei die Komponente in mehreren Ländern vertrieben wird),
- Rücklaufquote (Berücksichtigung des Verhältnisses zwischen Zulieferer und Hersteller) und
- Informationen zu epidemischen Ausfallbildern (Berücksichtigung von Expertenwissen).

Darüber hinaus sind je nach Anwendungsfall und Ziel der Prognose weitere Informationen und Einflussfaktoren denkbar, die eine Erweiterung des Modells ermöglichen (hierzu folgen am Ende diesen Abschnitts noch weitere Erläuterungen).

Daten zu Ausfällen von Systemen, Baugruppen und Komponenten der Fahrzeuge werden in der Regel nur während der Garantiezeit erfasst. Dabei besteht die Problematik, dass keine Betriebszeit in den Daten hinterlegt ist. Durch den Einsatz geeigneter Modelle ist es dennoch möglich, Aussagen über die geplante Lebensdauer der Komponente zu treffen und dies sogar

über die Garantiezeit hinaus. Hierzu wird die bis zum Ausfall gefahrene Strecke als adäquater Ersatz für die nicht vorhandene Betriebsdauer genutzt.

In nachfolgendem Bild 5-5 ist eine vereinfachte Darstellung des Ablaufs des Standardzuverlässigkeitsprognosemodells zu sehen.

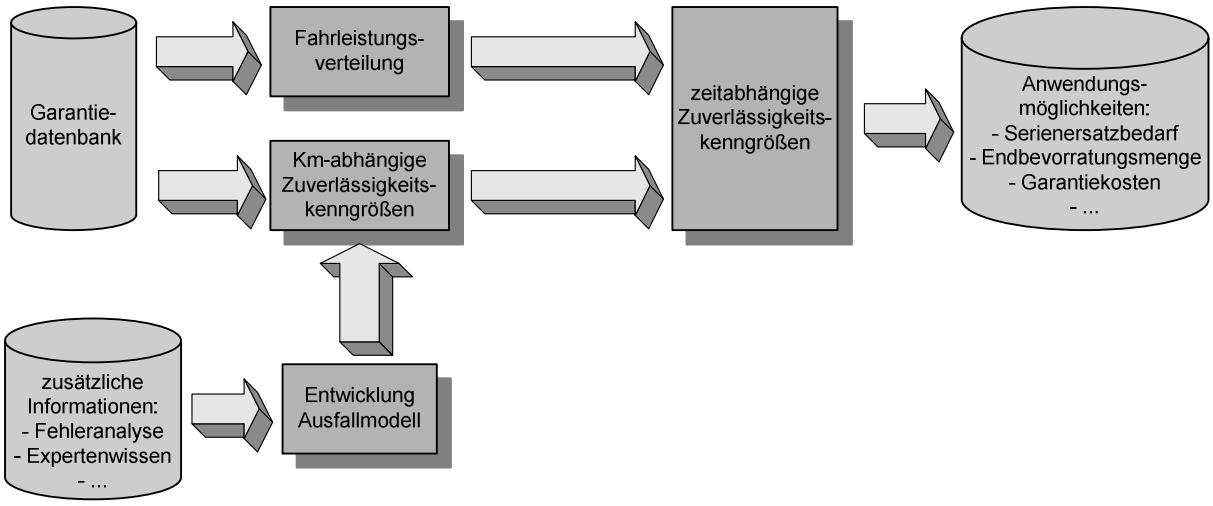


Bild 5-5: Vereinfachtes Ablaufdiagramm des Standardprognosemodells

Wie in obiger Abbildung 5-5 dargestellt, beginnt jede Prognose mit der Beschaffung und Aufbereitung der relevanten Daten. Da diesem Schritt eine immens hohe Bedeutung zukommt (er kann als Basis für alle weiteren Schritte angesehen werden), muss er besonderes sorgfältig vollzogen werden.

Das eigentliche Prognosemodell besteht im Wesentlichen aus den drei Schritten

- Fahrleistungsverteilung (aus Datenbank),
- Km-abhängige Zuverlässigkeitskenngrößen (aus Datenbank) und
- Zeitabhängige Zuverlässigkeitskenngrößen (aus FLV und km-abhängigen Kenngrößen),

auf die im Folgenden näher eingegangen wird. Für detaillierte Ausführungen wird auf die entsprechende Literatur (u.a. [PAU 96], [PAU 98], [MEY 03a], [MEY 10] und [BRA 11]) verwiesen. Die nachfolgend verwendeten Notationen sind an die zuvor genannten Literaturquellen angelehnt. Die notwendigen Berechnungen wie auch die dargestellten Abbildungen wurden mit der Software „Mathematica®“ erzeugt. Der Einsatz einer solchen Mathematik-Software oder ähnlichem ist notwendig, da Teile des mehrstufigen Modells nur numerisch gelöst werden können. Die dargestellten Ergebnisse wurden für einen

Beispieldatensatz ermittelt, die jedoch lediglich der Veranschaulichung des Modells dienen und nicht PiU-relevant sind.

Schritt 1: Fahrleistungsverteilung

Hinsichtlich der Bedeutung und der Vorgehensweise bei der Bestimmung der Fahrleistungsverteilung wird auf Abschnitt 5.4.2 verwiesen.

Schritt 2: Km-abhängige Prognose

Anhand der aus der Garantiedatenbank ermittelten Daten bzgl. der interessierenden Schadensfälle werden die km-abhängigen Zuverlässigkeitskenngrößen bestimmt. Die Belastung der Fahrzeugkomponenten wird durch die bis zum Ausfall gefahrene Strecke gut erfasst. Diese Angaben stehen für jeden Eintrag in der Garantiedatenbank zur Verfügung. Bei den Daten aus der Garantiezeit handelt es sich um eine so genannte gestutzte Stichprobe (Typ-I-Zensierung). Dabei muss die Tatsache berücksichtigt werden, dass die Ausfälle, die während der Garantiezeit zu einer bestimmten Strecke aufgetreten sind, nur einen Teil der gesamten Ausfälle darstellen. Es ist nämlich denkbar, dass Vielfahrer bei einer hohen Kilometerleistung während der Garantiezeit Fehler an ihren Fahrzeugen erleben, wohingegen Wenigfahrer diese Fehler nicht erfahren, da sie diese Kilometerleistung nicht erreichen. Dennoch können genau diese Fahrzeuge den Fehler zu einem späteren Zeitpunkt, wie z.B. nach der Garantiezeit, aufweisen. Durch diese noch zu erwartenden Fehler oder Ausfälle ergibt sich folglich eine gewisse Differenz, die durch eine so genannte Anwärterbestimmung ausgeglichen wird. Es gibt eine Reihe von Verfahren, um solche Anwärter zu prognostizieren, wie z.B. das Verfahren nach Eckel [ECK 77]. Untersuchungen in [FRI 00], [MEY 03a] und [BRA 11] führen aber zu dem Schluss, dass die Methode nach Pauli (s. [PAU 98]) zu bevorzugen ist.

Die korrigierte Anzahl der Ausfälle n_k zur Strecke s kann durch die während der Garantiezeit (bei der Strecke s) aufgetretenen Fehler $n_g(s)$ sowie die Fahrleistungsverteilung $L_g(s)$ zur Strecke s der Garantiezeit über

$$n_k(s) = \frac{n_g(s)}{1 - L_g(s)} \tag{5-7}$$

bestimmt werden. Diese Berechnung erfolgt für alle Strecken, bei denen Ausfälle aufgetreten sind.

Für die Prognose der km-abhängigen Lebensdauer wird des Weiteren die zugehörige Fertigungsmenge n_0 benötigt. Die empirische korrigierte Summenhäufigkeit wird durch sukzessive Kumulation der ermittelten Ausfallzahlen über

$$\tilde{F}_k(s) = \frac{n_k(s)}{n_0} = \frac{1}{n_0} \cdot \sum_{\zeta \le s} n_k(\zeta) = \frac{1}{n_0} \cdot \sum_{\zeta \le s} \frac{n_g(\zeta)}{1 - L_g(\zeta)} \tag{5-8}$$

berechnet.

Sofern vorhanden, sollte anstelle der Fertigungszahl die zugehörige Verkaufsmenge verwendet werden (s. Ausführungen in Abschnitt 5.4.1.1).

Nach [BRA 11] birgt der Einsatz des Verfahrens nach Pauli allerdings auch Gefahren, da es zu Verzerrungen bei der Fahrleistungsverteilung kommen kann, wenn die theoretische Fahrleistung stark von den empirischen Werten abweicht. Um eine Verfälschung der Anwärterkorrektur zu vermeiden, wird in [BRA 11] vorgeschlagen, Fahrleistungsparameter von unabhängigen Fallstudien zu verwenden. Eine solche Fahrleistungsdatenbank befindet sich derzeit im Aufbau beim Fachgebiet Sicherheitstheorie und Verkehrstechnik der Bergischen Universität Wuppertal. Auch die in Abschnitt 5.4.2 vorgeschlagenen unternehmensinternen Fahrleistungsdatenbanken bei den OEM sind in solchen Fällen eine gute Hilfe. Die Vorteile der Nutzung von unabhängigen Fahrleistungsdaten sind in [ALT 09b] geschildert.

Aus den empirischen Ausfallzeitpunkten können über geeignete Methoden die Parameter der anzupassenden theoretischen Verteilungsfunktion bestimmt werden. In der Regel lässt sich im zuverlässigkeitstechnischen Bereich das Ausfallverhalten sehr gut durch eine Weibull-Verteilung $W(\alpha, \beta)$ abbilden, da durch diese Verteilungsfunktion unterschiedliche Ausfallverhalten dargestellt werden können (s. hierzu Ausführungen zu Bild 4-1). Dies bedarf allerdings immer einer individuellen Überprüfung. Die Ausfallwahrscheinlichkeit der zweiparametrigen Weibull-Verteilung mit den Parametern $\alpha > 0$ und $\beta > 0$ ergibt sich aus:

$$F_k(s) = 1 - e^{-\alpha \cdot s^{\beta}} \quad \forall s \ge 0\,. \tag{5-9}$$

Anhand des Weibull-Parameters β, auch Ausfallsteilheit genannt, können direkt Aussagen zum Ausfallverhalten gemacht werden. Ist $\beta < 1$, so liegt ein Frühausfallverhalten vor. Beträgt die Ausfallsteilheit $\beta = 1$ so entspricht die Weibull-Verteilung der Exponentialverteilung, wobei der Parameter α der konstanten Ausfallrate λ entspricht. Ist $\beta > 1$, so handelt es sich um verschleißbedingte Ausfälle.

Als sehr geeignetes Verfahren, um die Parameter der Weibull-Verteilung zu ermitteln, hat sich die Methode der kleinsten Quadrate bewährt.

Schritt 3: Zeitabhängige Prognose

In der Automobilindustrie ist es üblich, wie in anderen Bereichen auch, bei sicherheits- und zuverlässigkeitstechnischen Fragestellungen einen Zeitbezug herzustellen. Es ist insbesondere von Interesse, mit wie vielen Ausfällen bis zu einem bestimmten Zeitpunkt zu rechnen ist. Mit Hilfe der Ergebnisse der ersten beiden Schritte können solche Aussagen zum zeitlichen Ausfallverhalten getroffen werden. Hierzu muss der km-abhängige Bezug der Verteilungsfunktion aus Formel 5-9 in einen zeitabhängigen Bezug transformiert werden. Die zeitabhängige Lebensdauerverteilung wird dabei aus der Integralgleichung

$$F(t) = \int_0^{\infty} f_k(s) \cdot \left(1 - L_1\left(\frac{s}{t}\right)\right) ds \quad \textit{für } t > 0 \tag{5-10}$$

mit $F(t)$: zeitabhängige Ausfallwahrscheinlichkeit,

$f_k(s)$: Dichte der korrigierten km-abhängigen Verteilungsfunktion und

L_1: jährliche Fahrleistungsverteilung

ermittelt. Dieses Integral ist nur numerisch zu lösen.

Die Parameter α und β der theoretischen Verteilungsfunktion

$$F(t) = 1 - e^{-\alpha \cdot t^{\beta}} \tag{5-11}$$

werden wiederum mit Hilfe von Parameterschätzverfahren, wie z.B. der Methode der kleinsten Quadrate, bestimmt.

Ist die zeitabhängige Verteilungsfunktion $F(t)$ mit allen Parametern bekannt, können andere Zuverlässigkeitskenngrößen, wie z.B. die Ausfallrate $h(t)$ über die einfache Beziehung

$$h(t) = \frac{1}{1 - F(t)} \cdot \frac{dF(t)}{dt}, \tag{5-12}$$

bestimmt werden.

Berücksichtigung von Modellkorrekturen

Das zuvor beschriebene Standardprognosemodell wurde in den vergangenen Jahren ständig weiterentwickelt. Nachfolgend aufgeführte Punkte sollten bei der Anwendung des Modells immer in Betracht gezogen werden.

Bei zeitnahen Garantiedaten kann es sein, dass sie noch nicht die vollständigen Informationen über das tatsächliche Ausfallverhalten eines Betrachtungsgegenstandes während der Garantiezeit enthalten. Von zeitnahen Garantiedaten wird dann gesprochen, wenn die Garantiezeiten aller Komponenten noch nicht verstrichen sind und die Ausfalldaten somit als unvollständig angesehen werden. Dies kann z.B. der Fall sein, wenn eine Prognose zu einem Zeitpunkt durchgeführt wird, zu dem die Serienproduktion noch läuft oder erst kürzlich beendet worden ist.

Der **Zulassungsverzug** beschreibt die Dauer zwischen der Produktion und der Erstzulassung eines Fahrzeugs und umfasst alle möglichen Lager-, Transport- und Montagezeiten. Mit der Erstzulassung beginnt in der Regel auch die Garantiezeit des Fahrzeugs und somit die des Betrachtungsgegenstandes. Es ist daher nicht unerheblich, den Anteil der Fahrzeuge zu approximieren, der zu einem bestimmten Zeitpunkt zugelassen ist und sich noch innerhalb des Garantiezeitraums befindet. Aus den in der Garantiedatenbank enthaltenen Informationen zum Fertigungs- und Zulassungsdatum, lässt sich die Verteilungsfunktion des Zulassungsverzugs $F_Z(t)$ schätzen. Untersuchungen haben gezeigt, dass sich hierzu die logarithmische Normalverteilung eignet (s. [MEY 03a] und [MEY 03b]). Die entsprechenden Parameter können wiederum über die MLM geschätzt werden. Mit Hilfe der Verteilungsfunktion für den Zulassungsverzug lässt sich die Anzahl der Fahrzeuge ermitteln, die bis zu einem bestimmten Monat zugelassen sind.

Der **Meldeverzug** beschreibt die Zeitspanne, welche zwischen dem Ausfall eines Produktes und dem Eintrag in eine Schadens- oder Garantiedatenbank liegt. Die Ursachen für einen solchen Meldeverzug haben meist organisatorische Gründe. Da das konkrete Ausfalldatum in der Regel in einer Garantiedatenbank nicht erfasst wird, wird hier das Reparaturdatum als Ersatz genutzt. Auch für die Beschreibung der Verteilungsfunktion für den Meldeverzug $F_M(t)$ eignet sich die Lognormal-Verteilung (s. [MEY 03a] und [MEY 03b]). Auch hier können die Parameter über die MLM geschätzt werden. Mit der ermittelten Verteilungsfunktion für den Meldeverzug lässt sich die Anzahl an Ausfällen bestimmen, die nach einer bestimmten Zeit in der Datenbank erfasst sind.

Aufgrund der ermittelten Verzugszeiten ist es möglich, sowohl die Zahl der Zulassungen als auch die aus der Garantiedatenbank zu einem Analysezeitpunkt bestimmten Ausfallzahlen zu korrigieren.

Ein weiterer wichtiger Punkt, der bei der Prognose berücksichtigt werden kann, ist der **Teilmarktfaktor** (TMF). Dieser ist interessant, wenn dem Hersteller nur Schadensfälle aus einem bestimmten Land bekannt sind, das Fahrzeug mit der entsprechenden Komponente aber noch in weiteren Ländern vertrieben wird. Ein Teilmarktfaktor $TMF = 15$ besagt beispielsweise, dass nur 15% des gesamten Marktes beobachtet wird und somit ca. jedes 15. Schadensteil untersucht werden kann. Das bedeutet allerdings auch, dass 15-mal mehr Schadensfälle aufgetreten sein können, als der Hersteller untersucht hat. Mit Hilfe des TMF muss somit die Grundgesamtheit, auf welche sich die Analyse bezieht, korrigiert werden. Damit wird der Anteil der nicht eingeschickten Komponenten berücksichtigt. Die mit dem Korrekturfaktor K_{TMF} korrigierte Grundgesamtheit berechnet sich nach [ALT 09a] zu

$$n_{korr,TMF} = n_{ges} \cdot K_{TMF} = n_{ges} \cdot \frac{1}{TMF} \tag{5-13}$$

mit n_{ges}: Grundgesamtheit und

$n_{korr,TMF}$: korrigierte Grundgesamtheit.

Ein weiterer Einflussfaktor ist die **Ausschlussquote** (AQ). Wie in Abschnitt 5.4.1.2 bereits erwähnt, werden unplausible und unvollständige Datensätze aus der Betrachtung ausgeschlossen. Allerdings stellen diese Datensätze immer noch ein für die Untersuchung relevantes Ereignis dar, welches es zu berücksichtigen gilt. Es liegt folglich eine Ausschlussquote vor, die sich folgendermaßen berechnen lässt:

$$AQ = \frac{n_A}{n} \tag{5-14}$$

mit n: Anzahl aller relevanten Datensätze und

n_A: Anzahl der ausgeschlossenen Datensätze.

Da nicht alle der verfügbaren Datensätze für die Analyse verwendet werden, muss die ursprüngliche Grundgesamtheit n_{ges} an produzierten Fahrzeugen um das Komplement der Ausschlussquote korrigiert werden, da die untersuchten Datensätze ansonsten zu positiv bewertet werden würden. Die somit korrigierte Grundgesamtheit $n_{korr,AQ}$ berechnet sich über

$$n_{korr,AQ} = n_{ges} \cdot (1 - AQ) = n_{ges} \cdot \left(1 - \frac{n_A}{n}\right). \tag{5-15}$$

Weitere Anpassungen des Standardprognosemodells können notwendig sein, wenn die kumulierten relativen Summenhäufigkeiten einen **grenzwertigen Verlauf** aufweisen. Nach [BRA 11] können beispielsweise „epidemische Fehler“ ein dominierendes Ausfallbild verursachen, welches starken Einfluss auf das Ausfallverhalten der kompletten Grundgesamtheit hat. Auch mit der bereits vorgestellten Anwärterprognose kann die relative Summenhäufigkeit in einem solchen Fall nicht derart angepasst werden, als dass eine empirische Ausfallwahrscheinlichkeit ermittelt wird, an welche eine theoretische Verteilungsfunktion zufrieden stellend angepasst werden kann. Eine Lösung bietet hier der in [MEY 03a] vorgestellte Ansatz eines „Teilpopulationsmodells“. Dieses erweitert die zweiparametrige Weibull-Verteilung aus Formel 5-11 um einen Anpassungsfaktor w zu

$$F_E(t) = w\left(1 - e^{-\alpha \cdot t^{\beta}}\right). \tag{5-16}$$

Der Parameter w begrenzt den Verlauf der Verteilungsfunktion derart, dass eine deutlich bessere Anpassung der theoretischen Verteilungsfunktion an die empirische Ausfallwahrscheinlichkeit möglich ist. Er kann durch Ablesen des höchsten Wertes der relativen Summenhäufigkeit bestimmt werden. Der Einsatz dieser Modelländerung sollte allerdings gut überdacht werden, da er nach [BRA 11] ein nicht zu vernachlässigendes Konfliktpotential bietet.

Anpassungen für eine PiU-Argumentation

Aufgrund der Tatsache, dass für einen Betriebsbewährtheitsnachweis Ereignisse analysiert werden, die zu einer Verletzung des Sicherheitsziels eines Kandidaten führen können, und dass diese Ereignisse nicht zwingend nur Ausfälle sein müssen (sondern z.B. auch Fehler einer Komponente, die nicht sofort zu einem Ausfall führen), wird im Rahmen der vorliegenden Arbeit eine andere Nomenklatur eingeführt. Es wird folglich nicht mehr von der Ausfallwahrscheinlichkeit $F(t)$ bzw. der Ausfallrate $h(t)$ gesprochen, sondern es werden die Termini Ereigniswahrscheinlichkeit $F_E(t)$ und Ereignisrate $h_E(t)$ eingeführt. Die zuvor genannten inhaltlichen und formelmäßigen Zusammenhänge bleiben bestehen und behalten ihre Gültigkeit.

In Abschnitt 6 wird die vorgestellte Vorgehensweise anhand eines realen Beispiels aus der Automobilindustrie exemplarisch durchgeführt.

5.4.3.2 Zerlegungen der Analysemenge

Die aus der Datenanalyse identifizierte PiU-relevante Analysemenge umfasst Datensätze, welche das Potential aufweisen, ein dem Kandidaten zugeordnetes Sicherheitsziel zu verletzen. Die Datensätze können zu Fahrzeugen aus unterschiedlichen Typen, Modellen und sogar Baureihen stammen. Aus diesem Grund kann es hilfreich sein, die Analysemenge aus verschiedenen Blickwinkeln zu betrachten. Damit ist gemeint, dass die Datensätze nicht nur komplett als eine Menge analysiert, sondern in verschiedene Teilmengen zerlegt und dann separat untersucht werden. Hierbei kann das Augenmerk sowohl auf eine zeitliche Zerlegung des Produktionszeitraums gelegt werden, um u.a. die Güte des Prognosemodells zu überprüfen, als auch auf eine fahrzeugbezogene Zerlegung. Aus der individuellen Analyse und anschließenden Bewertung mit Hilfe des Wuppertaler Prognosemodells können weitere wichtige Erkenntnisse gewonnen werden.

Zeitliche Zerlegung der Analysemenge

Um die Güte der durch das Wuppertaler Prognosemodell abgegebenen Prognosen zu untersuchen, ist es sinnvoll, die vorhandene Analysemenge zeitlich zu zerlegen. Dadurch können die einzelnen Ergebnisse der Prognosen und die tatsächlichen Ergebnisse miteinander verglichen werden. Über die zeitliche Zerlegung der Datensätze hinsichtlich des Produktionszeitraumes kann eine Überprüfung der Modellergebnisse vorgenommen werden. Wie die zeitliche Zerlegung der Analysemenge genau vorgenommen wird, hängt von der Zusammensetzung der Analysemenge ab. Es sollte darauf geachtet werden, dass die zeitlichen Abschnitte ungefähr den gleichen Umfang an Datensätzen beinhalten.

Bei einer großen Analysemenge kann außerdem versucht werden, die Zeitintervalle ungefähr gleich groß zu halten (z.B. jeweils ein Produktionsmonat). Dadurch kann der zeitliche Verlauf des Ereignisverhaltens genauer betrachtet und mögliche Schwachstellen in Produktionsmonaten aufgedeckt werden.

Eine beispielhafte zeitliche Zerlegung und deren Analyse sind in Abschnitt 6.3.2.2A gegeben.

Fahrzeugbezogene Zerlegung der Analysemenge

Über eine fahrzeugbezogene Zerlegung der Analysemenge durch Bildung von Clustern kann überprüft werden, wie sich die einzelnen Ergebnisse der identifizierten Fahrzeug-Cluster darstellen und auswirken. Bei der Bildung der Cluster sollten sowohl technische als auch statistische Aspekte Berücksichtigung finden. Hierfür kann sich u.a. an der Klasseneinteilung bei der Ermittlung der Fahrleistungsverteilungen (s. Ausführungen in Abschnitt 5.4.2) orientiert werden, wo solche Aspekte ebenfalls berücksichtigt werden.
Des Weiteren kann durch diese Zerlegung der Analysemenge untersucht werden, ob es eine dominierende Fahrzeuggruppe gibt, welche das gesamte Kollektiv maßgeblich beeinflusst.

Eine beispielhafte fahrzeugbezogene Zerlegung und deren Analyse sind in Abschnitt 6.3.2.2B gegeben.

Zuvor genannte mögliche Zerlegungen der Analysemenge sind optional, da ihr Einsatz von verschiedenen Aspekten abhängig ist, wie z.B. dem Umfang der Datensätze, der Zusammensetzung der Analysemenge hinsichtlich einer zeit- und/oder fahrzeugbezogenen Clusterung etc.

Die Ergebnisse der Fahrleistungsverteilungen aus dem ersten Teil der Felddatenanalyse können, wie bereits erwähnt, bei der Untersuchung der Analysemenge durch das Wuppertaler Prognosemodell verwendet werden. Hier ist eine mögliche Nutzung dieser Ergebnisse allerdings abhängig von der Zusammensetzung der Analysemenge. Sinnvoll ist eine Nutzung der Fahrleistungsverteilungen außerdem für die Analyse von Fahrzeug-Clustern, sofern eine solche fahrzeugbezogene Zerlegung vorgenommen werden kann.

5.5 Bewertung der Ergebnisse

In dem letzten Schritt einer PiU-Argumentation müssen die während der Felddatenanalyse erzielten Ergebnisse hinsichtlich der Betriebsbewährung bewertet werden. Hierzu ist in nachfolgendem Bild 5-6 die zu Beginn dieses Kapitels bereits ausführlich beschriebene Vorgehensweise noch einmal zusammenfassend dargestellt.

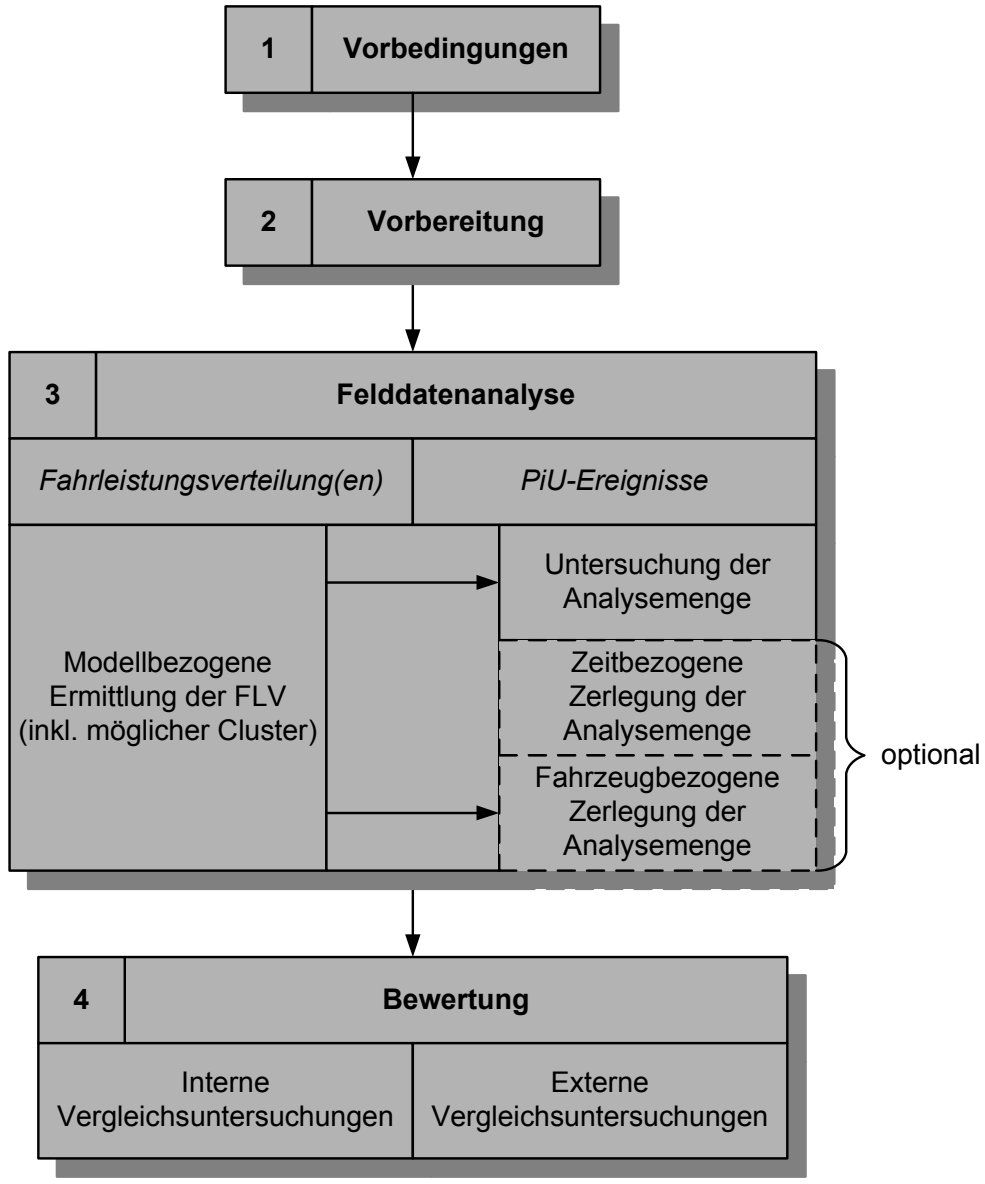


Bild 5-6: Zusammenfassende Darstellung der alternativen Vorgehensweise bei einer PiU-Argumentation

Wie in Bild 5-6 zu erkennen, umfasst der neue Ansatz eine Abfolge aus vier Schritten, wovon auf die ersten drei (Vorbedingungen, Vorbereitung und Felddatenanalyse mit den beiden Pfaden Fahrleistungsverteilung(en) und PiU-Ereignisse) bereits ausführlich eingegangen worden ist.

Bei der Bewertung der Ergebnisse der Analysen aus Schritt 3 gilt es nun, realistische und individuelle Kriterien zu verwenden – im Gegensatz zu den für die Praxis nicht anwendbaren Vorgaben der ISO 26262, die in Abschnitt 4.4 bereits kritisch hinterfragt worden sind. Wie in Bild 5-6 dargestellt, können hierfür sowohl interne als auch externe Vergleichsuntersuchungen herangezogen werden.

Unter *internen Vergleichsuntersuchungen* sind unternehmenseigene Analysen (z.B. bei einem Hersteller oder einem Zulieferer) zu verstehen, die nach der zuvor beschriebenen Vorgehensweise durchgeführt worden sind. Die Ergebnisse in Form von aus realen Felddaten ermittelten Verteilungsfunktionen stellen die **Referenzkriterien für zukünftige PiU-Untersuchungen** des gleichen Kandidaten dar. Damit ist gemeint, dass, wenn beispielsweise für einen Kandidaten hinsichtlich einer Baureihe X schon zeitliche Ereignisraten sowie Verteilungsfunktionen während einer früheren PiU-Argumentation ermittelt worden sind, diese Ergebnisse die Bewertungskriterien für eine neue PiU-Untersuchung unter gleichen Voraussetzungen (derselbe Kandidat, gleiches Sicherheitsziel etc.) in beispielsweise einer Baureihe Y darstellen. In einem solchen Fall können sogar hinsichtlich der Baureihe Y Aussagen zu frühen Zeitpunkten getroffen werden, sofern bereits PiU-relevante Ereignisse eingetreten sind.

Sind die neu ermittelten Verteilungsfunktionen bei der Untersuchung Y gleich gut oder besser als die der Untersuchung X, so kann der PiU-Argumentation Y ein positives Ergebnis ausgestellt werden. Dies ist allerdings nur möglich, sofern keine sicherheitskritischen Ereignisse aus dem Feldeinsatz des Kandidaten bekannt sind. Hierzu sind die entsprechenden Informationen von den zuständigen Experten und Verantwortlichen einzuholen. Nur wenn kein sicherheitskritisches Ereignis bekannt ist und die Ergebnisse der PiU-Untersuchung den Vergleich mit den Bewertungskriterien bestehen, kann der Kandidat als betriebsbewährt angesehen werden.

Sind keine internen Vergleichsuntersuchungen zum PiU-Kandidaten vorhanden, so können eventuell *externe Untersuchungen* als Bewertungskriterien herangezogen werden. Der Betrachtungsgegenstand und die Ergebnisse dieser Analysen müssen jedoch eine verwertbare und sinnvolle Bewertung der erzielten Ergebnisse des PiU-Kandidaten zulassen. Eine Komponente eines Bremssystems kann z.B. nicht ohne weiteres mit einer völlig anders gearteten Komponente eines Lenksystems verglichen werden. Es ist allerdings denkbar, Aussagen zu treffen, wenn die Bremsenkomponente mit Ergebnissen zum gesamten Bremssystem oder mit einer vergleichbaren Bremsenkomponente aus einer anderen Baureihe verglichen wird. Die mögliche Nutzung externer Kriterien muss bei jeder Untersuchung gewissenhaft untersucht und überprüft werden. Auf jeden Fall ist es notwendig, dass die externen Untersuchungen auf empirischen Daten beruhen und somit statistisch abgesichert sind.

Interne Untersuchungen sind, sofern vorhanden, den externen Vergleichsuntersuchungen vorzuziehen.

6 Anwendung der neuen Vorgehensweise anhand eines realen automotiven Beispiels

In diesem Kapitel wird die zuvor entwickelte neue Vorgehensweise für eine PiU-Argumentation anhand eines realen automotiven Beispiels durchgeführt. Die hierzu erforderlichen Daten stammen von einem deutschen Automobilhersteller und stellen praxisnahe und reale Betriebsdaten dar. Alle nachfolgenden Angaben und Ergebnisse sind anonymisiert.
Die in den folgenden Abschnitten notwendigen Berechnungen sowie die nachfolgend gezeigten Graphiken wurden mit der Software Mathematica® (Version 6.0.1.0) erzeugt.

6.1 Vorbedingungen

Für die exemplarische Durchführung der neuen PiU-Vorgehensweise wurde ein Betrachtungsgegenstand gewählt, welcher in einem sicherheitsbezogenen E/E-System in Fahrzeugen eingesetzt wird. Hierbei handelt es sich um ein aktives Regelungssystem zur Fahrdynamik. Dieses ist in mehreren Baureihen verbaut. Der Kandidat der PiU-Untersuchung wurde allerdings nur in einer Baureihe verbaut, hier jedoch in verschiedenen Fahrzeugtypen und auch -modellen. Diese Baureihe wurde über einen Zeitraum von sieben Jahren produziert und kann als großvolumig angesehen werden.

Für den Kandidaten ist im Vorfeld der Betriebsbewährtheitsuntersuchung bereits eine Gefahrenanalyse und Risikobewertung durchgeführt worden. Eines der dabei ermittelten Sicherheitsziele wurde mit einem ASIL D bewertet. Dieses wird in der vorliegenden PiU-Argumentation betrachtet.

Der Automobilhersteller verfügt über ein sehr umfangreiches und gut strukturiertes Datenbanksystem, in welchem Informationen aus unterschiedlichsten Bereichen zusammengeführt werden. Hierzu zählen Garantie- und Kulanzdaten zu allen Baureihen des Herstellers der vergangenen Jahre/Jahrzehnte. Des Weiteren sind dort auch Informationen zur Diagnosebewährung sowie zu Reparaturqualitäten enthalten.
Das Datenbanksystem verfügt weiterhin über diverse voreingestellte und standardisierte Auswertemöglichkeiten. Außerdem können die Informationen der Datenbank individuell

zusammengestellt werden, so dass die Möglichkeit besteht, nur die für die PiU-Argumentation relevanten Angaben zu verknüpfen und somit eigenständige Berichte zu erstellen.
Für die PiU-relevante Baureihe liegen die GuK-Daten seit Produktionsbeginn vor. Gleiches gilt für den Bereich der Diagnosebewährung.

6.2 Vorbereitung

Für das sicherheitsbezogene E/E-System wie auch für den Kandidaten selbst gab es umfangreiche Spezifikationsdokumente, so dass ein umfassendes und genaues Bild des Kandidaten hinsichtlich der Einsatzbedingungen, der Funktionsweise sowie der Überwachungsmöglichkeiten dargestellt wurde.

Zu dem sicherheitsbezogenen E/E-System wie auch zu dem Kandidaten selbst lag bei dem Automobilhersteller ein langjähriger und umfangreicher Erfahrungsschatz vor. Dieser bezieht sich sowohl auf das Betriebsverhalten als auch auf bekannte Fehler und Ausfälle sowie den damit zusammenhängenden Ursachen. Sicherheitskritische Ereignisse aus dem Feldeinsatz waren dem Hersteller außerdem nicht bekannt.

Da der Kandidat in verschiedenen Fahrzeugtypen und –modellen einer Baureihe verbaut ist, wurden mögliche Änderungen am Kandidaten selbst sowie an dem sicherheitsrelevanten E/E-System berücksichtigt, zu dem der Kandidat zugeordnet ist. Die Einbau-, Umgebungs- und Einsatzbedingungen waren bei allen Varianten die gleichen. Des Weiteren wurde für die Untersuchung eine bestimmte Version des E/E-Systems herausgesucht, so dass keine Änderungen in dem Betrachtungszeitraum vorliegen.

6.3 Felddatenanalyse

Nachfolgend werden die Arbeitsschritte der Felddatenanalyse beschrieben und die dabei erzielten Erkenntnisse und Ergebnisse präsentiert.

6.3.1 Pfad Fahrleistungsverteilung(en)

Wie zuvor beschrieben, wurde der Kandidat für den Betriebsbewährtheitsnachweis in einer Baureihe verbaut. Für diese Baureihe sind zunächst, die Fahrleistungsverteilungen nach dem in Abschnitt 5.4.2 beschriebenen Vorgehen zu ermitteln.

In der vorliegenden Arbeit wurde dies für insgesamt 49 Fahrzeugmodelle der relevanten Baureihe durchgeführt. Der dabei betrachtete Produktionszeitraum erstreckte sich über 115 Monate.

Die Ergebnisse der jährlichen FLV sind in nachfolgender Tabelle 6-1 übersichtlich dargestellt. Genauere Informationen sind Anhang A2 zu entnehmen, in dem alle Ergebnisse der Ermittlungen der jährlichen Fahrleistungsverteilungen inklusive deren graphischer Darstellungen enthalten sind. In Tabelle 6-1 sind zu jedem Fahrzeugmodell die verwendete Anzahl an Daten, die Parameter μ und σ der an die empirischen Daten angepassten logarithmischen Normalverteilung sowie der entsprechende Erwartungswert $E(S)$ der Verteilung und das Bestimmtheitsmaß B der Anpassung gegenübergestellt. Die Parameter der Lognormal-Verteilung wurden hierbei über die Maximum-Likelihood-Methode bestimmt (s. hierzu auch Abschnitt 5.4.2). Insgesamt wurden über 377.000 Datensätze ausgewertet, wobei diese die jeweils letzten GuK-Ereignisse der betrachteten Fahrzeuge darstellen und somit ein deutlich höherer Datenumfang untersucht worden ist.

Die Fahrzeugmodelle in der folgenden Gegenüberstellung sind anonymisiert dargestellt, so dass keine Schlüsse auf die realen Fahrzeuge gezogen werden können. Hierfür wurde eine alphanumerische Verschlüsselung gewählt. Die Ziffern von 01 bis 12 unterscheiden die Fahrzeugmodelle nach Hubraum, wobei dieser mit steigenden Ziffern zunimmt. Die an zweiter Stelle stehenden Großbuchstaben kennzeichnen die jeweilige Fahrzeugkategorie über:

- Limousinenfahrzeug (L),
- Kombifahrzeug (K) und
- Coupé oder Sportwagen (C).

Nach dem 2. Bindestrich befindet sich die Verschlüsselung für die Kraftstoffart des Fahrzeugmodells. Hierbei wird unterschieden in

- Benzinmotoren (b) und
- Dieselmotoren (d).

Nach der Kraftstoffcodierung folgen, gekennzeichnet durch die Schrägstriche, weitere Besonderheiten der entsprechenden Modelle, wie

- Fahrzeug mit Allradantrieb (a),
- Fahrzeug mit Direkteinspritzung (e),
- Fahrzeug mit Motoraufladung (m) und
- Tuningfahrzeug (t).

Tabelle 6-1: Ergebnisse der jährlichen Fahrleistungsverteilungen der PiU-relevanten Baureihe

Nr.	Fahrzeugmodell	Datenanzahl	Parameter der theoretischen jährlichen FLV		E(S) [Tkm]	B
			μ	σ		
1	01-C-b	109	2,6719	0,62059	17,54	0,99912
2	01-L-b/m	1.051	2,4404	0,49965	13,00	0,99968
3	02-L-b	15.147	2,4149	0,47310	12,51	0,99989
4	02-K-b	2.905	2,6358	0,46713	15,56	0,99929
5	02-C-b/m	5.771	2,4536	0,50102	13,19	0,99976
6	02-L-b/m	54.918	2,4632	0,52048	13,45	0,99988
7	02-K-b/m	24.927	2,7190	0,49246	17,12	0,99959
8	03-C-b/m	1.245	2,4909	0,51692	13,80	0,99918
9	03-L-b/m	37.836	2,5034	0,52545	14,03	0,99968
10	03-K-b/m	15.618	2,7494	0,49987	17,71	0,99973
11	03-L-b/e/m	289	2,6547	0,59031	16,93	0,99954
12	03-K-b/e/m	101	2,9018	0,59630	21,75	0,99874
13	03-C-d	992	2,8755	0,51614	20,26	0,99952
14	03-L-d	36.755	2,9379	0,66263	23,51	0,99872
15	03-K-d	27.952	3,2544	0,64328	31,86	0,99899
16	04-C-d	2.191	2,9169	0,51378	21,09	0,99996
17	04-L-d	56.659	3,0058	0,59278	24,08	0,99982
18	04-K-d	51.413	3,2485	0,56017	30,13	0,99986
19	05-C-b	1.104	2,5599	0,49665	14,63	0,99976
20	05-L-b	1.274	2,5381	0,52728	14,54	0,99965
21	05-K-b	1.243	2,8083	0,46605	18,48	0,99907
22	05-L-b/m	3.437	2,5908	0,52587	15,32	0,99982
23	05-K-b/m	567	2,9358	0,47330	21,07	0,99829
24	06-L-b	3.123	2,5462	0,58343	15,13	0,99949
25	06-K-b	1.381	2,7867	0,49344	18,33	0,99969
26	06-L-b/a	353	2,5355	0,54233	14,62	0,99940
27	06-K-b/a	330	2,7136	0,50030	17,10	0,99976

Fortsetzung von Tabelle 6-1

Nr.	Fahrzeugmodell	Datenanzahl	Parameter der theoretischen jährlichen FLV		E(S) [Tkm]	B
28	07-L-d	6.676	3,1713	0,56695	28,00	0,99995
29	07-K-d	9.072	3,2238	0,50132	28,49	0,99982
30	08-L-b	643	2,6370	0,54166	16,18	0,99947
31	08-K-b	1.068	2,8431	0,41722	18,73	0,99908
32	08-L-b/a	214	2,5303	0,56089	14,70	0,99902
33	08-K-b/a	300	2,8058	0,51645	18,90	0,99959
34	09-L-d/t	321	3,1191	0,49514	25,58	0,99841
35	09-K-d/t	276	3,2286	0,42146	27,59	0,99953
36	10-L-b	1.803	2,6560	0,56638	16,72	0,99980
37	10-K-b	788	2,8556	0,47343	19,45	0,99950
38	10-L-b/a	363	2,6114	0,57551	16,07	0,99902
39	10-K-b/a	348	2,8054	0,51531	18,88	0,99939
40	10-L-b/m/t	327	2,8846	0,49848	20,27	0,99961
41	10-K-b/m/t	406	2,9110	0,47358	20,56	0,99841
42	10-L-d	1.447	3,1598	0,56451	27,64	0,99979
43	10-K-d	2.804	3,2706	0,48242	29,58	0,99981
44	11-C-b	481	2,6654	0,53732	16,61	0,99965
45	11-L-b	223	2,7738	0,57062	18,85	0,99811
46	11-K-b	278	2,8744	0,48025	19,88	0,99875
47	11-L-b/a	42	2,4557	0,57445	13,75	0,99789
48	11-K-b/a	112	2,8638	0,46584	19,54	0,99757
49	12-L-b/t	395	2,9201	0,53631	21,41	0,99909

Die in Tabelle 6-1 angegebenen Fahrzeugmodellbezeichnungen sind wie folgt zu interpretieren:

Bei den Nummern 13 bis 15 handelt es sich um Fahrzeuge des gleichen Modelltyps und gleichen Hubraums mit gleicher Motorart. Sie unterscheiden sich lediglich dadurch, dass es sich einmal um eine Limousine (03-L-d), einmal um einen Kombi (03-K-d) und einmal um ein Sportcoupé (03-C-d) handelt. Die Fahrzeugmodelle 8 bis 12 sind die entsprechenden

Benzinmotorvarianten mit gleichem Hubraum wie die Dieselmotoren. Sie unterscheiden sich untereinander dadurch, dass es sowohl Fahrzeuge mit einer Motoraufladung (Nummern 8 bis 10) gibt als auch Fahrzeuge mit Motoraufladung und einer Benzindirekteinspritzung (Nummer 11 und 12).
Die beiden Fahrzeugmodelle 26 (06-L-b/a) und 47 (11-L-b/a) unterscheiden sich nur dadurch, dass Nummer 47 einen größeren Hubraum besitzt. Sowohl die Motorart (Benzinmotor) als auch die Antriebsart (Allradantrieb) sind gleich.
Über die gewählte Nomenklatur wird sichergestellt, dass die Fahrzeugmodelle in einer anonymisierten Art und Weise dargestellt sind und untereinander schnell verglichen werden können.

Die obige Tabelle 6-1 zeigt, dass ein großer Anteil (knapp 80%) der angepassten Verteilungsfunktionen ein sehr gutes Bestimmtheitsmaß von mehr als 99,9% aufweisen. Ab einem Wert von $B = 0{,}998$ kann von einer guten Anpassung gesprochen werden, was bei ca. 96% der Fall ist. Nur zwei Anpassungen (11-L-b/a und 11-K-b/a) haben ein Bestimmtheitsmaß, das geringfügig unter diesem Wert liegt. Die Anpassungen sind allerdings immer noch als gut einzustufen. Hierbei muss angemerkt werden, dass bei diesen Anpassungen zwei der geringsten Datenumfänge zur Verfügung standen. Insgesamt kann somit festgehalten werden, dass die Anpassungen für die PiU-relevante Baureihe sehr gut sind.

Es ist interessant festzustellen, dass jedes Kombifahrzeug eine höhere jährliche Fahrleistung aufweist als das entsprechende Standardmodell (Limousine). Dies gilt unabhängig vom Hubraum, der Motorart (Benziner oder Diesel) und sonstiger fahrzeugspezifischer Merkmale (z.B. Motoraufladung oder Allradantrieb). Im Schnitt liegt die Jahresfahrleistung eines Kombifahrzeuges um 3,44 Tkm über der jährlichen FLV der entsprechenden Limousine.

Des Weiteren ist Tabelle 6-1 zu entnehmen, dass die Fahrleistungen der einzelnen Modelle der Baureihe teilweise große Unterschiede zueinander aufweisen. Es scheint hierbei Gruppierungen oder Cluster innerhalb der Baureihe zu geben, die alle eine ähnliche Fahrleistung aufweisen. Aus diesem Grund wurden die Fahrzeugmodelle in Klassen zusammengefasst, so z.B. in Diesel-Fahrzeuge (L-d, K-d und d), in Fahrzeuge mit Allradantrieb (L-a, K-a und a), Fahrzeuge mit Motoraufladung (L-m, K-m und m) und Tuningfahrzeuge (t). Bei der Einteilung der Klassen wurden sowohl technische Aspekte als

auch statistische Merkmale berücksichtigt. Für die Gruppierungen wurde jeweils eine gemeinsame Fahrleistungsverteilung bestimmt. Die Anpassung erfolgte durch Einsatz der Monte-Carlo-Simulation. Nähere Erläuterungen hierzu sind in Abschnitt 5.4.2 zu finden.
Die Ergebnisse der Clusterungen sind in nachfolgender Tabelle 6-2 dargestellt. In Anhang A2 sind die graphischen Darstellungen der jährlichen FLV der Klasseneinteilungen der PiU-relevanten Baureihe enthalten.

Tabelle 6-2: Ergebnisse der jährlichen Fahrleistungsverteilungen für die Cluster der PiU-relevanten Baureihe

Fahrzeugcluster	Simulierte Datenanzahl	Parameter der theoretischen jährlichen FLV		E(S) [Tkm]
		μ	σ	
Limousine mit Allradantrieb (L-a)	20.412.000	2,5594	0,56203	15,14
Kombi mit Allradantrieb (K-a)	23.980.000	2,7837	0,50861	18,41
Alle Fahrzeuge mit Allradantrieb (a)	22.682.000	2,6779	0,54597	16,89
Alle Tuningfahrzeuge (t)	20.700.000	2,9975	0,50664	22,78
Limousine mit Dieselmotor (L-d)	23.427.340	2,9946	0,61976	24,21
Kombi mit Dieselmotor (K-d)	22.879.250	3,2486	0,57910	30,46
Alle Fahrzeuge mit Dieselmotor (d)	23.205.000	3,1149	0,61413	27.21
Limousine mit Motoraufladung (L-m)	20.909.400	2,4819	0,52224	13,71
Kombi mit Motoraufladung (K-m)	20.606.500	2,7340	0,49626	17,41
Alle Fahrzeuge mit Motoraufladung (m)	21.864.000	2,5533	0,52749	14,77
Gesamte Baureihe	22.624.680	2,8452	0,63659	21,07

Auch Tabelle 6-2 zeigt, dass die Kombifahrzeuge eine höhere jährliche Fahrleistung aufweisen als die entsprechenden Limousinen. Weiterhin ist ersichtlich, dass Diesel-Fahrzeuge die höchsten Fahrleistungen pro Jahr besitzen. Deutlich wird außerdem, dass die angepasste FLV für die gesamte Baureihe teils erheblich von den Fahrleistungen der einzelnen Modelltypen bzw. den Clustern abweicht. Aus den Ergebnissen der FLV wird klar, dass es nicht sinnvoll ist, eine generelle Fahrleistungsverteilung für die Baureihe zu bestimmen, da sie nicht repräsentativ für alle Modelle ist. Dementsprechend ist es erforderlich, die Analysemenge auf eine mögliche Clusterung hinsichtlich der FLV zu untersuchen. Zuvor muss diese Analysemenge allerdings identifiziert werden (s. nachfolgende Ausführungen).

6.3.2 Pfad PiU-Ereignisse

Wie in den Kapiteln 4 und 5 dargelegt, müssen bei einer PiU-Untersuchung spezielle Ereignisse identifiziert werden, die aus Felddaten analysiert werden können. Diese Ereignisse müssen das Potential haben, ein dem Kandidaten zugeordnetes Sicherheitsziel zu verletzen. Um eine solche Ereignisidentifikation durchführen zu können, sind intensive Gespräche mit den entsprechenden System- und/oder Komponentenexperten erforderlich, die über mögliche Ausfälle und Fehler Auskunft geben können. Hinzu kommen Ergebnisse von bereits durchgeführten Struktur- und Einflussanalysen, welche die potentiellen Fehlerursachen zum Gegenstand hatten. Dieses Wissen muss auf die zur Verfügung stehenden Daten aus der Feldaufzeichnung angewendet werden. Damit ist gemeint, dass sich die relevanten Fehler- und Ausfallursachen für die PiU-Argumentation in den Felddaten wiederfinden müssen.

Hierzu wurden verschiedene Datenquellen des Automobilherstellers analysiert. Eine alleinige Nutzung der GuK-Daten reichte nicht aus, da die Beschreibungen der Fehlerarten (hiervon wurde eine als relevant eingestuft) nicht spezifisch genug waren, um die PiU-Ereignisse, die das Potential zur Verletzung eines Sicherheitsziels haben, genau identifizieren zu können (s. hierzu auch Ausführungen in Abschnitt 5.4.1.4).
Im Rahmen der zuvor genannten Expertengespräche wurde der Fokus auch auf mögliche Diagnoseeinträge zu dem sicherheitsrelevanten E/E-System gelenkt, zu dem der Kandidat zugeordnet wird. Alle diagnostizierten Fehler der Systemkomponenten wurden in dem Systemsteuergerät als Fehlercode abgelegt. Dieser Fehlercode ist ein Code, der im Rahmen einer Diagnose Aufschluss über Fehlfunktionen von Fahrzeugkomponenten gibt. Für das

Systemsteuergerät lagen insgesamt über 120 Fehlercodes vor, von denen drei für die PiU-Untersuchung relevant waren. Ihnen wurde aufgrund von Strukturanalysen ein entsprechendes Potential zur Verletzung des Sicherheitsziels zugeordnet. An dieser Stelle sei allerdings noch einmal betont, dass dem Hersteller keine Feldereignisse bekannt sind, in denen ein solcher Fehler zu einem tatsächlichen sicherheitskritischen Ereignis geführt hat. Für die drei Fehlercodes wurden insgesamt über 15.000 Diagnoseeinträge aus der Datenbank identifiziert. Hierbei kam es vor, dass ein einziges Fahrzeug mehrere Dutzend Einträge an einem Tag oder an aufeinanderfolgenden Tagen aufwies. Diese Zeitspannen stellen die Werkstattaufenthalte dar. Bei diesen wurde das entsprechende Fahrzeug mehrmals diagnostiziert, so dass Diagnoseeinträge mehrfach auftraten. Da anhand der Einträge nicht klar erkennbar war, ob bei den Werkstattaufenthalten auch etwas an der entsprechend identifizierten Komponente, also dem Kandidaten, repariert worden ist, konnten die Diagnosedaten allein nicht verwendet werden.

Die beiden Datenmengen aus Garantie und Kulanz und Diagnosebewährung mussten miteinander kombiniert werden, da die GuK-Daten nicht spezifisch genug waren und bei den Diagnosedaten nicht zweifelsfrei festgestellt werden konnte, welche Einträge wirklich relevant waren. Eine Übersicht über die aus der Datenbank gewonnenen Informationen der Datensätze aus den beiden Bereichen ist in nachfolgender Tabelle 6-3 gegeben.

Tabelle 6-3: Gegenüberstellung der Informationen aus GuK-Bereich und Diagnosebewährung

GuK	**Diagnose**
Fahrzeugidentifizierungsnummer	
Produktionsdatum	
Erstzulassungsdatum	
Vertriebsland	
Reparaturdatum	Startdatum Diagnose
	Werkstattaufenthalt (Diagnose)
Reparaturland	Reparaturland (Diagnose)
Fehlerort	Steuergerät
Fehlerart	Fehlercode
Fahrzeuglaufleistung in km	Fahrzeuglaufleistung in km (Diagnose)

Wie obige Tabelle 6-3 zeigt, verwenden beide Bereiche z.T. sowohl identische Informationen (Fahrzeugidentifizierungsnummer, Produktionsdatum, Fertigungsdatum und Vertriebsland) als auch unterschiedliche Angaben (wie z.B. Reparaturdatum und Startdatum Diagnose bzw. Fehlerart und Fehlercode) sowie eigene Informationen, wie der Werkstattaufenthalt (Diagnose), dem ein entsprechendes Pendant im Bereich Garantie und Kulanz fehlt.

Die Kombination und Bestimmung der Schnittmenge aus beiden Datenmengen erfolgt zunächst über die Fahrzeugidentifizierungsnummer, anhand derer ein Fahrzeug eindeutig identifizierbar ist (s. Ausführungen in Abschnitt 5.4.1.4). Durch die FIN wurde bei der Datenkombination gewährleistet, dass es sich bei den Datensätzen aus dem Bereich Garantie und Kulanz sowie der Diagnosebewährung um Einträge desselben Fahrzeugs handelt. Weiterhin werden bei der Identifikation der Schnittmenge das Reparaturdatum und das Startdatum (Diagnose) bzw. der Werkstattaufenthalt (Diagnose) verwendet. Damit ist gemeint, dass nur die Ereignisse in die Schnittmenge gelangen, bei denen das Reparaturdatum aus dem GuK-Bereich mit dem Startdatum der Diagnosebewährung zusammen passt. Diese beiden Datumsangaben müssen jedoch nicht vollständig übereinstimmen, da ein Fahrzeug durchaus länger als einen Tag in einer Werkstatt gewesen sein kann. Vielmehr muss das Reparaturdatum in der Zeitspanne des Werkstattaufenthalts (diese Angabe ist Teil der Informationen eines Datensatzes der Diagnose) liegen.

Als Ergebnis der Kombination kann festgehalten werden, dass die Analysemenge 46 Ereignisse umfasst, denen das Potential zugesprochen wird, das dem Kandidaten zugeordnete Sicherheitsziel verletzen zu können.
Eine genauere Begutachtung dieser Datensätze macht allerdings deutlich, dass zwei aus den weiteren Betrachtungen ausgeschlossen werden müssen. Ein Datensatz war unplausibel, da er einen Datumsfehler beinhaltete, wobei das Zulassungsdatum vor dem Produktionsdatum lag. Ein anderer Datensatz hatte eine zu geringe Jahresfahrleistung. Das bedeutet, dass die Analysemenge nunmehr 44 Datensätze von zwölf Fahrzeugmodellen beinhaltete. Der dabei betrachtete Produktionszeitraum umfasste 28 Monate, in denen 122.727 Fahrzeuge der zwölf Modelle gefertigt worden sind. Diese PiU-relevanten Ereignisse werden nun mit Hilfe des Wuppertaler Prognosemodells analysiert.

6.3.2.1 Untersuchung der Analysemenge

Zunächst wurde auch für die gesamte Analysemenge die Fahrleistungsverteilung ermittelt. In nachfolgendem Bild 6-1 ist die einjährige logarithmisch normalverteilte Fahrleistung für die Analysemenge dargestellt.

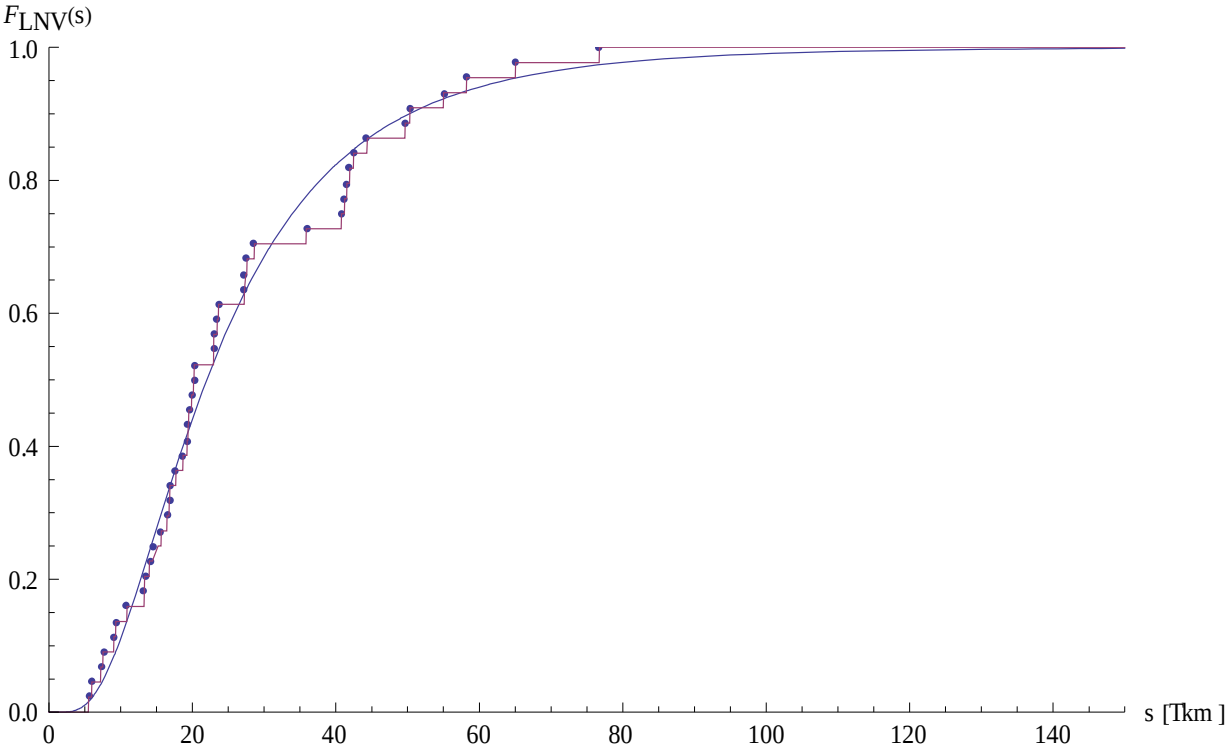


Bild 6-1: Jährliche FLV ($LN\left(\mu,\sigma^2\right)$) der Analysemenge

Obiges Bild 6-1 zeigt neben den empirischen Daten (blaue Punkte mit roter Linie) auch die angepasste theoretische Verteilungsfunktion (blaue Linie.) Die mit Hilfe der MLM bestimmten Parameter der Fahrleistungsverteilung der Analysemenge lauten:

- $\mu = 3{,}7833$ und
- $\sigma = 0{,}64433$.

Die Verteilungsfunktion hat einen Erwartungswert von $E(S) = 27{,}05\,Tkm$ und weist ein Bestimmtheitsmaß von $B = 0{,}9966$ auf.

In einem zweiten Schritt werden die km-abhängigen Kenngrößen ermittelt, wobei die vorhandenen Datensätze korrigiert und Anwärter bestimmt werden. Mit Hilfe dieser kann die korrigierte km-abhängige Lebensdauerverteilung ermittelt werden, welche das zu erwartende Ereignisverhalten im Feld beschreibt, wenn alle Fahrzeuge die jeweilige Strecke absolviert

haben. In nachfolgendem Bild 6-2 sind die kilometerabhängigen Ereigniswahrscheinlichkeiten der Analysemenge dargestellt. Die roten Punkte stellen die unkorrigierte empirische und die orange Linie die theoretische unkorrigierte Ereigniswahrscheinlichkeit (Weibull-verteilt) dar. Analog entsprechen die blauen Punkte der mit den Anwärtern korrigierten empirischen Ereigniswahrscheinlichkeit und die hellblaue Linie der mit den Anwärtern korrigierten theoretischen Ereigniswahrscheinlichkeit (Weibull-verteilt).

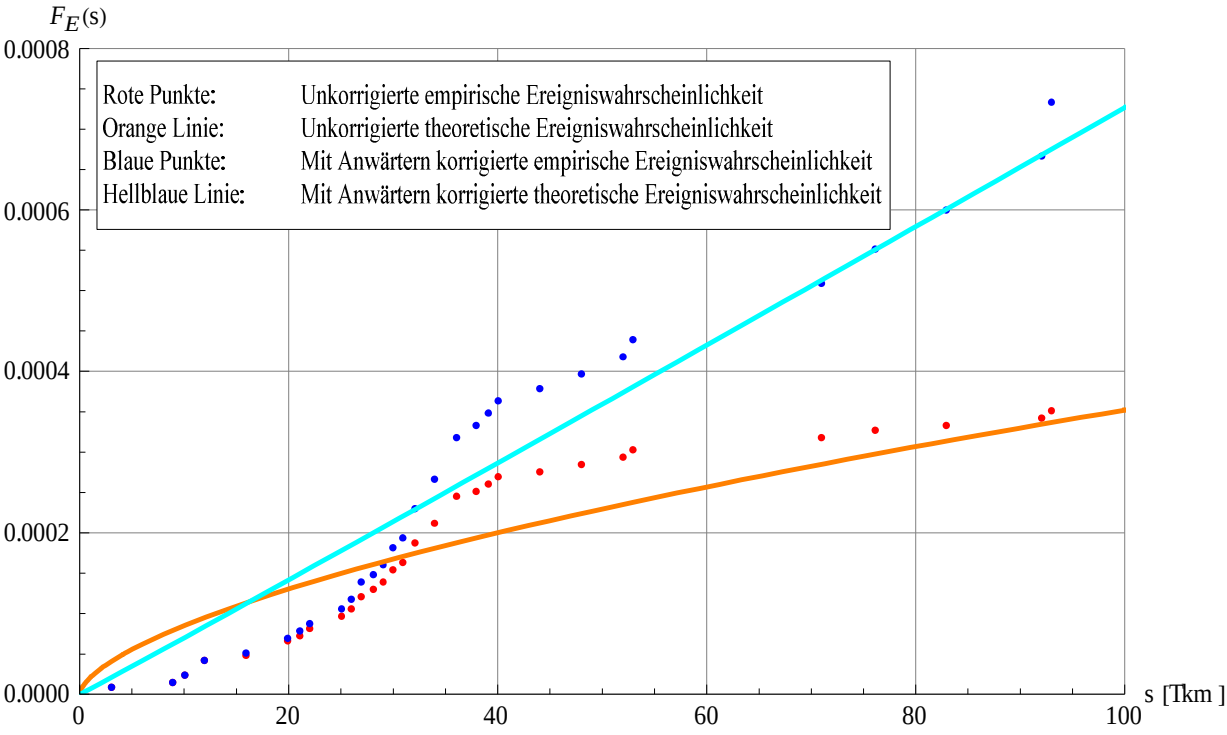


Bild 6-2: Km-abhängige Ereigniswahrscheinlichkeiten (unkorrigiert / korrigiert) der Analysemenge

Obiges Bild 6-2 zeigt, dass die Güte der Anpassung der theoretischen an die empirischen Werte in beiden Fällen nicht sehr hoch ist. Dies wird deutlich, wenn das Bestimmtheitsmaß der Anpassungen ermittelt wird. Im unkorrigierten Fall beträgt es $B = 0{,}9430$ und im korrigierten Fall wurde ein Bestimmtheitsmaß von $B = 0{,}9828$ erreicht. Die Anpassungen mit einer 2-parametrigen Weibull-Verteilung an die empirischen unkorrigierten und korrigierten Werte beschreiben den realen Verlauf folglich nicht zufrieden stellend.

Eine Möglichkeit, um eine bessere Anpassung zu erzielen, besteht darin, die Weibull-Verteilung um einen Anpassungsfaktor zu ergänzen, der die Ereigniswahrscheinlichkeit limitiert (s. Ausführungen in Abschnitt 5.4.3.1 zu der Berücksichtigung von Modellkorrekturen). Die um den Anpassungsfaktor w erweiterte Ereigniswahrscheinlichkeit

$F_E(t)$ für die Weibull-Verteilung mit den Parametern $\alpha > 0$ und $\beta > 0$ berechnet sich nach Gleichung (5-16) über

$$F_E(t) = w\left(1 - e^{-\alpha \cdot t^{\beta}}\right).$$

Nun müssen allerdings nicht nur die beiden Parameter der Weibull-Verteilung, sondern zusätzlich noch der Korrekturfaktor geschätzt werden. Auch hierzu wird die Methode der kleinsten Quadrate gewählt, wobei die lineare Regression und das Ablesen des höchsten Wertes der relativen Summenhäufigkeit den Startwert liefern.

In Bild 6-3 sind die kilometerabhängigen Ereigniswahrscheinlichkeiten mit Berücksichtigung des Anpassungsfaktors w dargestellt. Die roten bzw. blauen Punkte stellen wiederum die unkorrigierten bzw. der mit den Anwärtern korrigierten empirischen Ereigniswahrscheinlichkeiten dar. Die rote bzw. blaue Linie entspricht nun der unkorrigierten bzw. der mit den Anwärtern korrigierten theoretischen Ereigniswahrscheinlichkeit – in beiden Fällen inklusive des Anpassungsfaktors w.

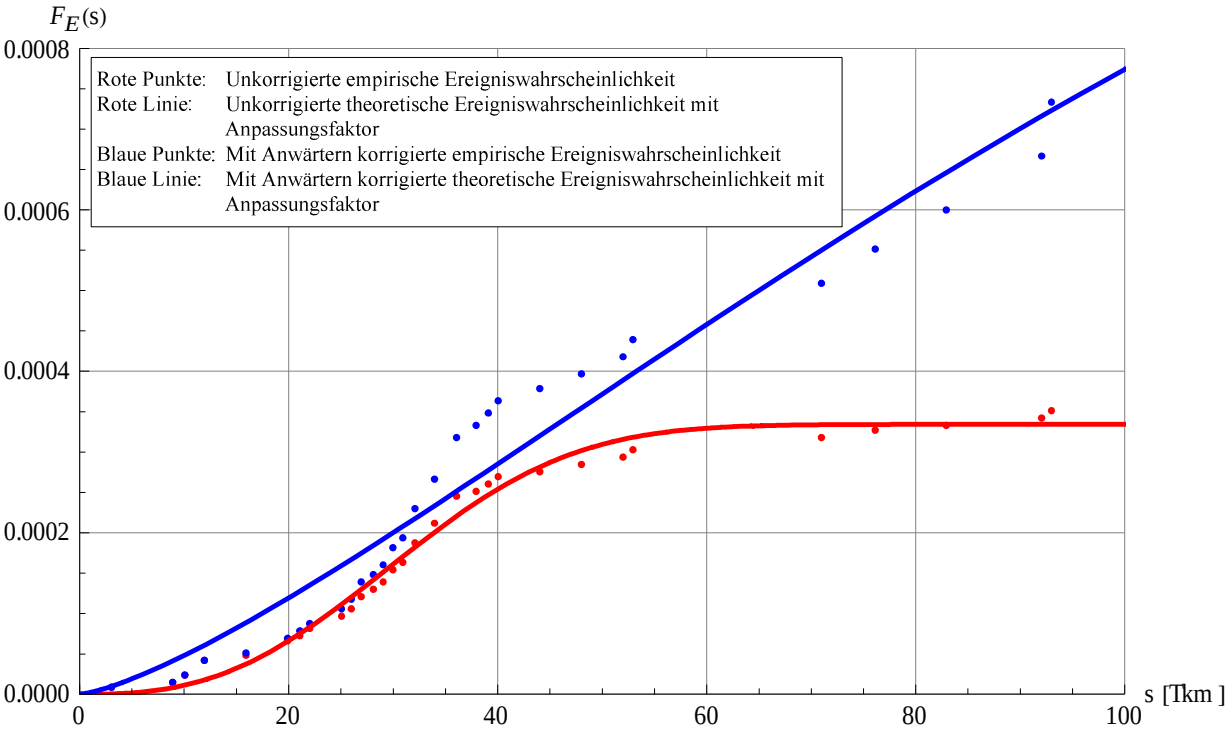


Bild 6-3: Km-abhängige Ereigniswahrscheinlichkeiten (unkorrigiert / korrigiert) der Analysemenge mit Anpassungsfaktor

Deutlich zu erkennen ist in obiger Darstellung die wesentlich bessere Anpassung im unkorrigierten Fall. Das Bestimmtheitsmaß für diese Anpassung beträgt nunmehr

$B = 0{,}9964$. Aber auch die Anpassung im korrigierten Fall ist mit $B = 0{,}9880$ besser als zuvor. Der Unterschied zwischen den Anpassungen mit und ohne Anpassungsfaktor ist in folgender Abbildung Bild 6-4 gut zu erkennen, in der alle vier Fälle dargestellt sind.

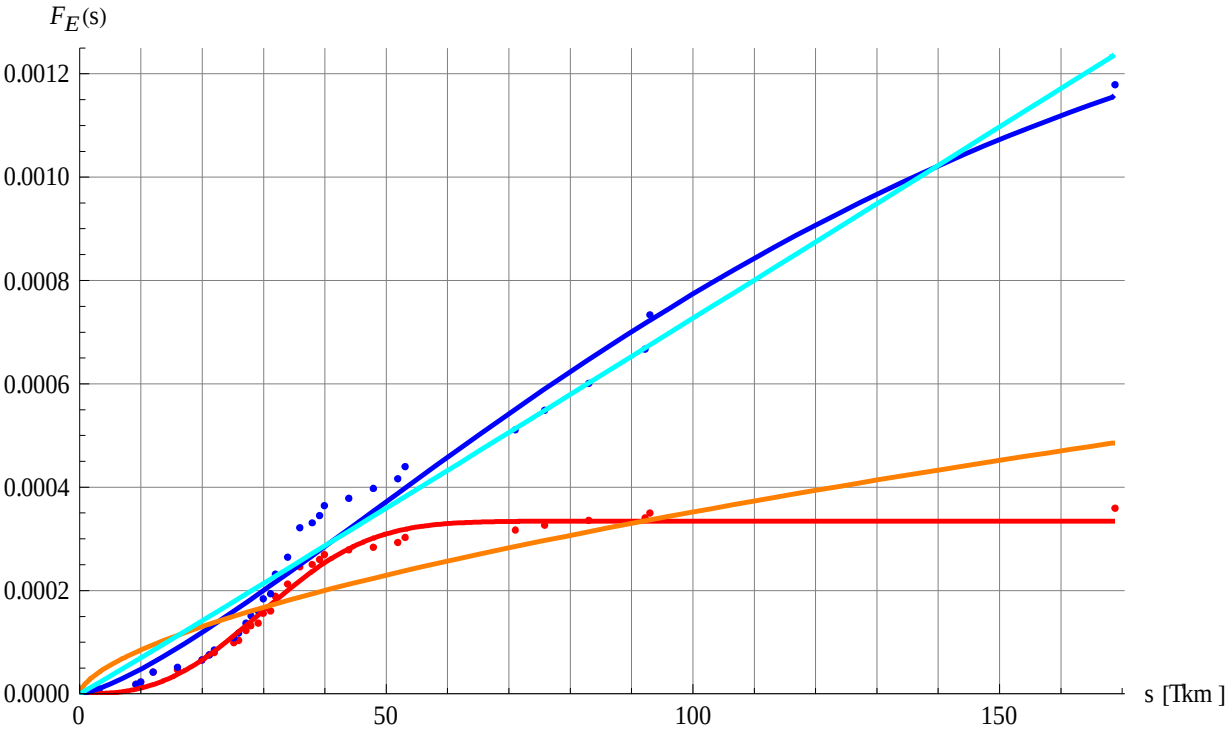


Bild 6-4: Km-abhängige Ereigniswahrscheinlichkeiten (unkorrigiert / korrigiert) der Analysemenge mit und ohne Anpassungsfaktor

Dass die Anpassungen trotz der Verwendung eines Anpassungsfaktors zwar gut, aber noch nicht sehr gut sind, liegt u.a. an einem Ereignis, das bei ca. 170 Tkm aufgetreten ist (in den vorherigen Darstellungen nicht abgebildet) und einen „Ausreißer“ darstellt. Dieser muss bei der Anpassung der theoretischen Verteilungsfunktion an die empirischen Daten allerdings mit berücksichtigt werden.

Je besser die Anpassungen der theoretischen Verteilungsfunktionen an die empirischen Werte in diesem Schritt sind, desto genauer wird das km-abhängige Verhalten abgebildet. Dies ist deswegen wichtig, da die km-abhängigen Lebensdauerverteilungen im nächsten Schritt weiter verwendet werden.

In diesem dritten Schritt wird nun mit Hilfe der zuvor gewonnenen km-abhängigen Lebensdauerverteilung und der Fahrleistungsverteilung die zeitabhängige Lebensdauerverteilung ermittelt. In folgendem Bild 6-5 sind die zeitabhängige unkorrigierte (in roter Farbe) und die zeitabhängige korrigierte (in blauer Farbe) Ereignisrate $h_E(t)$ für eine

Zeitspanne von sechs Jahren dargestellt. Bei beiden Fällen wurde der Anpassungsfaktor w berücksichtigt.

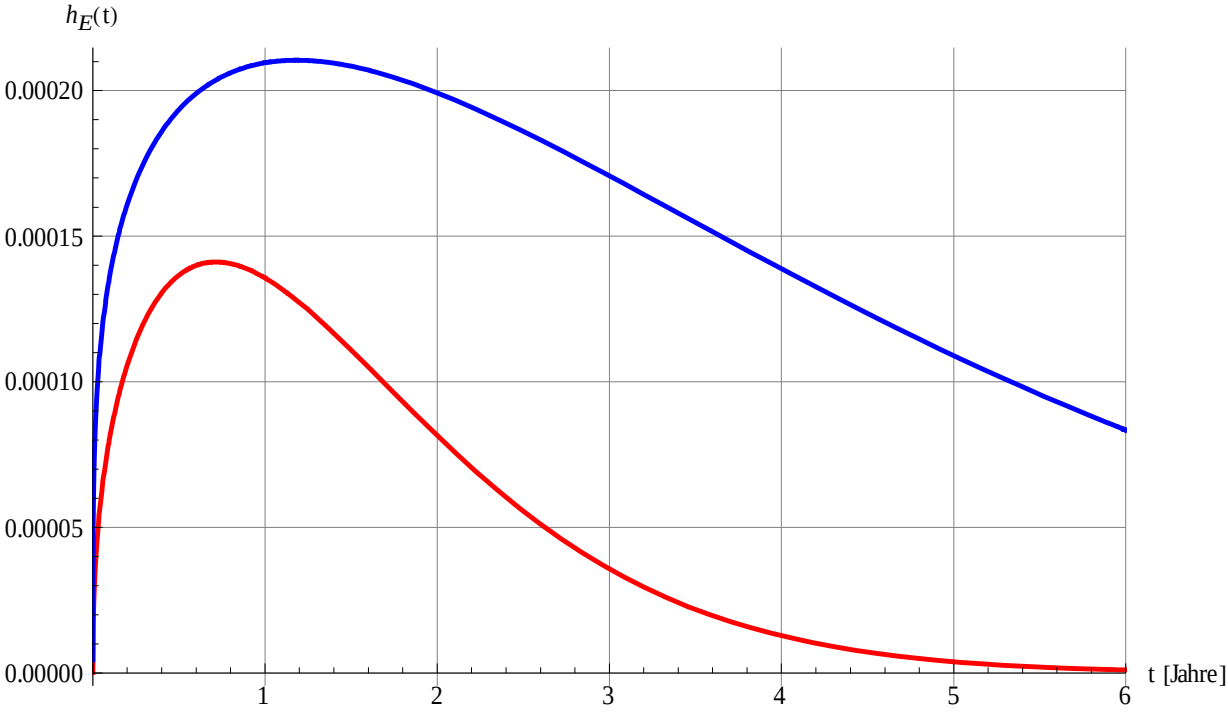


Bild 6-5: Zeitabhängige Ereignisraten (unkorrigiert / korrigiert) der Analysemenge mit Anpassungsfaktor

In obigem Bild 6-5 ist zu erkennen, dass die Ereignisrate für den unkorrigierten Fall zunächst stark ansteigt und ihr Maximum bei ca. acht Monaten erreicht. Anschließend fällt die Rate wieder bis sie nach etwa vier Jahren einen nahezu konstanten Verlauf einnimmt. Einen ähnlichen charakteristischen Verlauf besitzt auch die zeitliche Ereignisrate der mit den Anwärtern korrigierten Analysemenge.
Hierbei ist allerdings zu beachten, dass die dargestellten Ereignisraten in Bild 6-5 selbstverständlich nicht gegen Null konvergieren. Dies gilt auch für alle folgenden Darstellungen.

In nachfolgender Abbildung Bild 6-6 sind neben den bereits bekannten zeitabhängigen unkorrigierten und korrigierten Ereignisraten mit Berücksichtigung des Anpassungsfaktors auch die zeitabhängigen unkorrigierten (in oranger Farbe) und korrigierten (in hellblauer Farbe) Ereignisraten ohne Berücksichtigung des Anpassungsfaktors in einer Gegenüberstellung dargestellt.

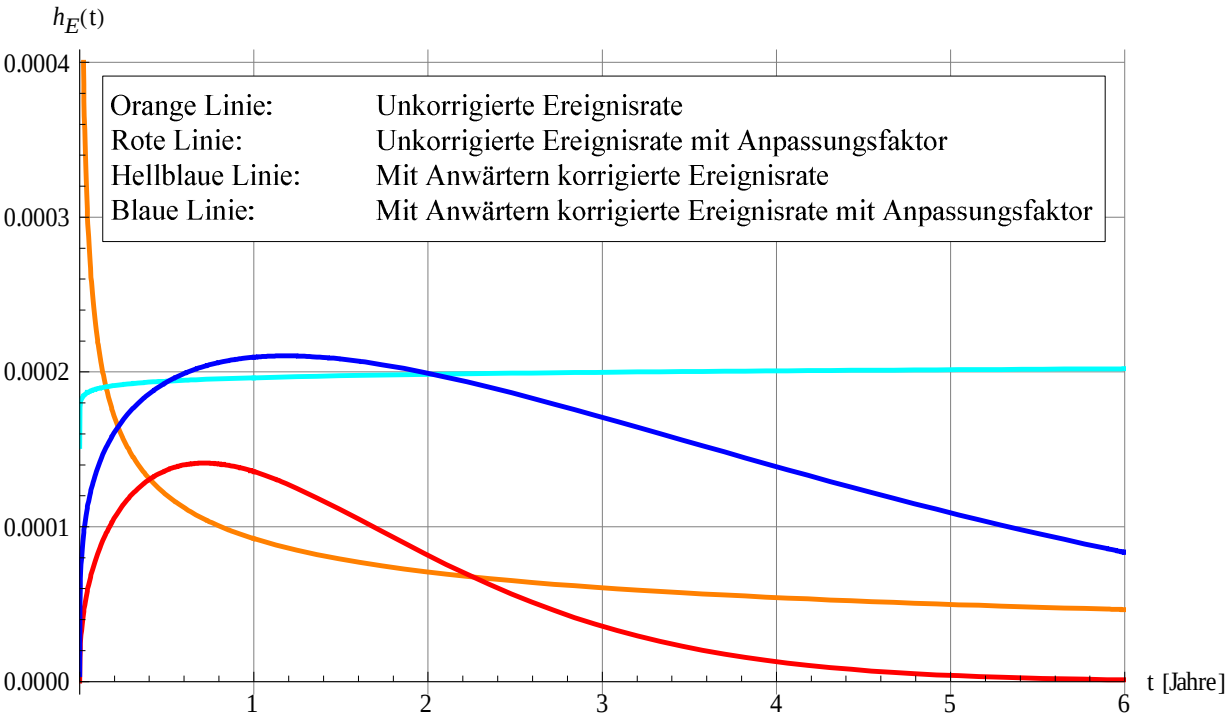


Bild 6-6: Zeitabhängige Ereignisraten (unkorrigiert / korrigiert) der Analysemenge mit und ohne Anpassungsfaktor

Bild 6-6 zeigt, dass die Ereignisraten ohne Anpassungsfaktor deutlich schneller in einen konstanten Bereich übergehen als die Ereignisraten mit Anpassungsfaktor.

Es ist allerdings noch ein weiterer Korrekturfaktor notwendig. Die eigentliche Analysemenge umfasste, wie zu Beginn dieses Abschnitts dargelegt, 46 Datensätze, wovon allerdings zwei ausgeschlossen werden mussten. Es liegt folglich eine Ausschlussquote AQ vor, die sich nach Gleichung (5-14) folgendermaßen berechnen lässt:

$$AQ = \frac{n_{Á}}{n} = \frac{2}{46} \approx 0{,}0435.$$

Die korrigierte Grundgesamtheit berechnet sich nach Gleichung (5-15) somit zu

$$n_{korr} = n_{ges} \cdot (1 - AQ) = 122.727 \cdot \left(1 - \frac{2}{46}\right) \approx 117.391.$$

Den Einfluss, den die Berücksichtigung der Ausschlussquote auf die zeitlichen Kenngrößen hat, wird in nachfolgender Abbildung 6-7 ersichtlich. Darin dargestellt sind als dicke rote bzw. dicke blaue Linie die bereits bekannten unkorrigierten bzw. mit den Anwärtern korrigierten Ereignisraten unter Berücksichtigung des Anpassungsfaktors. Die dünne rote

bzw. dünne blaue Linie stellen die nun noch zusätzlich um die Ausschlussquote korrigierten Ereignisraten dar.

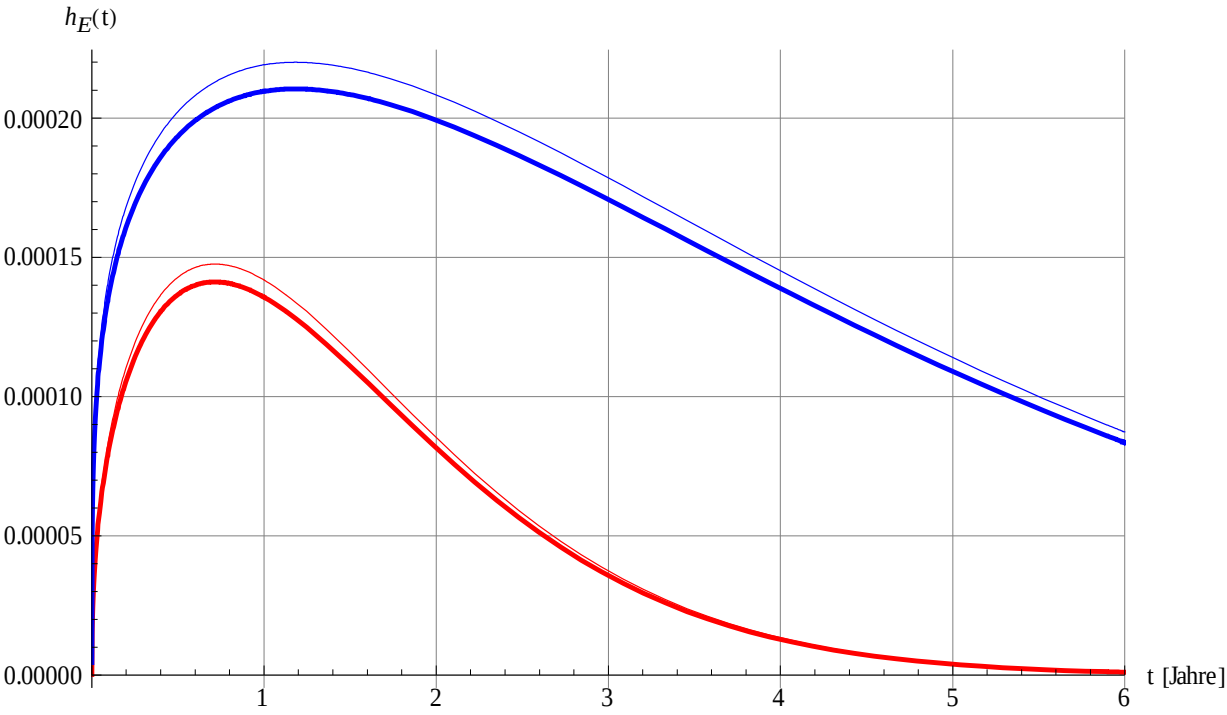


Bild 6-7: Zeitabhängige Ereignisraten (unkorrigiert / korrigiert) der Analysemenge mit Anpassungsfaktor und Ausschlussquote

In Bild 6-7 ist zu erkennen, dass die Ereignisraten, bei denen die Ausschlussquote berücksichtigt wird, jeweils leicht über den ursprünglichen Ereignisraten liegen. Dies ist allerdings auch zu erwarten, da sich die Analyse nun auf eine geringere Grundgesamtheit bezieht und dementsprechend die Ereignisrate etwas höher sein muss.

Nachfolgendes Bild 6-8 stellt die Ereigniswahrscheinlichkeiten $F_E(t)$ für den Zeitraum bis sechs Jahre dar. Darin abgebildet sind als dicke rote bzw. dicke blaue Linie die Verteilungsfunktionen für den unkorrigierten bzw. den mit den Anwärtern korrigierten Fall jeweils mit Berücksichtigung des Anpassungsfaktors. Die dünne rote bzw. dünne blaue Linie stellen die noch zusätzlich um die Ausschlussquote korrigierten Verteilungsfunktionen dar.

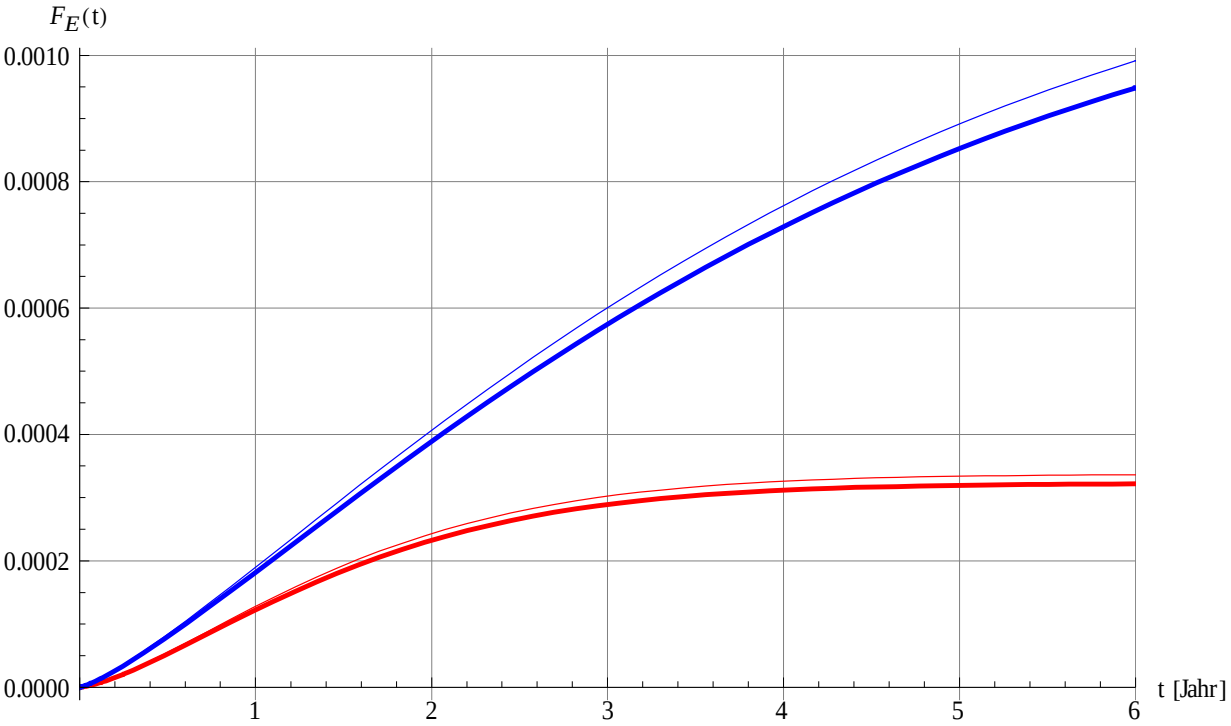


Bild 6-8: Zeitabhängige Ereigniswahrscheinlichkeiten (unkorrigiert / korrigiert) der Analysemenge mit Anpassungsfaktor und Ausschlussquote

Anhand von Bild 6-8 ist zunächst festzustellen, dass die Ereigniswahrscheinlichkeiten im korrigierten Fall größer sind als im unkorrigierten. Weiterhin sind die um die Ausschlussquote berücksichtigten Wahrscheinlichkeiten wiederum größer als die ohne Ausschlussquote. Außerdem ist ersichtlich, dass sich die Verteilungsfunktion im unkorrigierten Fall einem Wert annähert und diesen nicht überschreitet. Bei diesem Wert handelt es um den Anpassungsfaktor w, der die Ereigniswahrscheinlichkeit limitiert. Ein solcher Anpassungsfaktor wurde auch bei der Verteilungsfunktion für den mit den Anwärtern korrigierten Fall ermittelt, allerdings wirkt sich diese Beschränkung der Funktion erst zu einem späteren Zeitpunkt aus, der hier nicht dargestellt ist. Nach einer Zeit von sechs Jahren ist folglich mit einer Wahrscheinlichkeit für den Eintritt eines PiU-relevanten Ereignisses $F_E(6a)$ von ca. $0{,}99 \cdot 10^{-3}$ zu rechnen.

Die genauen Ergebnisse der ermittelten Verteilungsfunktionen mit allen relevanten Parametern für alle zuvor beschriebenen Fälle sind in Anhang A3 zu finden.

In den nachfolgenden Untersuchungen werden (sofern nicht explizit anders erwähnt) immer die unkorrigierten sowie die mit den Anwärter korrigierten Kenngrößen unter

Berücksichtigung des Anpassungsfaktors w und der Ausschussquote AQ betrachtet und angegeben.

6.3.2.2 Zerlegung der Analysemenge

Nachfolgend wird die Analysemenge aus verschiedenen Blickwinkeln betrachtet. Damit ist gemeint, dass die Datensätze nicht nur komplett als eine Menge analysiert, sondern in verschiedene Teilmengen zerlegt und dann detailliert untersucht werden. Hierbei wird das Augenmerk zunächst auf eine zeitliche Zerlegung des Produktionszeitraums gelegt, um die Güte des Prognosemodells zu überprüfen. Im Anschluss daran wird die Analysemenge in fahrzeugbezogene Teilmengen zerlegt, die wiederum einzeln untersucht werden.

A Zeitliche Zerlegung der Analysemenge

Um die Güte der durch das Wuppertaler Zuverlässigkeitsprognosemodell abgegebenen Prognose zu untersuchen ist es sinnvoll, die vorhandene Analysemenge zeitlich zu zerlegen. Dadurch können die einzelnen Ergebnisse der Prognosen und die tatsächlichen Ergebnisse miteinander verglichen werden. In Bild 6-9 ist die Zerlegung der Produktionsmonate der Analysemenge dargestellt. Nachfolgend dargestellt ist die jeweilige Anzahl der PiU-relevanten Ereignisse aufgeteilt nach den Produktionsmonaten der Fahrzeuge. Die Produktionsjahre sind hierbei anonymisiert worden.

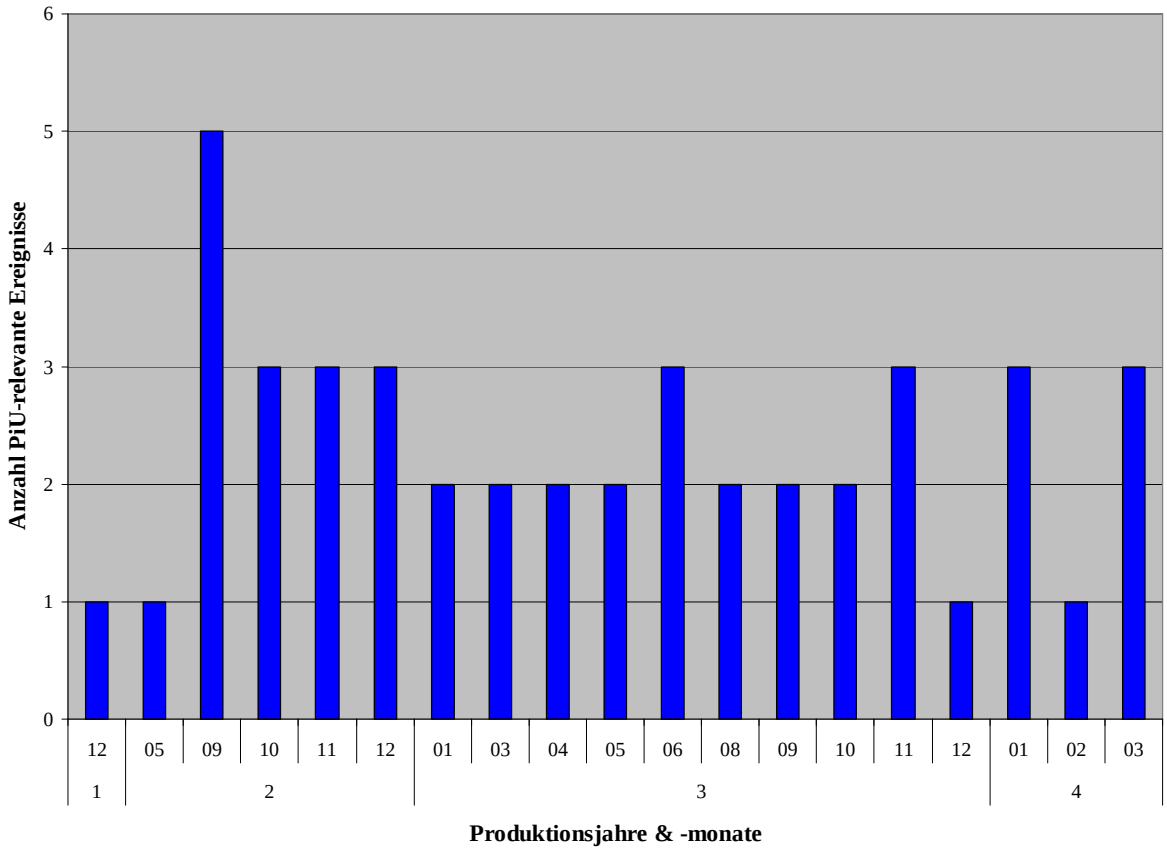


Bild 6-9: Zeitliche Zerlegung der Analysemenge nach Produktionsmonaten

In obiger Abbildung Bild 6-9 ist zunächst zu erkennen, dass sich die Produktionsmonate der Analysemenge von Dezember des Jahres 1 bis März des Jahres 4 erstrecken, also 28 Monate umfassen. Weiterhin ist ersichtlich, dass nicht in allen Monaten dieser Zeitspanne ein Fahrzeug produziert worden ist, welches ein PiU-relevantes Ereignis aufweist. Obwohl mit dem September aus dem Jahr 2 ein Produktionsmonat mit fünf PiU-relevanten Fahrzeugen vorliegt, kann festgehalten werden, dass keine signifikanten Auffälligkeiten bei der Anzahl der Ereignisse bezogen auf die Produktionsmonate vorliegen. Im Schnitt wurden pro Monat 2,3 PiU-relevante Fahrzeuge produziert, wobei nur die Monate berücksichtigt wurden, in denen auch ein PiU-relevantes Fahrzeug produziert worden ist.

Um nun die Analysemenge in mehrere, vom Umfang her möglichst gleich große Abschnitte zu unterteilen, kann der erste Abschnitt von Dezember Jahr 1 bis Dezember Jahr 2 (16 Ereignisse), der zweite Abschnitt von Januar bis September Jahr 3 (15 Ereignisse) und somit der letzte Abschnitt von Oktober Jahr 3 bis März Jahr 4 (13 Ereignisse) reichen. Es ergeben sich die nachfolgenden zeitlichen Aufteilungen der Produktionsmonate der Analysemenge.

- *Analysemenge Zeitmenge 1:*
  - Umfang: Dezember Jahr 1 bis Dezember Jahr 2 (13 Fertigungsmonate)
  - Fertigungsmenge: 63.875 Fahrzeuge
  - Datenanzahl: 16 Ereignisse
- *Analysemenge Zeitmenge 2:*
  - Umfang: Dezember Jahr 1 bis September Jahr 3 (22 Fertigungsmonate)
  - Fertigungsmenge: 101.358 Fahrzeuge
  - Datenanzahl: 31 Ereignisse
- *Analysemenge Zeitmenge 3:*
  - Umfang: Dezember Jahr 1 bis März Jahr 4 (28 Fertigungsmonate)
  - Fertigungsmenge: 122.727 Fahrzeuge
  - Datenanzahl: 44 Ereignisse

Diese drei zeitlichen Mengen sind in der Übersicht in nachfolgendem Bild 6-10 graphisch gegenübergestellt.

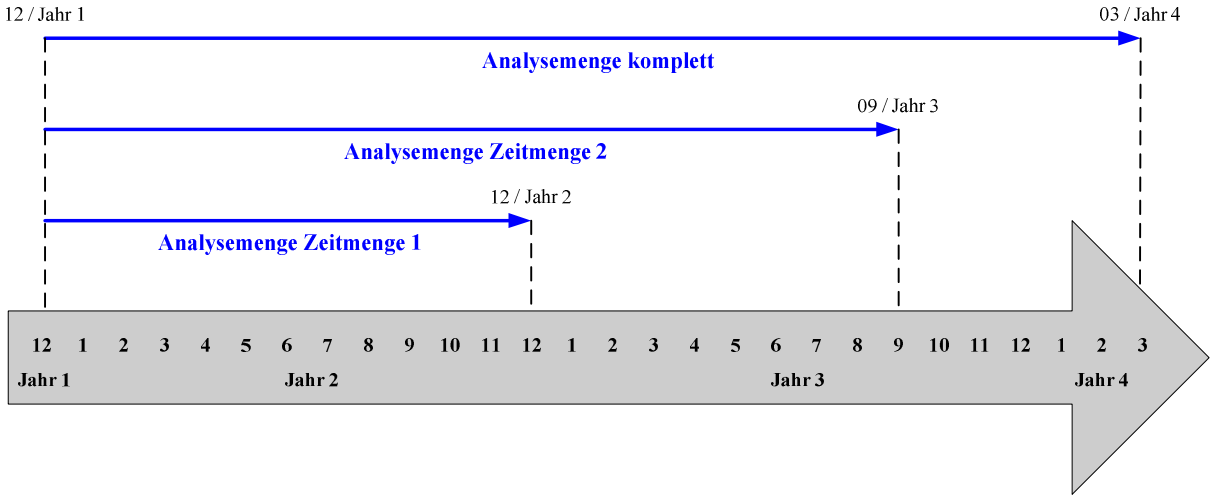


Bild 6-10: Übersicht der zeitlichen Zerlegungen der Analysemenge

Bild 6-10 zeigt, dass die zeitliche Menge 1 die Daten von etwas mehr als einem Jahr enthält. Die Zeitmenge 2 beinhaltet den Abschnitt 1 sowie zusätzlich die Daten der nächsten neun Produktionsmonate. Die zeitliche Menge 3 ist gleich der gesamten Analysemenge und

umfasst den gesamten Abschnitt 2 inklusive der nächsten sechs Produktionsmonate. Diese drei Datenmengen werden nun im Wuppertaler Zuverlässigkeitsprognosemodell untersucht.

Nachfolgendes Bild 6-11 stellt die Ergebnisse dieser Analysen dar, wobei die roten Kurven die unkorrigierten und die blauen Kurven die korrigierten Ereignisraten zeigen. Die Ergebnisse der Zeitmenge 1 werden dabei durch die grob gepunkteten Linien repräsentiert, die des zeitlichen Abschnitts 2 durch die fein gepunkteten und die bereits bekannten Ergebnisse der kompletten Analysemenge durch die durchgezogene Linien.

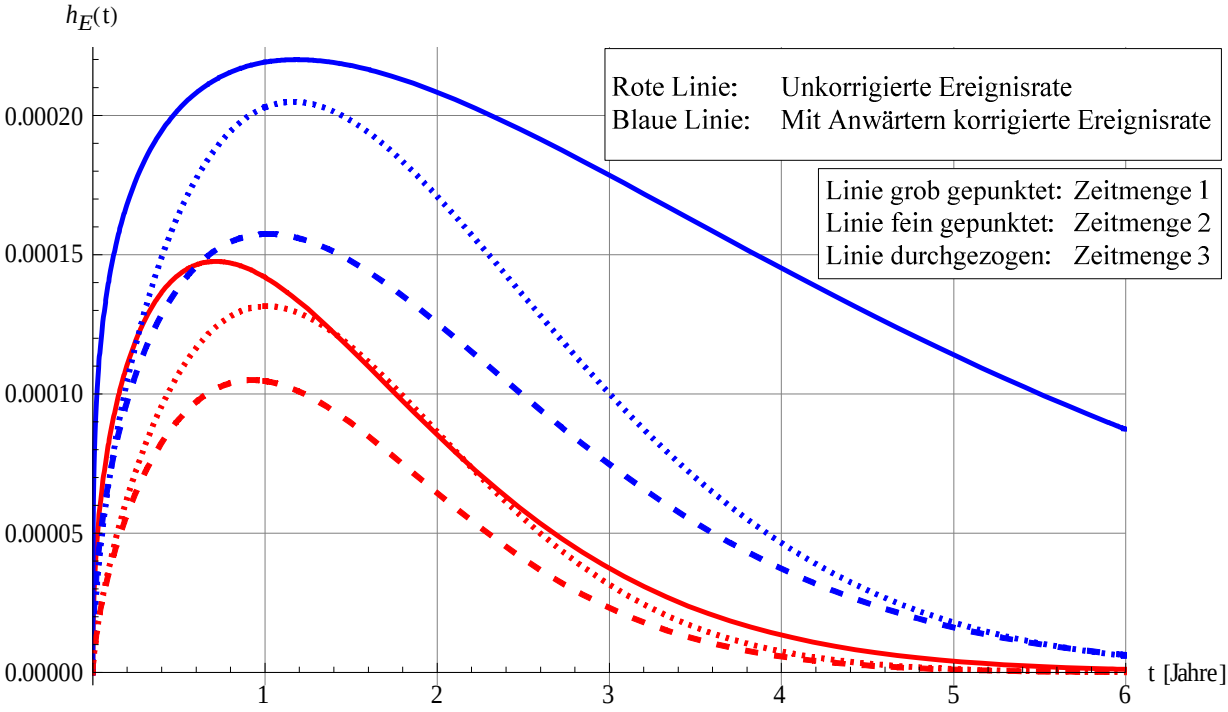


Bild 6-11: Zeitabhängige Ereignisrate (unkorrigiert / korrigiert) der zeitlichen Zerlegung der Analysemenge

In Bild 6-11 ist zunächst zu erkennen, dass alle korrigierten Ereignisraten erwartungsgemäß oberhalb der jeweiligen unkorrigierten Rate liegen. Alle Kurvenverläufe weisen weiterhin einen ähnlich charakteristischen Verlauf auf. Zunächst steigt die Rate stark an, um nach Erreichen eines Maximums wieder abzufallen, ehe sie in eine nahezu konstante Phase übergeht. Weiterhin ist zu erkennen, dass sich die Maximalwerte aus zeitlicher Sicht in einem ähnlichen Bereich befinden, für die unkorrigierten Raten im Bereich von 8 bis 12 Monaten und für die korrigierten Raten im Bereich von 12 bis 15 Monaten. Außerdem ist ersichtlich, dass sowohl bei den unkorrigierten als auch bei den korrigierten Ereignisraten die Ergebnisse

der Zeitmenge 1 (grob gepunktet) unterhalb der Ergebnisse von Zeitmenge 2 (fein gepunktet) und diese wiederum unterhalb von Zeitmenge 3 (durchgezogen) liegen. Lediglich die unkorrigierte Ereignisrate der Zeitmenge 2 liegt in dem Zeitraum von ca. 1,5 Jahren bis etwas über 2 Jahren knapp oberhalb der Ereignisrate der Zeitmenge 3.

Genauere Einblicke in die zeitlichen Ergebnisse werden gewonnen, wenn die Darstellung aus Bild 6-11 gefiltert wird. Damit ist gemeint, dass beispielsweise die korrigierte Ereignisrate der kompletten Analysemenge für diese Betrachtung nicht relevant ist, da mit ihr keine Erkenntnisse hinsichtlich der Güte der durchgeführten Prognose getroffen werden können. Gleiches gilt z.B. für die unkorrigierte Ereignisrate der Zeitmenge 1. In nachfolgendem Bild 6-12 sind lediglich die für einen solchen Vergleich relevanten Ereignisraten dargestellt. Dabei handelt es sich um

- die korrigierte Ereignisrate der Zeitmenge 1 (blaue grob gepunktete Linie),
- die unkorrigierte Ereignisrate der Zeitmenge 2 (rote fein gepunktete Linie),
- die korrigierte Ereignisrate der Zeitmenge 2 (blaue fein gepunktete Linie) sowie
- die unkorrigierte Ereignisrate der Zeitmenge 3 (rote durchgezogene Linie).

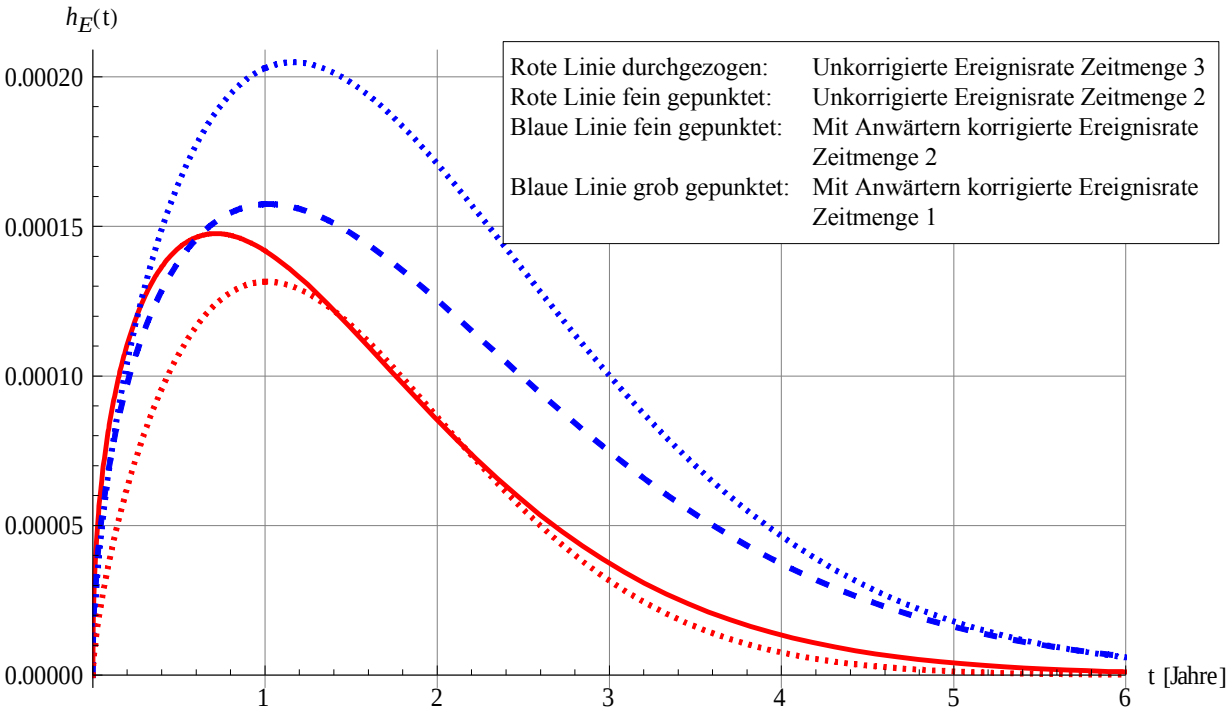


Bild 6-12: Gefilterte Darstellung der zeitabhängigen Ereignisraten der zeitlichen Zerlegung der Analysemenge

Wird das Augenmerk zunächst auf den Vergleich der Prognose aus den Datensätzen der ersten 13 Produktionsmonate (korrigierte Ereignisrate Zeitmenge 1) mit dem tatsächlichen Verhalten aus den ersten 22 Fertigungsmonaten (unkorrigierte Ereignisrate Zeitmenge 2) gelegt, so fällt auf, dass die getroffene Prognose konservativer ist als die tatsächlich vorliegende Rate. Dies ist ein zufrieden stellendes Ergebnis. Wenn die Prognose beispielsweise unterhalb des tatsächlichen zeitlichen Verhaltens liegen würde, wäre dies ein Indiz für ein fehlerhaftes Modell. Auch der Vergleich der Prognose aus den ersten 22 Fertigungsmonaten (Zeitmenge 2) mit dem realen Verhalten der gesamten 28 Produktionsmonate (Zeitmenge 3) führt zu dem Schluss, dass das Prognosemodell vernünftige Ergebnisse liefert, denn auch die prognostizierte Ereignisrate liefert konservativere Ergebnisse als sie letztendlich aufgetreten sind.

Die genauen Ergebnisse der ermittelten Verteilungsfunktionen für die zeitlichen Zerlegungen der Analysemenge mit allen relevanten Parametern sind in Anhang A4 zu finden.

B Fahrzeugbezogene Zerlegung der Analysemenge

In Abschnitt 6.3.1 wurden bereits die Ergebnisse der ermittelten Fahrleistungsverteilungen aus den gesamten GuK-Daten für die PiU-relevante Baureihe dargelegt. Diese werden nun bei der fahrzeugbezogenen Zerlegung der Analysemenge weiter verwendet. Die Analysemenge kann bei dieser Zerlegung auf zwei unterschiedliche Arten im Prognosemodell untersucht werden:

- Fall A: FLV aus Analysemenge ermittelt und
- Fall B: FLV aus GuK-Daten ermittelt.

Für den Fall A wird die benötigte Fahrleistungsverteilung aus den Datensätzen der Analysemenge direkt ermittelt. Hierzu ist anzumerken, dass es möglich sein kann, dass zwei unterschiedliche Kilometerstandsangaben mit unterschiedlichen Terminen zur Verfügung stehen: einmal die aus den GuK- und einmal die aus den Diagnosedaten. Diese Fahrleistungen sind im Idealfall identisch, müssen dies aber nicht sein. Für die analysierte Schnittmenge des Kandidaten (46 Datensätze ohne Ausschluss der zwei unplausiblen Datensätze) waren bei 20 Datensätzen die Kilometerangaben gleich, in 17 Fällen waren die Angaben der GuK-Daten größer und neunmal die Angaben der Diagnosedaten. Die Unterschiede waren dabei teilweise erheblich (bis zu über 300 km). Dies lässt sich dadurch erklären, dass das Datum der Diagnose und das GuK-Reparaturdatum nicht übereinstimmen müssen. Dadurch kann in der

Zwischenzeit eine gewisse Fahrleistung zusätzlich hinzukommen. Mögliche Erklärungen hierfür sind z.B. Überprüfungsfahrten in der entsprechenden Werkstatt oder die Durchführung der GuK-Reparatur und der Diagnose in unterschiedlichen und örtlich getrennten Werkstätten. Wie groß diese Fahrleistungsdifferenz in der Praxis sein kann, wurde im Rahmen der vorliegenden Arbeit nicht weiter untersucht. Stattdessen werden im Prognosemodell vier mögliche Varianten untersucht, die sich wie folgt zusammensetzen:

- Reparaturdatum mit zugehöriger Fahrleistung,
- Startdatum Diagnose mit zugehöriger Fahrleistung,
- früheres Datum mit zugehöriger Fahrleistung (bei gleicher Datumsangabe wurde die kleinere Fahrleistung gewählt) und
- späteres Datum mit zugehöriger Fahrleistung (bei gleicher Datumsangabe wurde die größere Fahrleistung gewählt).

Als Fazit dieser Analysen muss festgehalten werden, dass es keinen signifikanten Einfluss auf die Ergebnisse hat, welche Datumsangaben mit welcher Fahrleistung in der Analysemenge enthalten sind. Die Abweichungen in den Resultaten sowohl bei der Ermittlung der Fahrleistungsverteilungen als auch bei der Bestimmung der zeitabhängigen Kenngrößen sind zu vernachlässigen. Dies kann dadurch begründet werden, dass die zeitlichen Differenzen sowie die Unterschiede bei den Fahrleistungen nicht groß genug sind, als dass sie ins Gewicht fallen könnten. Genauere Informationen zu den Resultaten der Analysen der vier Varianten sind in Anhang A6 in einer Gegenüberstellung zu finden. Für die nachfolgenden Untersuchungen wird jeweils das Reparaturdatum des GuK-Bereichs mit der entsprechenden Kilometerangabe verwendet.

Für den Fall B werden die Fahrleistungsverteilungen aus allen GuK-Daten bestimmt (s. Ausführungen in Abschnitt 6.3.1) und anschließend in das Prognosemodell implementiert. Dies wird nachfolgend mit „FLV übergeben“ kenntlich gemacht. Die Analysemenge wird nun hinsichtlich einer möglichen fahrzeugbezogenen Klasseneinteilung untersucht. Die Anteile der relevanten Fahrzeugmodelle innerhalb der Analysemenge sind in nachfolgendem Bild 6-13 dargestellt.

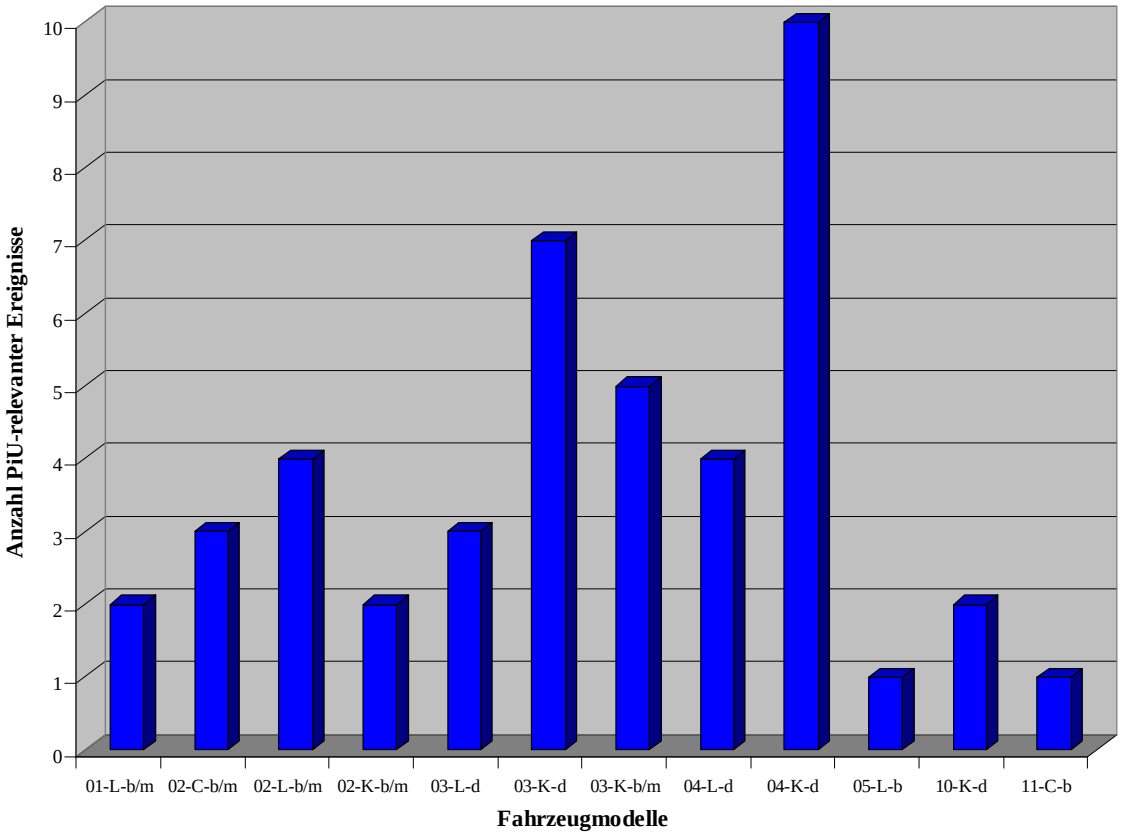


Bild 6-13: Fahrzeugbezogene Zerlegung der Analysemenge nach Fahrzeugmodellen

Aus Bild 6-13 ist zu entnehmen, dass sich die Analysemenge mit ihren 44 Ereignissen aus insgesamt 12 Fahrzeugmodellen zusammensetzt. Dabei ist das Modell 04-K-d mit zehn Einträgen am häufigsten vertreten. Fünf Modelle (01-L-b/m, 02-K-b/m, 05-L-b, 10-K-d und 11-C-b) sind nur ein- oder zweimal vorhanden. Somit ist es nicht sinnvoll, eine modellbezogene Clusterung (Klasse 1: 01-L-b/m, Klasse 2: 02-C-b/m, Klasse 3: 02-L-b/m etc.) vorzunehmen, da dies eine zu geringe Anzahl an Fahrzeugen und somit Ereignissen in manchen Klassen zur Folge hätte. Die Klasseneinteilung kann, wie in Abschnitt 6.3.1 erklärt, unter Berücksichtigung von technischen und statistischen Gesichtspunkten vorgenommen werden. Die Ergebnisse dieser Clusterung sind in nachfolgendem Bild 6-14 dargestellt.

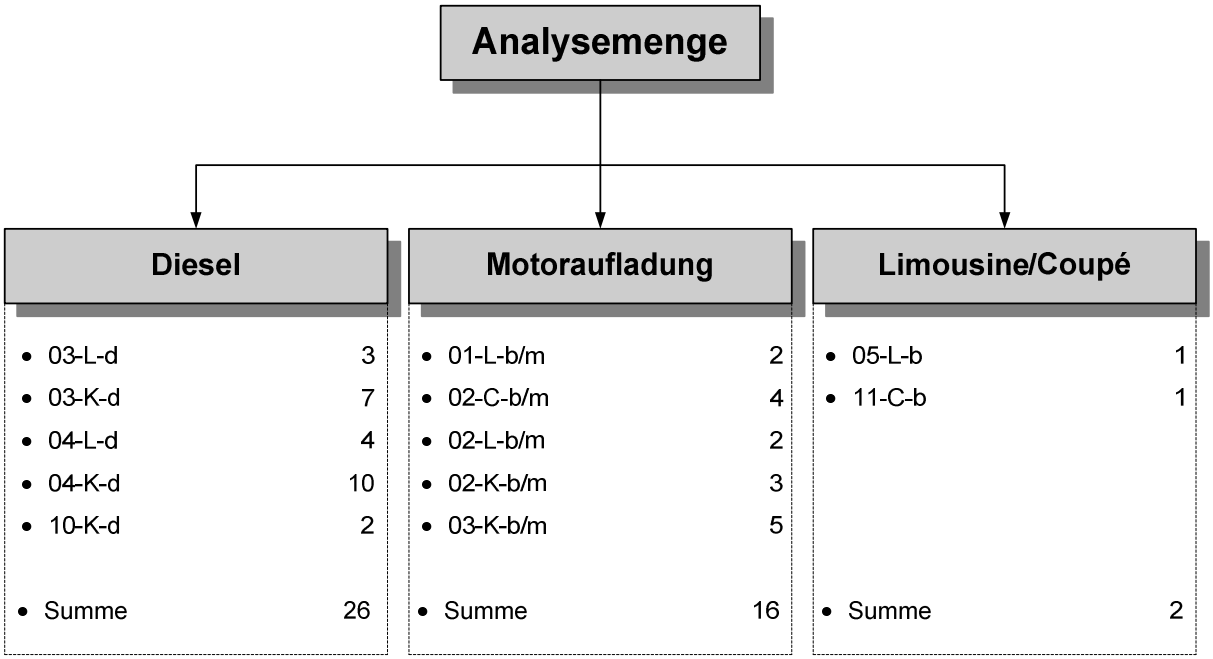


Bild 6-14: Fahrzeugbezogene Clusterung der Analysemenge

In Darstellung 6-14 ist zu erkennen, dass es zwei größere und eine kleine Klasse gibt. Die erste Klasse umfasst die 26 Diesel-Fahrzeuge der Analysemenge und zwar unabhängig davon, ob es sich um eine Limousine oder ein Kombifahrzeug handelt. Diese Fahrzeuge weisen alle eine ähnliche FLV auf (s. Ergebnisse in Tabelle 6-1 und Tabelle 6-2). Die zweite Klasse beinhaltet alle 16 Fahrzeuge, die über eine Motoraufladung verfügen, und zwar wiederum unabhängig davon, ob es sich um eine Limousine oder ein Kombifahrzeug handelt. In dieser Klasse ist außerdem ein Coupé vorhanden, das aufgrund der technischen Äquivalenz zugeordnet wurde. Das dritte Cluster umfasst zwei Fahrzeuge mit Benzinmotoren, die keinem der beiden zuvor genannten Clustern zugeordnet werden konnten.

Für die beiden großen Klassen (Diesel und Motoraufladung) müssen die zugehörige FLV (mit Hilfe der MCS) sowie die Fertigungsmenge für das relevante Produktionsintervall bestimmt werden. Die beiden Cluster werden anschließend separat im Prognosemodell untersucht. Die Ergebnisse dieser Analysen werden mit den Ergebnissen der gesamten Analysemenge verglichen. Eine eigenständige Untersuchung des dritten Clusters ist nicht sinnvoll, da diese Klasse nur zwei Datensätze umfasst und eine Analyse im Prognosemodell keine verwertbaren Ergebnisse liefern würde. Die Ergebnisse der Ermittlungen der für die Prognose der beiden Cluster notwendigen Informationen sind in nachfolgender Tabelle 6-4 gegenübergestellt. Der Vollständigkeit halber sind dort auch die Ergebnisse für das dritte Cluster mit angegeben.

Tabelle 6-4: Informationen zu den fahrzeugbezogenen Clustern

Cluster	Parameter der theoretischen jährlichen FLV		E(S) [Tkm]	Fertigungsmenge
	μ	σ		
Diesel	3,1066	0,62117	27,10	71.673
Motoraufladung	2,5683	0,52603	14,98	49.077
Limousine/Coupé	2,5730	0,53308	15,11	1.977
Analysemenge	2,9063	0,64262	22,48	122.727

In Tabelle 6-4 sind außerdem die Ergebnisse der angepassten Fahrleistungsverteilung für die gesamte Analysemenge angeführt. Es ist zu erkennen, dass diese FLV teils sehr deutlich von den Fahrleistungsverteilungen der beiden Cluster abweicht. Wie bereits in Abschnitt 6.3.1 für die PiU-relevante Baureihe beschrieben, ist es nicht sinnvoll, die FLV für die gesamte Analysemenge zu übergeben.

In folgendem Bild 6-15 sind die unkorrigierten (hellblau) und die mit den Anwärtern korrigierten (blau) zeitbezogenen Ereignisraten des Diesel-Clusters für die Fälle A (dicke Linie) und B (dünne Linie) dargestellt.

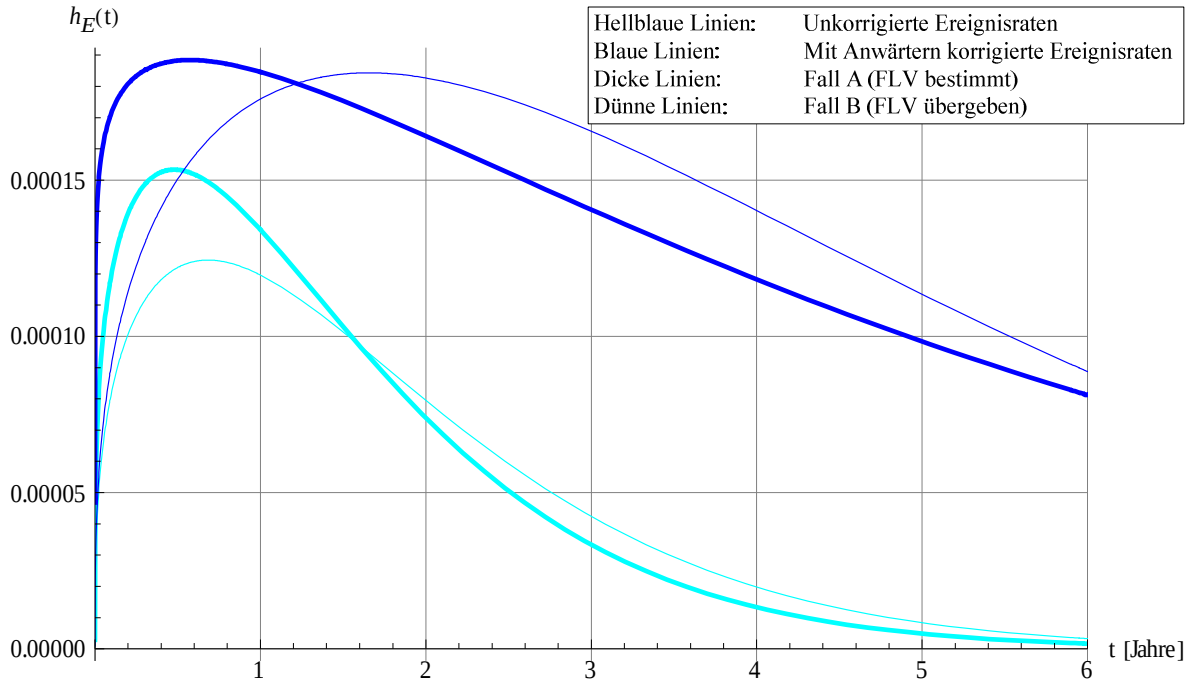


Bild 6-15: Zeitliche Ereignisraten (unkorrigiert / korrigiert) des Clusters Diesel für beide Fälle

Bild 6-15 zeigt, dass die Kurvenverläufe der Ereignisraten von Fall A und Fall B zwar sowohl für den unkorrigierten als auch den korrigierten Fall eine ähnliche Charakteristik aufweisen, jedoch durchaus unterschiedlich sind. So weist die unkorrigierte Ereignisrate für Fall A einen höheren Maximalwert auf als die entsprechende Rate im Fall B. Auffällig ist weiterhin, dass die Maximalwerte der mit den Anwärtern korrigierten Ereignisraten fast gleich groß sind. Die unkorrigierten Ereignisraten weisen bei den Maximalwerten einen erkennbaren Unterschied auf. Darüber hinaus werden im Fall A die Maximalwerte der Ereignisraten sowohl im unkorrigierten als auch im korrigierten Fall zu einem ähnlichen Zeitpunkt eingenommen, bei Fall B erreicht die korrigierte Ereignisrate ihr Maximum rund ein Jahr später als die unkorrigierte Rate.

In folgender Abbildung 6-16 sind die unkorrigierten (orange) und die mit den Anwärtern korrigierten (rot) zeitbezogenen Ereignisraten des Clusters Motoraufladung für die Fälle A (dicke Linie) und B (dünne Linie) dargestellt.

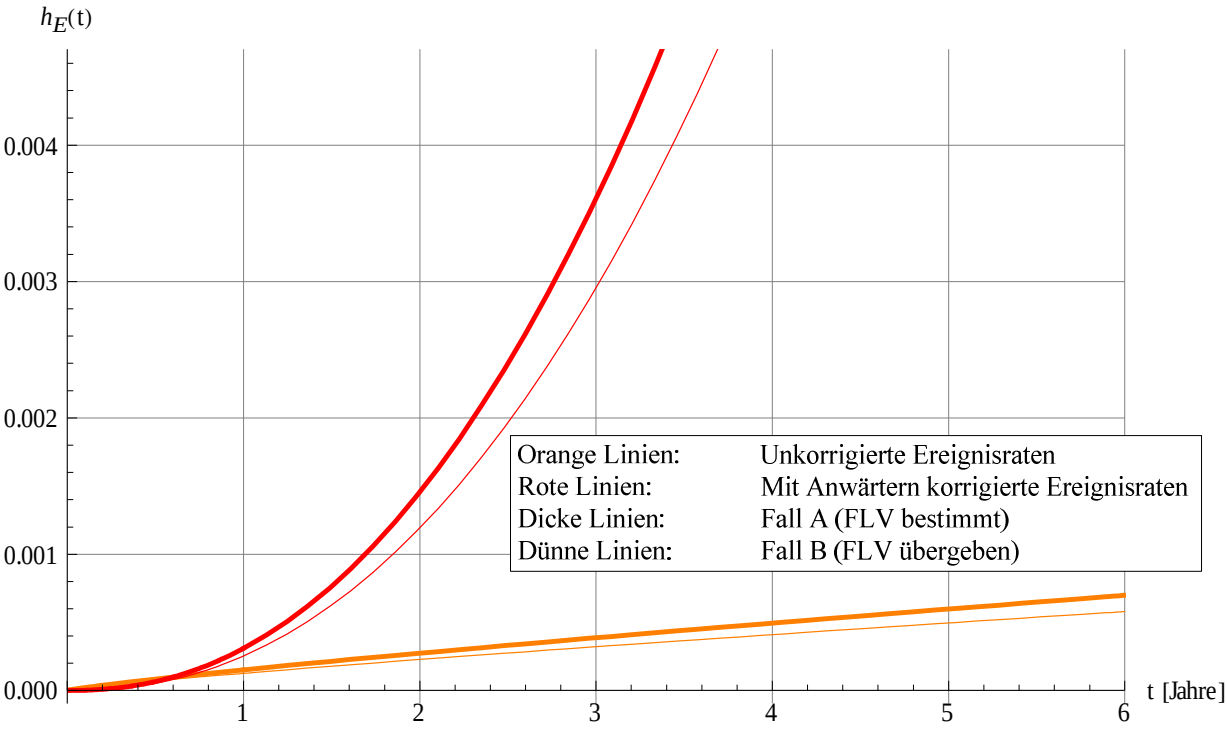


Bild 6-16: Zeitliche Ereignisraten (unkorrigiert / korrigiert) des Cluster Motoraufladung für beide Fälle

An den Darstellungen in Bild 6-16 fällt zunächst auf, dass die Kurvenverläufe der Ereignisraten (sowohl korrigiert als auch unkorrigiert) eine deutlich andere Charakteristik aufweisen als die ermittelten Ereignisraten zuvor. Für alle Fälle muss eine stetig steigende Ereignisrate festgestellt werden. Dies begründet sich dadurch, dass bei der Anpassung der

Datensätze des Clusters der Fahrzeuge mit Motoraufladung der Korrekturfaktor die Güte der Anpassung der theoretischen an die empirischen Werte bei den kilometerabhängigen Kenngrößen nicht verbesserte (s. auch Ergebnisse in Anhang A5). Weiterhin ist zu erkennen, dass sowohl bei den unkorrigierten als auch den korrigierten Ergebnissen die Ereignisraten für den Fall A (Fahrleistungsverteilung bestimmt) leicht höher sind als die Ereignisraten für Fall B (FLV übergeben).

In den beiden nachfolgenden Darstellungen sind die Ergebnisse der Untersuchung der fahrzeugbezogenen Zerlegung der Analysemenge in Form der zeitlichen Ereignisraten zum Vergleich gegenübergestellt. Hierbei wird zwischen den Ergebnissen für Fall A (Bild 6-17) und Fall B (Bild 6-18) unterschieden. Das Cluster Diesel ist dabei in beiden Fällen in den bläulichen Farben, das Cluster Motoraufladung in den rötlichen Farben und die Analysemenge in schwarzer bzw. grauer Farbe dargestellt.

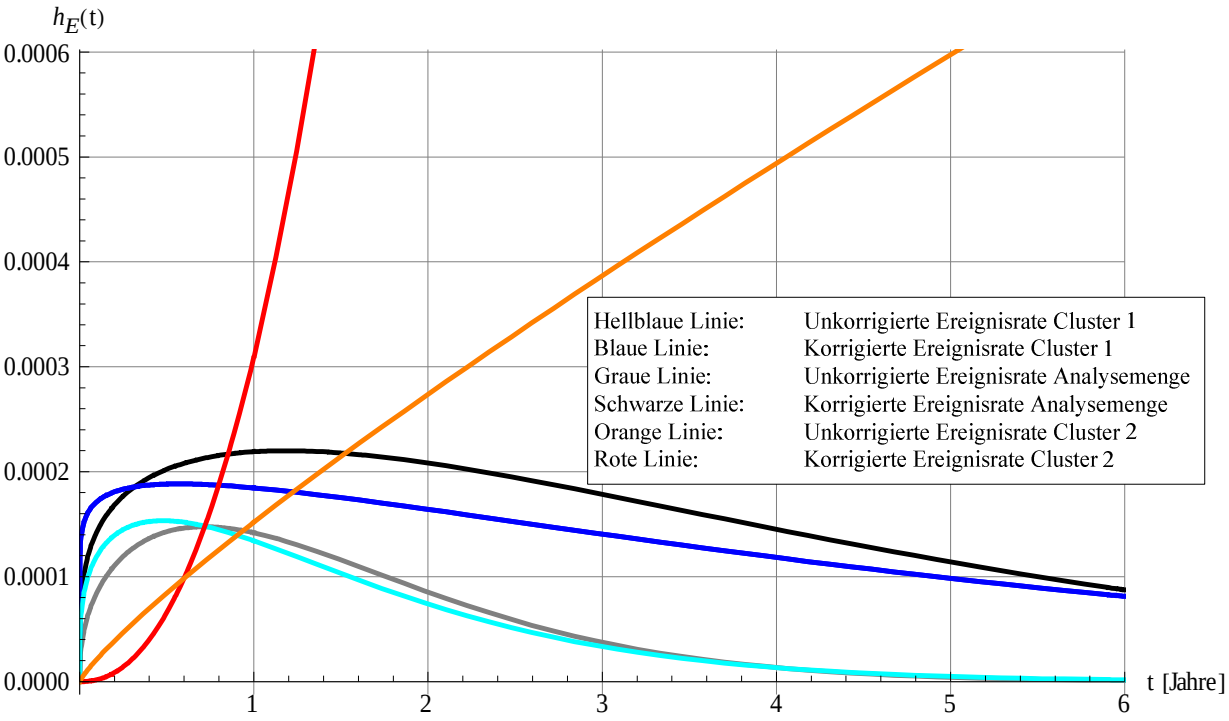


Bild 6-17: Zeitliche Ereignisraten (unkorrigiert / korrigiert) der beiden Cluster und der Analysemenge für den Fall A (FLV bestimmt)

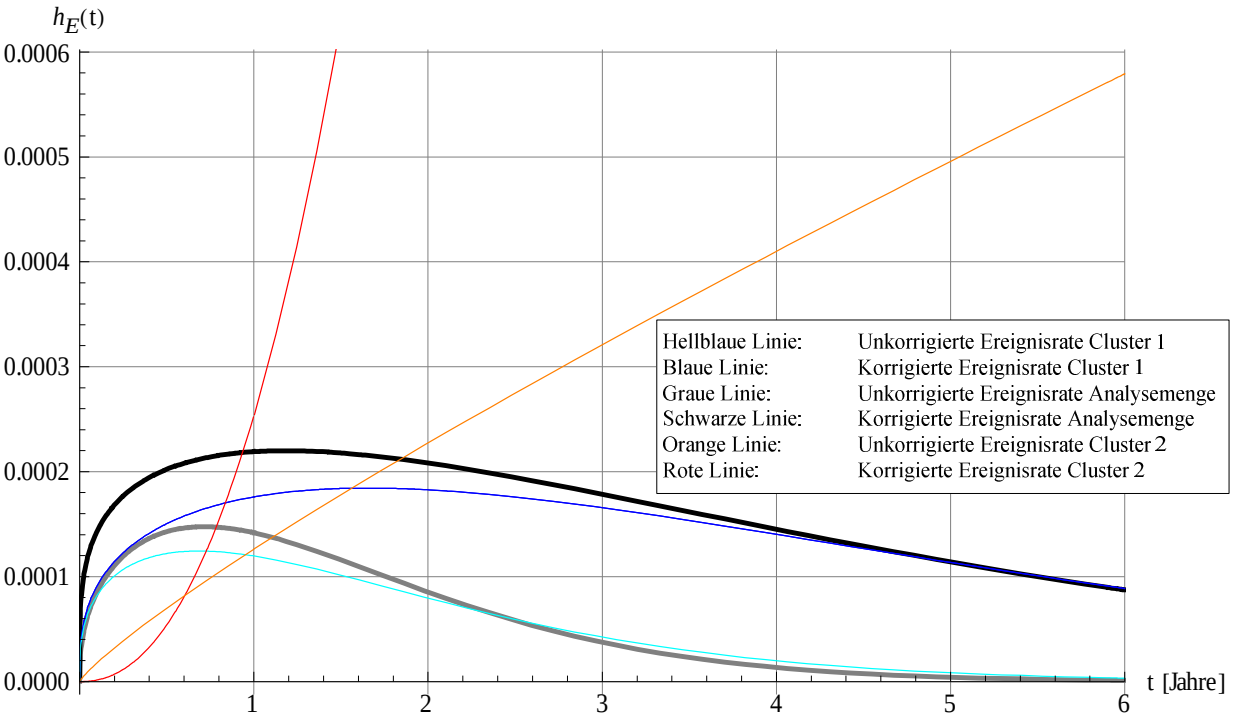


Bild 6-18: Zeitliche Ereignisraten (unkorrigiert / korrigiert) der beiden Cluster und der Analysemenge für den Fall B (FLV übergeben)

In beiden vorstehenden Abbildungen ist zu erkennen, dass die Ereignisraten für das Diesel-Cluster einen sehr ähnlichen Verlauf zu den Ereignisraten der Analysemenge aufweisen. Dies wird noch deutlicher, wenn das Augenmerk auf die Ereignisraten des Clusters Motoraufladung gelegt wird, welche eine völlig andere Charakteristik zeigen.
Zu den Darstellungen muss festgehalten werden, dass die Ereignisraten der Analysemenge in Bild 6-18 für den Fall A und nicht für den Fall B, wie die anderen Raten, dargestellt sind. Wie in Abschnitt 6.3.1 beschrieben und in Tabelle 6-4 ersichtlich, ist es nicht sinnvoll, die Fahrleistungsverteilung für die Analysemenge zu übergeben. Aus diesem Grund sind in beiden Abbildungen 6-18 und 6-19 die unkorrigierten und korrigierten Ereignisraten der Analysemenge für den Fall, dass die FLV direkt aus den Datensätzen der Analysemenge ermittelt worden ist, angegeben (dicke Linien).

Die Verteilungsfunktionen $F_E(t)$ der beiden Cluster für den Fall, dass die Fahrleistungsverteilung aus den gesamten GuK-Daten ermittelt worden ist, sind in Bild 6-19 denen der Analysemenge gegenübergestellt. Die farblichen Darstellungen der Funktionen sind dabei dieselben wie zuvor bei den Ereignisraten.

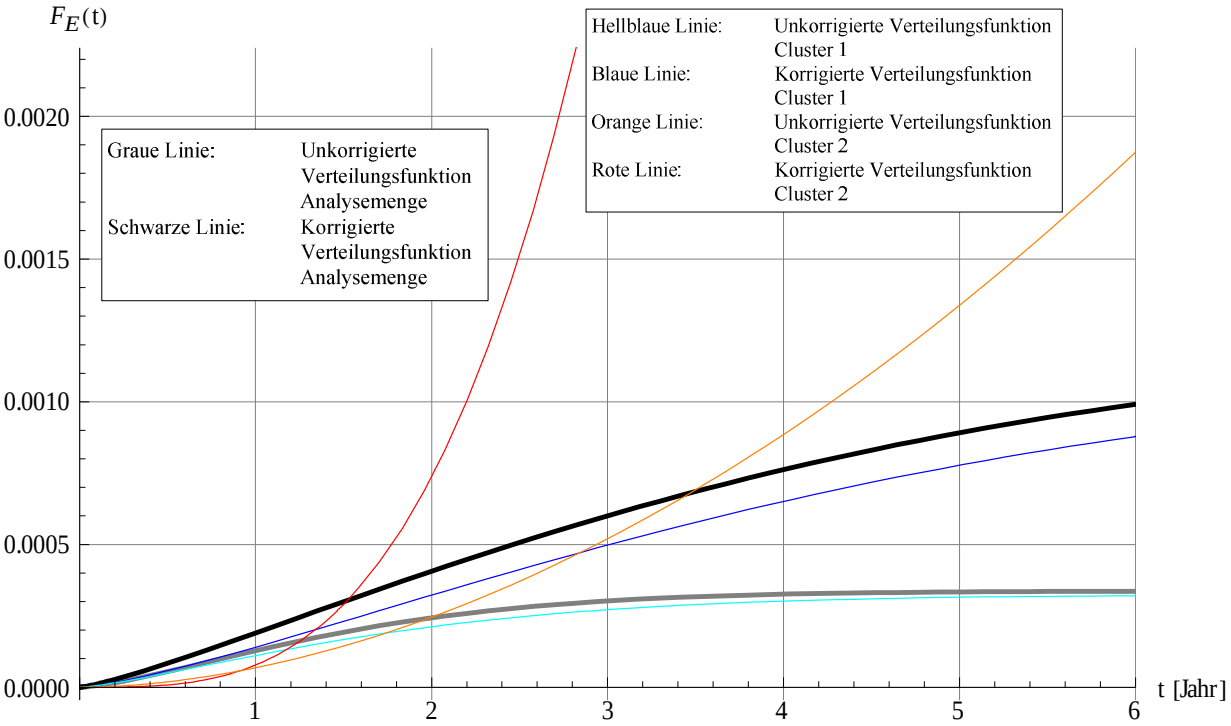


Bild 6-19: Ereigniswahrscheinlichkeiten (unkorrigiert / korrigiert) der beiden Cluster und der Analysemenge für Fall B (FLV übergeben)

Anhand von Bild 6-19 ist auch zu erkennen, dass der Verlauf der Verteilungsfunktion des Diesel-Clusters sehr ähnlich zu dem der Analysemenge ist. Die Funktionen des Clusters Motoraufladung weichen hingegen in ihrer Charakteristik deutlich von ihnen ab.

Die genauen Ergebnisse der ermittelten Verteilungsfunktionen mit allen relevanten Parametern für die fahrzeugbezogenen Cluster sind in Anhang A5 zu finden.

6.4 Bewertung der Ergebnisse

Nachfolgend werden die Ergebnisse der zahlreichen durchgeführten Untersuchungen zusammengefasst und bezüglich der PiU-Untersuchung bewertet.

Als erstes wichtiges Ergebnis wurden die **jährlichen Fahrleistungsverteilungen** für die gesamte PiU-relevante Baureihe ermittelt, wodurch Erkenntnisse über die Nutzung der einzelnen Modelltypen erlangt wurden. Datengrundlage hierfür waren die gesamten GuK-Daten der Baureihe. So weist z.B. jedes Kombifahrzeug eine höhere jährliche Fahrleistung auf als die entsprechende Limousine (vgl. Tabelle 6-1). Außerdem konnten fahrzeugbezogene Cluster bestimmt werden, bei denen ähnliche Fahrzeugmodelle zusammengefasst wurden, wie

z.B. Fahrzeuge mit Dieselmotor, Fahrzeuge mit Allradantrieb oder Fahrzeuge mit Motoraufladung. Bei der Clusterung wurden sowohl technische als auch statistische Gesichtspunkte berücksichtigt. Auch für diese Cluster wurden jeweils die jährlichen Fahrleistungsverteilungen ermittelt (vgl. Tabelle 6-2). Bei diesen Untersuchungen wurde darüber hinaus festgestellt, dass es nicht sinnvoll ist, die Fahrleistung einer gesamten Baureihe zu bestimmen, da diese teilweise erheblich von denen der einzelnen Modelle und Cluster abweicht. Eine Verwendung einer solchen Fahrleistung in weiteren Analyseschritten würde zu verzerrten und praxisfernen Ergebnissen führen.

Nachdem die für die PiU-Untersuchung relevante Schnittmenge identifiziert worden ist, in denen die Ereignisse enthalten sind, denen das Potential zugeordnet wird das Sicherheitsziel des Kandidaten zu verletzen, ermöglichte die Analyse dieser Datensätze die Nutzung des Wuppertaler Prognosemodells. Zunächst wurde das mehrstufige Standardprognosemodell (beschrieben in den drei Schritten in Abschnitt 5.4.3.1) verwendet. Bei der Anpassung der theoretischen an die empirischen kilometerabhängigen Werte wurde allerdings deutlich, dass ein Korrekturfaktor und somit eine Modellerweiterung erforderlich ist, so dass die Güte der Anpassung ein akzeptables Niveau erreicht. Es muss an dieser Stelle allerdings darauf hingewiesen werden, dass dieser **Anpassungsfaktor** keine zwingende Notwendigkeit für alle zukünftigen PiU-Untersuchungen darstellt. Es kann nicht davon ausgegangen werden, dass eine solche Korrektur des Prognosemodells für PiU-Untersuchungen anderer Bauteile und/oder anderer Fehlerfälle ebenfalls erforderlich ist. Die Möglichkeit der Berücksichtigung eines solchen Anpassungsfaktors sollte allerdings immer in die Überlegungen einbezogen werden.
Weiterhin wurde in dem Prognosemodell die Grundgesamtheit um einen Faktor korrigiert, der die **Ausschlussquote** berücksichtigt. Falls bei künftigen Untersuchungen ebenfalls Datensätze ausgeschlossen werden müssen, sollte dieser Faktor implementiert werden, da sonst die Datensätze zu positiv bewertet werden würden. Außerdem sollte bei künftigen Untersuchungen immer überprüft werden, ob mögliche Modellkorrekturen bzw. -erweiterungen, wie in Abschnitt 5.4.3.1 beschrieben, Verwendung finden können oder nicht.

Bei der Ermittlung der **zeitlichen Ereignisraten** für die Analysemenge wurde festgestellt, dass sowohl die unkorrigierte als auch die mit den Anwärtern korrigierte Ereignisrate einen ähnlichen qualitativen Verlauf aufweisen. Nach einem Anstieg bis auf ein Maximum fallen die Ereignisraten wieder ab, um nach einer gewissen Zeit in einen nahezu konstanten Bereich

überzugehen. Wird der Fokus auf den quantitativen Verlauf gerichtet, so können aus den durchschnittlichen Ereignisraten über die Zeit weitere Erkenntnisse gewonnen werden. In nachfolgendem Bild 6-20 sind die durchschnittlichen Ereignisraten $\overline{h_E}(t)$ für die Analysemenge bis zum entsprechenden Jahr für den mit den Anwärtern korrigierten Fall dargestellt.

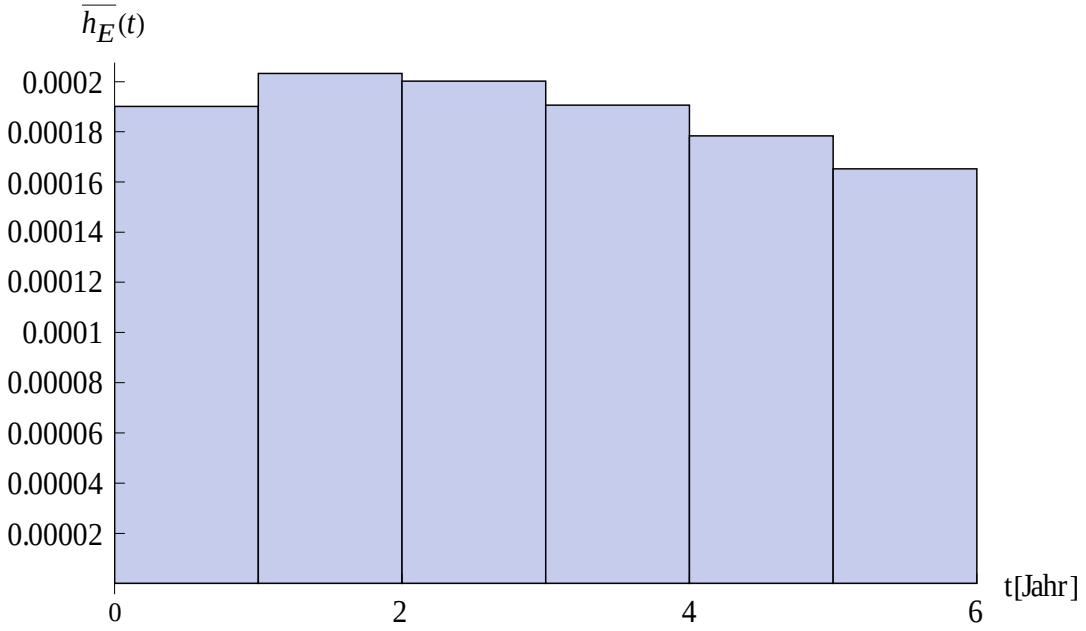


Bild 6-20: Durchschnittliche Ereignisrate (korrigiert) der Analysemenge bis zum sechsten Jahr

Zu erkennen ist in Bild 6-20, dass beispielsweise die durchschnittliche Ereignisrate nach einem Jahr bei circa $0{,}19 \cdot 10^{-3} \frac{1}{a}$ liegt, nach zwei Jahren etwas mehr als $0{,}2 \cdot 10^{-3} \frac{1}{a}$ beträgt und nach fünf Jahren auf knapp unter $0{,}18 \cdot 10^{-3} \frac{1}{a}$ gesunken ist. Wird diese durchschnittliche Ereignisrate nun in einen Wert in $\frac{1}{h}$ umgerechnet, so gibt es mehrere Möglichkeiten.

Zum einen können für ein Jahr 8.760 h als Betriebszeit zugrunde gelegt werden, was allerdings nicht der Realität entspricht, da kein E/E-System im Fahrzeug über die gesamte Lebensdauer aktiv ist.

Zum anderen besteht die Möglichkeit, für ein Jahr den in der Praxis oftmals verwendeten Wert von 400 Betriebsstunden zu benutzen. Auch dies ist allerdings nur eine Abschätzung.

Eine weitere Möglichkeit der Umrechnung bietet sich über die bereits bestimmte jährliche Fahrleistung an. Wird nämlich eine Durchschnittsgeschwindigkeit im Jahr von $50\frac{km}{h}$ und der Erwartungswert $E(S)$ der jährlichen FLV verwendet, kann über die einfache Beziehung

$$v = \frac{s}{t} \tag{6-1}.$$

mit v: Geschwindigkeit in [km/h]

s: Strecke in [km]

t: Zeit in [h]

die jährliche Betriebszeit in Stunden genauer abgeschätzt werden. Für die Analysemenge ergibt sich somit eine jährliche Betriebszeit von:

$$t = \frac{s}{v} = \frac{E(S)}{50\frac{km}{h}} = \frac{27{,}05\ Tkm}{50\frac{km}{h}} \approx 541\ h\,.$$

Der zuvor angegebene Wert von $50\frac{km}{h}$ stammt aus der Bestimmung der ebenfalls zuvor bereits angeführten 400 Betriebsstunden, wofür eben diese Geschwindigkeit sowie eine Jahresfahrleistung von 20.000 km verwendet wird und stellt somit gleichermaßen eine Abschätzung dar. Sofern genauere Kenntnisse über die jährliche Durchschnittsgeschwindigkeit bei den betrachteten Fahrzeugen vorliegen, sollten diese Angaben benutzt werden.

Wird der Wert von 541 Betriebsstunden nun verwendet, um die durchschnittliche Ereignisrate zu bestimmen, ergibt sich nach einem Jahr eine durchschnittliche Rate von $3{,}51 \cdot 10^{-7}\,\frac{1}{h}$ und nach fünf Jahren eine durchschnittliche Rate von $3{,}3 \cdot 10^{-7}\,\frac{1}{h}$.

Zum Vergleich wird bei einer Verwendung von 400 h pro Jahr nach einem Jahr bzw. fünf Jahren eine durchschnittliche Ereignisrate von $4{,}75 \cdot 10^{-7}\,\frac{1}{h}$ bzw. $4{,}46 \cdot 10^{-7}\,\frac{1}{h}$ erzielt.

Sowohl an den quantitativen Werten als auch an dem qualitativen Verlauf der Ereignisraten ist zu erkennen, dass die Ereignisrate der PiU-relevanten Datensätze mit zunehmender Dauer abnimmt.

Die so ermittelten quantitativen Werte sind größer als die in der ISO 26262 geforderten Werte für die beobachtbare Ereignisrate (vgl. Tabelle 4-1). In Abschnitt 4.4 wurde bereits dargelegt,

dass die Vorgaben in dem Normenwerk kritisch zu betrachten sind. Es muss festgehalten werden, dass die aus den realen Felddaten ermittelten Ereignisraten allesamt in einem Bereich liegen, der als unkritisch anzusehen ist. D.h. der Maximalwert der mit den Anwärtern korrigierten zeitlichen Ereignisrate der Analysemenge beträgt knapp $0{,}22 \cdot 10^{-3} \frac{1}{a}$ bzw. rund $4{,}07 \cdot 10^{-7} \frac{1}{h}$ (bei Verwendung von 541 Betriebstunden pro Jahr).

Als ein weiteres Ergebnis der Untersuchung der Analysemenge wurde die **Ereigniswahrscheinlichkeit** oder auch **Verteilungsfunktion** $F_E(t)$ ermittelt (s. Bild 6-21).

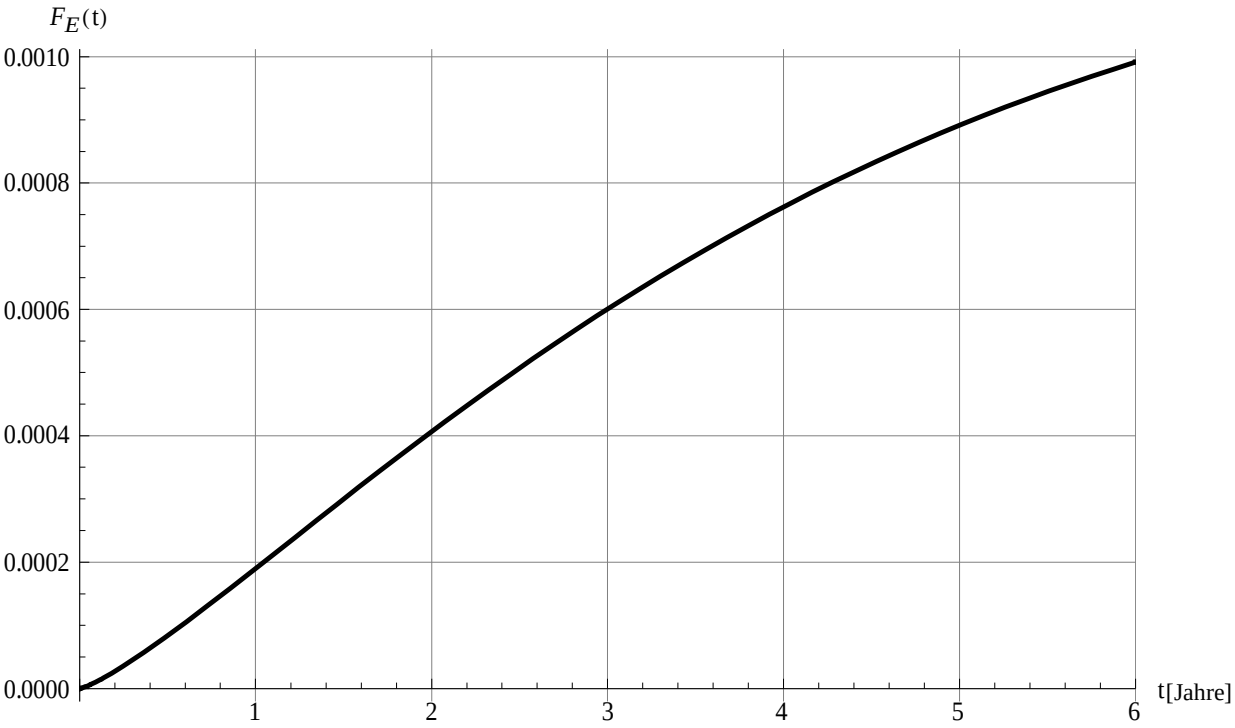


Bild 6-21: Verteilungsfunktion (korrigiert) der PiU-relevanten Analysemenge

Wie in Bild 6-21 zu erkennen ist, weist die Verteilungsfunktion der Analysemenge einen leicht konkaven (rechtsgekrümmten) Verlauf auf. Dies verdeutlicht noch einmal das leichte Frühereignisverhalten, wofür ein solcher Verlauf typisch ist (s. auch [ALT 09a]). Dieses Verhalten wurde bereits anhand der zeitlichen Ereignisraten festgestellt (vgl. Bild 6-7). Nach einem Jahr liegt eine Wahrscheinlichkeit für den Eintritt eines PiU-relevanten Ereignisses von ungefähr $0{,}19 \cdot 10^{-3}$ und nach einer Zeit von sechs Jahren eine Ereigniswahrscheinlichkeit von ca. $0{,}99 \cdot 10^{-3}$ vor. Genau diese aus realen Felddaten ermittelte Verteilungsfunktion stellt das **Referenzkriterium für künftige PiU-Untersuchungen** des Kandidaten dar, da für diesen

keine sicherheitsrelevanten Ereignisse aus dem Feld bekannt sind. Dieser als Alternative zu den vorgegebenen Grenzwerten in der ISO 26262 entwickelte neue Bewertungsmaßstab ist individuell für den Kandidaten ermittelt worden. Er repräsentiert das tatsächliche Verhalten im Feld hinsichtlich der identifizierten PiU-relevanten Ereignisse.

Nachfolgend soll kurz folgendes Beispielszenario betrachtet werden: der Kandidat ist in einer anderen Baureihe unter gleichen Einbaubedingungen verbaut worden und soll nun hinsichtlich des gleichen Sicherheitsziels einer PiU-Untersuchung unterzogen werden. Auch für die neue Baureihe liegen Felddaten vor, so dass die PiU-relevanten Ereignisse wie in vorliegender Arbeit identifiziert werden können. Für diese Ereignisse wird wiederum die Ereignisrate bzw. die Ereigniswahrscheinlichkeit ermittelt. Als Bewertungsmaßstab für den PiU-Nachweis gilt die zuvor ermittelte Verteilungsfunktion (s. Bild 6-21), sofern keine zeit- oder fahrzeugbezogene Zerlegung der Analysemenge vorgenommen wird (s. Ausführungen weiter unten). Sind die Ergebnisse für die neue Baureihe gleich gut oder besser und sind dem Hersteller keine sicherheitskritischen Ereignisse aus dem Feldeinsatz bekannt, so ist der Nachweis erbracht, sind sie schlechter oder sind sicherheitskritische Ereignisse aus dem Feldeinsatz bekannt, so kann (noch) kein positiver Betriebsbewährtheitsnachweis ausgestellt werden.

Über eine **zeitliche Zerlegung** der Analysemenge wurde nachgewiesen, dass die erzielten Ergebnisse durch den Einsatz des Wuppertaler Prognosemodells zwar konservativer als die Realität sind (vgl. Bild 6-12 und Bild 6-22), das Modell aber sinnvolle und realitätsnahe Ergebnisse liefert.
Bild 6-22 zeigt zum Vergleich die Verläufe der Ereigniswahrscheinlichkeiten der zeitlichen Zerlegung der Analysemenge, wobei die roten Kurven die unkorrigierten und die blauen Kurven die mit den Anwärtern korrigierten Wahrscheinlichkeiten darstellen. Die Ergebnisse der Zeitmenge 1 werden dabei durch die grob gepunkteten Linien repräsentiert, die des zeitlichen Abschnitts 2 durch die fein gepunkteten und die Ergebnisse der kompletten Analysemenge durch die durchgezogene Linien.

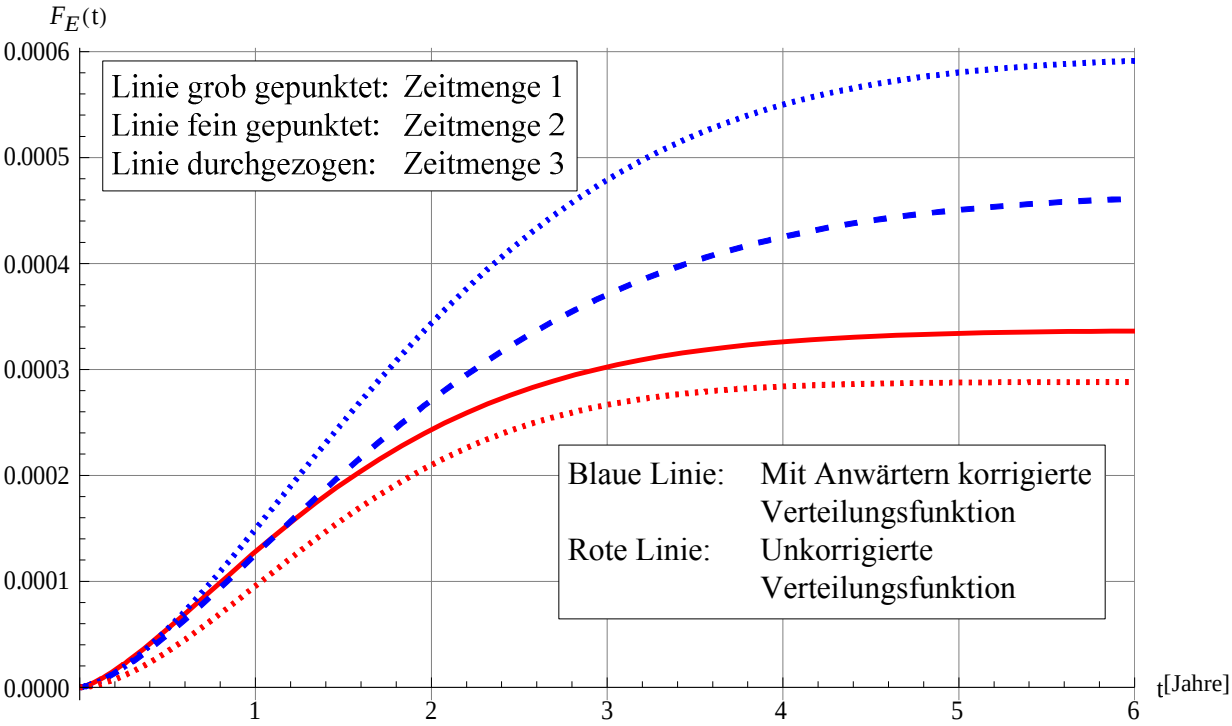


Bild 6-22: Verteilungsfunktionen der zeitlichen Zerlegung der Analysemenge

Auch in Bild 6-22 ist für alle Zeitmengen wiederum der charakteristische rechtsgekrümmte Verlauf der Verteilungsfunktionen festzustellen. Die konservativeren Ergebnisse der Prognose gegenüber den tatsächlichen Ergebnissen sind im Vergleich der Ereigniswahrscheinlichkeiten von Zeitmenge 2 (blaue fein gepunktete Linie) und Zeitmenge 3 (rote durchgezogene Linie) zu erkennen.

Durch eine **fahrzeugbezogene Clusterung** der Analysemenge, bei der sowohl technische als auch statistische Gesichtspunkte berücksichtigt wurden, wurde gezeigt, dass es ein dominierendes Fahrzeug-Cluster in der Analysemenge zu geben scheint, welches das zeitliche Ereignisverhalten maßgeblich bestimmt. Dabei handelt es sich um die Fahrzeuge mit Dieselmotoren (03-L-d, 03-K-d, 04-L-d, 04-K-d und 10-K-d). Deren zeitliches Ereignisverhalten ist dem der gesamten Analysemenge sehr ähnlich. Das Verhalten des zweiten Clusters (Fahrzeuge mit Motoraufladung) scheint keinen signifikanten Einfluss auf das Verhalten der Analysemenge zu haben (vgl. Bild 6-18 und Bild 6-19), da die Verteilungsfunktion der Analysemenge eher der von Cluster 1 ähnelt und deutlich von der des Clusters 2 abweicht. Würden die Fahrzeuge mit Motoraufladung stattdessen alleine betrachtet (vgl. Bild 6-16), müsste festgehalten werden, dass deren Ereignisverhalten durchaus als kritisch anzusehen ist, da deren Verteilungsfunktion exponentiell ansteigt. Hierbei ist anzumerken, dass die erzielten Ergebnisse zum Einen auf einer kleinen Stichprobe beruhen

und diese zum Anderen nicht zufrieden stellend in dem vorgestellten Modell zu untersuchen waren. Als Teil der Analysemenge hatte das Cluster allerdings keinen erkennbaren Einfluss auf das Ergebnis.

Die Ergebnisse der zeit- und fahrzeugbezogenen Zerlegungen der Analysemenge können ebenfalls als Referenzkriterien für künftige PiU-Untersuchungen angesehen werden, sofern dort auch fahrzeugbezogene Cluster gebildet werden können.

7 Zusammenfassung und Ausblick

Der künftige Automobilstandard zur Funktionalen Sicherheit von sicherheitsrelevanten E/E-Systemen im Kraftfahrzeug berücksichtigt für einen Betrachtungsgegenstand eine Vielzahl von Phasen, die dessen gesamten Sicherheitslebenszyklus (von der Entwicklung bis zur Außerbetriebnahme) umfassen. Dabei werden diejenigen Tätigkeiten systematisch erfasst, die notwendig sind, um die Funktionale Sicherheit zu gewährleisten. Insbesondere die Automobilindustrie hat bereits seit Jahren Produkte in den Fahrzeugen im Einsatz, die sich über Tausende von gefahrenen Kilometern bewährt haben. Während des Betriebs ist es zu keinen sicherheitskritischen Fehlern oder Ausfällen gekommen. Um genau solche Produkte hinsichtlich der Normenkonformität bewerten zu können, bietet die ISO 26262 die Möglichkeit, einen Nachweis der Betriebsbewährtheit durchzuführen. Dieser basiert auf der Auswertung von Felddaten, die das reale Ereignisverhalten des entsprechenden Kandidaten darstellen. Dabei werden solche Ereignisse betrachtet, die das Potential besitzen, ein dem Kandidaten während der Gefahrenanalyse und Risikobewertung zugeordnetes Sicherheitsziel zu verletzen. Hierzu gibt der künftige Automobilstandard eine Reihe von Angaben, die sich sowohl an die Einsatzbedingungen einer solchen PiU-Argumentation richten als auch an die Vorgehensweise. Weiterhin werden probabilistische Grenzwerte aufgezeigt, die der Kandidat zu erfüllen hat, wenn ein Betriebsbewährtheitsnachweis erbracht werden soll (vgl. Ausführungen in Abschnitt 4.3).

Im Rahmen der vorliegenden Arbeit wurden die normativen Vorgaben des PiU-Kapitels sowohl aus praxisnaher als auch aus wissenschaftlicher Sicht untersucht. Als Ergebnis wurde eine Reihe von Kritikpunkten identifiziert (vgl. Abschnitt 4.4).
Vom wissenschaftlichen Standpunkt aus wird der erste Kritikpunkt an die normative Annahme eines konstanten Ausfall- bzw. Ereignisverhaltens gestellt. Gerade komplexe elektronische Systeme können sich durch ein ausgeprägtes Frühausfallverhalten auszeichnen. Es sollte folglich, um die Wirklichkeit bei einer PiU-Argumentation abzubilden, immer das reale zeitliche Ereignisverhalten des Betrachtungsgegenstands ermittelt werden.
Aufgrund der vereinfachten Betrachtung über die Exponentialverteilung fehlt es der Norm an konkreten Handlungsanweisungen, wie ein nicht-konstantes Ereignisverhalten mit den normativen Zielwerten zu vergleichen und zu bewerten ist. Nur im Fall einer ermittelten konstanten Ereignisrate (Phase 2 in Bild 4-1) ist eine sinnvolle Bewertung dieser mit den Normzielwerten möglich. In allen anderen Fällen (Phasen 1 und 3 in Bild 4-1) kann ein

positiver PiU-Nachweis praktisch nicht erbracht werden (vgl. Bild 4-2). Auch ein Vergleich der normativen Werte mit dem Durchschnittswert der ermittelten Ereignisrate ist nicht sinnvoll, da das zugrundeliegende Zeitintervall nicht definiert ist.
Darüber hinaus wurden neben sprachlichen Inkonsistenzen bei einigen Begriffsverwendungen auch unklare und teils widersprüchliche Angaben bei dem normativen rechnerischen Formalismus aufgedeckt, der einen Kernpunkt des Betriebsbewährtheitsnachweises darstellt.
Des Weiteren müssen die probabilistischen Werte, die in der ISO 26262 als quantitative Grenzen für die PiU-Argumentation vorgegeben werden, selbst in Frage gestellt werden.
Aus praxisnaher Sicht muss festgehalten werden, dass die in der ISO 26262 angegebenen Grenzwerte für Betrachtungsgegenstände von kleinen Kollektiven, wie z.B. kleinvolumige Baureihen, praktisch nicht zu erfüllen sind. Selbst bei großvolumigen Baureihen (oder die Summe vieler kleiner Baureihen) ist es denkbar, dass ein Nachweis selbst für wenige sicherheitskritische Ereignisse des Kandidaten erst nach einer sehr langen Produktionszeit erbracht werden kann. Dies ist aus praktischer Sicht nicht zielführend.

Die Motivation der vorliegenden Arbeit bestand (als Konsequenz der zuvor identifizierten Kritikpunkte an der ISO 26262) in der Entwicklung einer wissenschaftlich fundierten, aber zugleich in der Praxis anwendbaren Vorgehensweise für eine PiU-Argumentation in der Automobilindustrie. Ein weiteres Ziel bestand in der Entwicklung neuartiger individueller Bewertungskriterien, so dass eine sinnvolle Beurteilung der Ergebnisse des neuen Betriebsbewährtheitsnachweises möglich ist.

Die neuartige Vorgehensweise für einen Nachweis der Betriebsbewährtheit von automotiven Betrachtungsgegenständen umfasst eine mehrstufige Schrittfolge (vgl. Bild 5-6), die die folgenden vier Punkte umfasst:

(1) Vorbedingungen,
(2) Vorbereitung,
(3) Zweigeteilte Felddatenanalyse und
(4) Bewertung.

Der **erste Schritt** besteht aus den *Vorbedingungen*, welche getroffen und erfüllt werden müssen, um eine PiU-Argumentation überhaupt zu beginnen. Die Vorbedingungen umfassen

- die Identifikation des Kandidaten,
- die Ergebnisse einer G+R für den Kandidaten und

- das Vorhandensein von Felddaten für den Kandidaten.

Der **zweite Schritt** beinhaltet die *Vorbereitung* der PiU-Argumentation. Darunter ist die Beschaffung und Sichtung von den Kandidaten betreffenden relevanten Informationen zu verstehen. Aus vorhandenen Dokumenten muss sich ein möglichst umfangreiches Bild über die Funktionsweise, die Einsatzbedingungen, die Nutzungsprofile usw. des Kandidaten ergeben, um einen möglichst umfassenden Kenntnisstand bezüglich des Kandidaten zu erlangen.

Anschließend erfolgt der wichtigste und umfangreichste **Schritt 3**: die *zweigeteilte Felddatenanalyse*.
Im 1. Teil der Felddatenanalyse sind aus allen GuK-Daten für diejenigen Fahrzeuge, die während der Vorbedingungsphase (Schritt 1) identifiziert worden sind, die jährlichen Fahrleistungsverteilungen zu bestimmen. Hierbei sollte das Augenmerk auch auf eine mögliche Clusterung der Fahrzeugmodelle (Diesel, Fahrzeuge mit Motoraufladung, Fahrzeuge mit Allradantrieb, Tuningfahrzeuge etc.) gelegt werden (vgl. Ausführungen in Abschnitt 5.4.2).
Im 2. Teil der Felddatenanalyse müssen zunächst die Datensätze für den Kandidaten bestimmt werden, welche die PiU-relevanten Ereignisse darstellen. Um dies erfolgreich durchzuführen, ist eine enge Zusammenarbeit mit den entsprechenden Entwicklern bzw. Experten des Kandidaten notwendig, da diese Personen den diesbezüglich umfangreichsten Wissensstand aufweisen. Es kann darüber hinaus bei der Ereignisidentifizierung erforderlich sein, den Fokus nicht nur ausschließlich auf den Bereich Garantie und Kulanz zu legen, sondern andere Quellen, wie z.B. die Diagnosebewährung, mit einzubeziehen. Infolgedessen muss in solchen Fällen die Schnittmenge der beiden Datenmengen anhand der jeweiligen Datumsangaben für die Reparatur (GuK) und die Diagnose gebildet werden, um die Analysemenge mit den relevanten Datensätzen zu ermitteln (s. unter anderem Abschnitt 5.4.1.4). Diese Analysemenge wird mit Hilfe des Wuppertaler Prognosemodells untersucht (vgl. Abschnitt 5.4.3.1). Bei der Umsetzung dieses mehrstufigen Prognosemodells sollte darauf geachtet werden, dass eventuelle Modellkorrekturen (Anpassungsfaktor, Ausschlussquote etc.) erforderlich sein können. Diese sind gegebenenfalls zu berücksichtigen, um die bestmögliche Anpassung und realistische Ergebnisse zu erhalten. Die Ergebnisse stellen sich in Form von zeitabhängigen Ereignisraten $h_E(t)$ sowie Verteilungsfunktionen (Ereigniswahrscheinlichkeiten) $F_E(t)$ dar. An dieser Stelle sei noch einmal darauf

hingewiesen, dass das Prognosemodell aufgrund bisheriger Untersuchungen des Lehrstuhls Sicherheitstheorie und Verkehrstechnik der Bergischen Universität Wuppertal für einen Zeitraum bis zu fünf bzw. sechs Jahren gute Ergebnisse liefert. Für einen längeren Zeitraum können zwar Ergebnisse bestimmt, diese konnten aber insbesondere bei E/E-Komponenten, noch nicht überprüft werden.

Weiterhin können aus einer zeitlichen sowie einer fahrzeugbezogenen Zerlegung der Analysemenge und anschließenden Bewertung dieser Teilmengen mit Hilfe des Prognosemodells weitere wichtige Erkenntnisse gewonnen werden. Eine zeitliche Zerlegung der Datensätze hinsichtlich des Produktionszeitraumes erlaubt eine Überprüfung der Modellergebnisse (s. Bild 6-12). Außerdem kann der zeitliche Verlauf des Ereignisverhaltens genauer betrachtet werden. Über eine fahrzeugbezogene Zerlegung der Analysemenge durch Bildung von Clustern - wobei sowohl technische als auch statistische Gesichtspunkte berücksichtigt werden sollten - kann überprüft werden, wie sich die einzelnen Ergebnisse der identifizierten Fahrzeug-Cluster auswirken. Schließlich kann festgestellt werden, ob es eine dominierende Fahrzeuggruppe gibt, welche das gesamte Kollektiv maßgeblich bestimmt. Die zuvor genannten Zerlegungen der Analysemenge sind optional, da ihr Einsatz von verschiedenen Aspekten abhängig ist, wie z.B. dem Umfang der Datensätze, der Zusammensetzung der Analysemenge hinsichtlich einer zeit- und/oder fahrzeugbezogenen Clusterung etc. Genauere Ausführungen zu den möglichen Zerlegungen sind in Abschnitt 5.4.3.2 zu finden.

Die Ergebnisse der Fahrleistungsverteilungen aus dem ersten Teil der Felddatenanalyse können bei der Untersuchung der Analysemenge durch das Wuppertaler Prognosemodell verwendet werden. Hier ist eine mögliche Nutzung dieser Ergebnisse allerdings abhängig von der Zusammensetzung der Analysemenge. Sinnvoll ist eine Nutzung der Fahrleistungsverteilungen außerdem für die Analyse von Fahrzeug-Clustern, sofern eine solche fahrzeugbezogene Zerlegung vorgenommen werden kann.

In einem ***letzten Schritt*** erfolgt die *Bewertung der Ergebnisse*. Für eine PiU-Argumentation müssen individuelle Bewertungskriterien verwendet werden. Hierzu kann sich entweder internen oder externen Vergleichsuntersuchungen bedient werden.

Unter *internen Vergleichsuntersuchungen* sind nach zuvor beschriebener Vorgehensweise bereits durchgeführte Analysen zum zeitlichen Ereignisverhalten des Kandidaten zu verstehen. Sind für einen Kandidaten beispielsweise hinsichtlich einer Baureihe X schon zeitliche Ereignisraten sowie Verteilungsfunktionen während einer früheren PiU-

Argumentation ermittelt worden (wie z.B. in vorliegender Arbeit in Kapitel 6), so stellen diese Ergebnisse die Bewertungskriterien für eine neue PiU-Untersuchung unter gleichen Voraussetzungen (derselbe Kandidat, gleiches Sicherheitsziel etc.) in einer Baureihe Y dar. Sind die neu ermittelten Verteilungsfunktionen bei der Untersuchung Y gleich gut oder besser als die der Untersuchung X, so kann der PiU-Argumentation Y ein positives Ergebnis ausgestellt werden. Dies setzt voraus, dass keine sicherheitskritischen Ereignisse aus dem Feldeinsatz des Kandidaten bekannt sind. Nur dann kann der Kandidat als betriebsbewährt angesehen werden.
Sind keine internen Vergleichsuntersuchungen zum PiU-Kandidaten vorhanden, so können *externe Untersuchungen* als Bewertungskriterien herangezogen werden. Der Betrachtungsgegenstand und die Ergebnisse dieser Analysen müssen jedoch eine verwertbare und sinnvolle Bewertung der Ergebnisse des PiU-Kandidaten ermöglichen. Hierbei ist es sehr wichtig, dass die externen Untersuchungen auf empirischen Daten beruhen und somit statistisch abgesichert sind. Den externen Vergleichsuntersuchungen sind aber, sofern vorhanden, interne Untersuchungen vorzuziehen.

Diese neue Vorgehensweise für einen Betriebsbewährtheitsnachweis wurde exemplarisch für einen realen Kandidaten aus einem sicherheitsrelevanten E/E-Kraftfahrzeugsystem angewendet. Die Datenbasis hierzu lieferte ein deutscher Automobilhersteller. Die Ergebnisse dieser Untersuchungen sind in Kapitel 6 dargestellt. Hierbei zeigte sich die praktikable Durchführbarkeit der alternativen Methode.
Gleichzeitig wurden einige Punkte aufgedeckt, die zu einer Vereinfachung der neu erarbeiteten Vorgehensweise beitragen können. So ist es für ein Unternehmen der Automobilindustrie hilfreich, wenn einige der erforderlichen Arbeitsschritte automatisiert ablaufen könnten. Dies kann beispielsweise bei der Ermittlung der Fahrleistungsverteilungen geschehen. Alle notwendigen Informationen sind beispielsweise bei den OEM in der Regel in entsprechenden Datenbanksystemen vorhanden, so dass eine Realisierung der automatischen Ermittlung von theoretischen jährlichen Fahrleistungsverteilungsfunktionen aufgrund empirischer Daten für selektierte Fahrzeugmodelle möglich ist.
Innerhalb der Unternehmen sollten Fahrleistungsdatenbanken aufgestellt werden, in welcher die Ergebnisse aller Baureihen, aller Modelltypen und aller Motorisierungsvarianten vorhanden sind. Sogar regionale und länderspezifische Betrachtungen sind hierbei möglich und sinnvoll. Aus den somit gewonnenen Informationen können wichtige Erkenntnisse über die Nutzung der einzelnen Fahrzeugtypen gewonnen werden. Bei einer automatisierten

Bestimmung der Fahrleistungsverteilungen müssen die erzielten Ergebnisse zwar immer noch auf Plausibilität und Korrektheit überprüft werden, der Arbeitsaufwand würde aber erheblich reduziert. Um eine möglichst große Wissensbasis hinsichtlich der internen Vergleichsuntersuchungen als Bewertungskriterien für die neue PiU-Vorgehensweise zu erlangen, sollten die Unternehmen Analysen von PiU-relevanten Kandidaten mit Hilfe der vorgeschlagenen alternativen Vorgehensweise durchführen.

Eine visionäre und aus wissenschaftlicher Sicht sinnvolle Erweiterung der Einrichtung zuvor genannter unternehmensinterner Datenbanken (sowohl hinsichtlich Fahrleistungen als auch bezüglich PiU-Kriterien) ist der Aufbau einer branchenumfassenden und somit unternehmensübergreifenden Datenbank, in welche die gesamte Automobilindustrie (Hersteller und Zulieferer) ihre entsprechenden Informationen eintragen kann. Selbstverständlich handelt es sich bei solchen Daten um sehr sensible Informationen, die ein Unternehmen nicht bereitwillig unbeteiligten Personen oder sogar Konkurrenzunternehmen zur Verfügung stellt. Deswegen ist es wichtig, dass eine solche Datenbank von einer neutralen und in der Branche anerkannten Institution verwaltet wird. Hier sei als mögliches Beispiel der VDA als Dachverband genannt. Des Weiteren müsste gewährleistet sein, dass die Daten anonymisiert werden. Sofern eine solche Datenbank realisiert werden könnte, wären umfassende Analysen des gesamten deutschen Automobilmarktes möglich, woraus unzählige Erkenntnisse gewonnen werden könnten.

Hinsichtlich der neu erarbeiteten Vorgehensweise für einen Betriebsbewährtheitsnachweis wäre es wünschenswert, die vorgestellte Schrittfolge auf weitere konkrete und reale Feldbeispiele in der Automobilindustrie anzuwenden. Hier sollte das Augenmerk sowohl auf Untersuchungen innerhalb einzelner Unternehmen als auch in unterschiedlichen Unternehmen auf Hersteller- sowie Zuliefererseite gelegt werden. Des Weiteren wären Untersuchungen interessant, die sich mit einer PiU-Argumentation in anderen Industrien beschäftigen.

Weiterhin kann eine Implementierung von Bayes-Ansätzen in die Vorgehensweise erfolgen, so dass bei fehlenden Ereignisinformationen Daten aus Vorgängerprodukten oder aus Testdurchläufen genutzt werden können. Hier haben sich erste Untersuchungen vielversprechend gezeigt.

Insgesamt kommt der ISO 26262 eine hohe Bedeutung in der Funktionalen Sicherheit im Automobilbereich zu. Sie schreibt den Stand von Wissenschaft und Technik fest, der zum Zeitpunkt ihrer Veröffentlichung aktuell ist. Ein weiterer Ausbau des in der Norm enthaltenen Betriebsbewährtheitsnachweises ist unerlässlich, um den Interessen der Automobilhersteller gerecht zu werden und die Vorgehensweise praktikabel einsetzen zu können.

8 Literaturverzeichnis

[ACE 11] Auto Club Europa: Hitliste Autopannen 2010, ACE Pannenhilfe, 2011.

[ALT 09a] Althaus, D.: Ein praxisorientierter empirischer Ansatz zur Bestimmung des Ausfallverhaltens konventioneller Bremssysteme in Personenkraftwagen. Dissertation, Bergische Universität Wuppertal, 2009.

[ALT 09b] Althaus, D.; Meyna, A.; Braasch, A.: Zuverlässigkeitsprognosen mit unabhängigen Fahrleistungsdaten. VDI-Bericht 2065, 24. Fachtagung Technische Zuverlässigkeit, VDI Verlag, Düsseldorf, 2009.

[BOH 04] Bohr, B.: Die Diskussion wird nicht immer präzise geführt. Beitrag im Forum der Meinungen „Höhere Ausfallraten durch Fahrzeugelektronik?“. Automobiltechnische Zeitschrift, ATZ 11/2004 Jahrgang 106, 2004.

[BÖR 11] Börcsök, J.: Funktionale Sicherheit – Grundzüge sicherheitstechnischer Systeme. 3. überarbeitete Auflage, Hüthig Verlag, 2011.

[BRA 07] Braasch, A.; Meyna, A; Hübner, H.-J.: Zuverlässigkeitsprognosen bei zeitnahen Garantiedaten für automobile Telekommunikationssysteme. VDI-Bericht 1984, Tagung Technische Zuverlässigkeit, VDI Verlag, Düsseldorf, 2007.

[BRA 11] Braasch, A.: Zuverlässigkeitsprognosemodelle im Bereich der mobilen Telekommunikation. Dissertation, Bergische Universität Wuppertal, 2011.

[BRA 12] Braband, J.; Schäbe, H.: The Collective Risk, the Individual Risk and Their Dependence in Exposition Time. Advances in Safety, Reliability and Risk Management, ESREL 2011, Taylor & Francis Group, London, 2012.

[BRO 06a] Brockhaus Enzyklopädie, Band 6, 21. Auflage, Verlag F.A. Brockhaus GmbH, Leipzig, Mannheim, 2006.

[BRO 06b] Brockhaus Enzyklopädie, Band 22, 21. Auflage, Verlag F.A. Brockhaus GmbH, Leipzig, Mannheim, 2006.

[DIN 02a] DIN EN 61508-1: Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbar elektronischer Systeme Teil 1: Allgemeine Anforderungen. Beuth Verlag, Berlin, 2002.

[DIN 02b] DIN EN 61508-4: Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbar elektronischer Systeme Teil 4: Begriffe und Abkürzungen. Beuth Verlag, Berlin, 2002.

[DIN 02c] DIN EN 61508-5: Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbar elektronischer Systeme Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität. Beuth Verlag, Berlin, 2002.

[DIN 02d] DIN EN 61508-7: Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbar elektronischer Systeme Teil 7: Anwendungshinweise über Verfahren und Maßnahmen. Beuth Verlag, Berlin, 2002.

[DIN 05] DIN EN 61511-1: Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware. Beuth Verlag, Berlin, 2005.

[DIN 06] E DIN EN 61508-4: Funktionale Sicherheit elektrischer/ elektronischer/ programmierbar elektronischer sicherheitsbezogener Systeme - Teil 4: Begriffe und Abkürzungen. Beuth Verlag, Berlin, 2006.

[DIN 07] DIN EN 45020: Normung und damit zusammenhängende Tätigkeiten – Allgemeine Begriffe. Beuth Verlag, Berlin, 2007.

[DIN 90] DIN V VDE 0801: Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben. Beuth Verlag, Berlin, 1990.

[DKE 02] Deutsche Kommission Elektrotechnik Elektronik Informationstechnik: Rechtliche Stellung der Normen der Reihe DIN EN 61508 (VDE 0803). DKE-Mitteilung, Frankfurt am Main, 2002.

[DOL 08] Dold, A.: Implementation of Requirements From ISO 26262 in the Development of E/E Components and Systems – Challenges & Approach. Automotive Electronicsand Electrical Systems Forum 2008, Stuttgart, 2008.

[DUD 04] Dudenhöfer, F.; Krüger, M.: Ausfallrate durch Elektrik/Elektronik steigt weiter. Automobiltechnische Zeitschrift, ATZ 11/2004 Jahrgang 106, 2004.

[E+H 04] Endress+Hauser: DIN EN IEC 61508 / IEC 61511 – Funktionale Sicherheit in der Prozess-Instrumentierung zur Risikoreduzierung. Informationsbroschüre der Firma Endress+Hauser, Weil am Rhein, 2004.

[ECK 77] Eckel, G.: Bestimmung des Anfangsverlaufs der Zuverlässigkeitsfunktion von Automobilteilen. Qualität und Zuverlässigkeit, Jahrg. 22, Heft 9, Carl Hanser Verlag, München, 1977.

[EFL 04] Efler, M.: Firlefanz fliegt raus. Focus Magazin, Nr. 21 (2004).

[FAB 98] Faber, G.: Der Mensch soll die Maschine beherrschen, nicht nur bedienen. Magazin der Technischen Universität Chemnitz, Heft 4/98, Chemnitz, 1998.

[FAH 07] Fahrmeir, L.; Künstler, R.; Pigeot, I.; Tutz, G.: Statistik – Der Weg zur Datenanalyse. 6. Auflage, Springer Verlag, Heidelberg, 2007.

[FET 11] Fetzer, J.: Umbruch in der etablierten Wertschöpfungskette. Elektronik und Automobil – Technologies to Watch, September 2011, Beilage zu VDI Nachrichten Nr. 36, Düsseldorf, 2011.

[FRI 00] Fritz, A.; Krolo, A.; Bertsche, B.: Analysis of Warranty Data For the Prediction of the Early-Failure-Behavior of Automotive Systems. Proceeding of ESREL 2000, Balkema Verlag, Rotterdam, 2000.

[GAL 00] Gall, H.; Kemp, K.; Schäbe, H.: Betriebsbewährung von Hard- und Software beim Einsatz von Rechnern und ähnlichen Systemen für Sicherheitsaufgaben. Schriftenreihe der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin: Forschungsbericht, Fb 888, Wirtschaftsverlag NW, Bremerhaven, 2000.

[GNE 06] Gneuss, M.: Chips bestimmen, wo es lang geht. Handelsblatt, 19.09.2006.

[GRA 03] Grass, S.: Bestnoten für die Mechatronik, Teil 5 der Serie: Innovationen auf Wachstumskurs. Handelsblatt, 15.08.2003.

[GRS 01] Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH: Bewertung des Unfallrisikos fortschrittlicher Druckwasserreaktoren in Deutschland – Methoden und Ergebnisse einer umfassenden Probabilistischen Sicherheitsanalyse (PSA). GRS – 175, 2001.

[GRS 90] Gesellschaft für Reaktorsicherheit: Deutsche Risikostudie Kernkraftwerke – Phase B. Verlag TÜV Rheinland, Köln, 1990.

[HAA 10] Haasper, C.; Junge, M.; Ernstberger, A.; Brehme, H.; Hannawald, L.; Langer, C.; Nehmzow, J.; Otte, D.; Sander, U.; Krettek, C.; Zwipp, H.: Die Abbreviated Injury Scale (AIS) – Potenzial und Probleme bei der Anwendung. Der Unfallchirurg 113, Nr. 5, Springer-Verlag, Berlin, 2010.

[HAR 05] Hartung, J.: Statistik. 14. Auflage, Oldenbourg Verlag, München, 2005.

[HÄR 83] Härtler, G.: Statistische Methoden für die Zuverlässigkeitsanalyse. VEB Verlag Technik, Berlin, 1983.

[HB 05a] DPA/GMS: Immer mehr Hard- und Software im Auto. Handelsblatt, 08.02.2005.

[HB 05b] DPA: Software wird die Zukunft der Autos bestimmen. Handelsblatt, 21.06.2005.

[HB 05c] HB: Autohersteller zweifeln am Sinn der High-Tech-Ausstattung. Handelsblatt, 09.05.2005.

[HSE 92] Health and Safety Executive: The Tolerability of Risk From Nuclear Power Stations. London, 1992.

[ISE 08] Isermann, R.: Mechatronische Systeme - Grundlagen. 2. Auflage, Springer Verlag, Berlin Heidelberg, 2008.

[ISO 10a] ISO/FDIS 26262-1: Road Vehicles – Functional Safety Part 1: Vocabulary. International Organization for Standardization, 2010.

[ISO 10b] ISO/FDIS 26262-2: Road Vehicles – Functional Safety Part 2: Management of Functional Safety. International Organization for Standardization, 2010.

[ISO 10c] ISO/FDIS 26262-3: Road Vehicles – Functional Safety Part 3: Concept Phase. International Organization for Standardization, 2010.

[ISO 10d] ISO/FDIS 26262-5: Road Vehicles – Functional Safety Part 5: Product Development: Hardware Level. International Organization for Standardization, 2010.

[ISO 10e] ISO/FDIS 26262-8: Road Vehicles – Functional Safety Part 8: Supporting Processes. International Organization for Standardization, 2010.

[ISO 10f] ISO/FDIS 26262-10: Road Vehicles – Functional Safety Part 10: Guideline. International Organization for Standardization, 2010.

[JUN 08] Jung, C.: ISO WD 26262 – Der zukünftige Standard zur Funktionssicherheit in der Automobilindustrie. ISO TC22 SC3 WG16 Functional Safety, 2008.

[KBA 10] Kraftfahrt-Bundesamt: Jahresbericht 2010. Flensburg, 2010.

[KLA 11] Klauda, M.; Hamann, R.; Kriso, S.: ISO 26262 – Was kommt da auf uns zu? VDI-Berichte 2132, Elektronik im Kraftfahrzeug, VDI Verlag GmbH, Düsseldorf, 2011.

[KOC 96] Kocher, D.: Criteria For Establishing De Minimis Levels of Radionuclides and Hazardous Chemicals in the Environment. ES/ER/TM-187, U.S. Department of Energy, Health Science Research Division, Oak Ridge (Tennessee), 1996.

[KRI 11] Kriso, S.; Hamann, R.: Die ISO 26262 ist veröffentlicht – Konsequenzen für OEMs und Zulieferer. VDI-Berichte 2132, Elektronik im Kraftfahrzeug, VDI Verlag GmbH, Düsseldorf, 2011.

[KRÖ 10] Kröger, W.: Grundlagen der technischen Risikoanalytik – Methodik der probabilistischen/quantitativen Risikoanalyse. Vorlesungsunterlagen zum Herbstsemester 2010, ETH Zürich, Laboratorium für Sicherheitsanalytik, 2010.

[KTA 02] KTA 3507: Werksprüfungen, Prüfungen nach Instandsetzung und Nachweis der Betriebsbewährung der Baugruppen und Geräte der Leittechnik des Sicherheitssystems. Sicherheitstechnische Regel des KTA, Salzgitter, 2002.

[LAN 07] Langeron, Y.; Barros, A.; Grall, A.; Bérenguer, C.: Safe Failures Impact on Safety Instrumented Systems. Risk, Reliability and Societal Safety, ESREL 2006, Taylor & Francis Group, London, 2007.

[LÖW 10] Löw, P.; Pabst, R.; Petry, E.: Funktionale Sicherheit in der Praxis. dpunkt.verlag, Heidelberg, 2010.

[MAR 02] Marseguerra, M.; Zio, E.: Basics of the Monte Carlo Method With Application to System Reliability. LiLoLe-Verlag GmbH, Hagen, 2002.

[MAS 12] Massé, F.; Tiennot, R.; Signoret, J.P.; Blancart, P.; Dupin, G.; Marle, L.: Benchmark Study on International Functional Safety Standards. Advances in Safety, Reliability and Risk Management, ESREL 2011, Taylor & Francis Group, London, 2012.

[MEY 03a] Meyer, M.: Methoden zur Analyse von Garantiedaten für die Sicherheits- und Zuverlässigkeitsprognose von Komponenten und Baugruppen im Kraftfahrzeug. Dissertation, Bergische Universität Wuppertal, 2003.

[MEY 03b] Meyer, M.; Meyna, A.; Pauli, B.: Zuverlässigkeitsprognose für Kfz-Komponenten bei zeitnahen Garantiedaten. Automobiltechnische Zeitschrift, ATZ 3/2003 Jahrgang 105, 2003.

[MEY 04] Meyer, M.; Meyna, A.: Alternative Reliability Prognosis Models For Automotive Components. Tagungsband ESREL'04, Springer Verlag, London, 2004.

[MEY 10] Meyna, A.; Pauli, B.: Zuverlässigkeitstechnik – Quantitative Bewertungsverfahren. Hanser Verlag, München, 2010.

[MON 03] Monée, B.: Sicher mit SIL – Steuerungen im Normungskontext. Chemie Technik Nr. 6 2003 (32. Jahrgang), 2003.

[MRL 02] MRL: „Ersetzt IEC 61508 künftig EN 954?". MRL-News – 14/04/02, 2002.

[NET 11] Netter, P.: Wie die Sicherheit laufen lernte – Entwicklung der funktionalen Sicherheit in Deutschland. Hauptbeitrag der NAMUR-Hauptsitzung, atp edition 1-2/2011, Oldenbourg Industrieverlag, München, 2011.

[PAU 00] Pauli, B.; Meyna, A.: Zuverlässigkeitsprognosen für Kfz-Komponenten bei unvollständigen Daten. Automobiltechnische Zeitschrift, ATZ 102 (2000) 12, 2000.

[PAU 96] Pauli, B.; Meyna, A. : Zuverlässigkeitsprognosen für elektronische Steuergeräte im Kraftfahrzeug. VDI Berichte 1287, Elektronik im Kraftfahrzeug, VDI Verlag, Düsseldorf, 1996.

[PAU 98] Pauli, B.: Zuverlässigkeitsprognosen für elektronische Steuergeräte im Kraftfahrzeug: Modellbildungen und deren praktische Anwendungen. Dissertation, Bergische Universität Wuppertal zugleich Shaker Verlag, Aachen, 1998.

[PAU 99a] Pauli, B.; Meyna, A.: Reliability Prognoses With Commercial Applications For Electronic Control Units in Motor Vehicles. 32nd ISATA, ISATA Paper 99AE034, Croydon, 1999.

[PAU 99b] Pauli, B.: Eine neue Methode zur Bestimmung der kilometerabhängigen Lebensdauerverteilung von Kfz-Komponenten. Automobiltechnische Zeitschrift, ATZ 101 (1999) 4, 1999.

[PRO 08] Proske, D.: Catalogue of Risks – Natural, Technical, Social and Health Risks. Springer Verlag, Heidelberg, 2008.

[REI 11a] Reiff, K: Bosch Autoelektrik und Autoelektronik – Bordnetze, Sensoren und elektronische Systeme. 6. Auflage, Vieweg + Teubner Verlag, Wiesbaden, 2011.

[REI 11b] Reißing, R.; Gast, S.: Funktionale Sicherheit in mechatronischen Systemen. Hochschultag Oberfranken 2011 – Info-Workshop 1, 2011.

[SAE 96] SAE Aerospace Recommended Practice 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. Warrandale, USA, 1996.

[SCH 04] Schlummer, M.: Durchführung einer Risikoanalyse für ein Fahrzeugsystem in Anlehnung an die IEC 61508 am Beispiel eines elektromechanischen Bremskraftverstärkers. Diplomarbeit, Bergische Universität Wuppertal, 2004.

[SCH 06] Schlummer, M.; Meyna, A.: Risikoanalyse in der Automobilindustrie. Tagung Risikomanagement in der Automobilindustrie, Tagungsband TÜV SÜD Akademie, München, 2006.

[SCH 07a] Schilling, S.: On the Use of „Probabilities'" in IEC 61508. BMW Group Report (contact the author for more information), 2007.

[SCH 07b] Schlummer, M.; Meyna, A.: Die Risikoanalyse in der Automobilindustrie. Zeitschrift für die gesamte Wertschöpfungskette Automobilwirtschaft (ZfAW), 10. Jahrgang (2007), Heft Nr. 2/2007.

[SFK 04] Störfall-Kommission beim Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit: Risikomanagement im Rahmen der Störfall-Verordnung. Bericht des Arbeitskreises Technische Systeme, Risiko und Verständigungsprozesse, SFK-GS-41, 2004.

[SMI 04] Smith, D.; Simpson, K.: Functional Safety – A Straightforward Guide to Applying IEC 61508 and Related Standards. 2nd Edition, Butterworth-Heinemann, Oxford, 2004.

[STÄ 06] Ständer, T.; Becker, U.: Eine vergleichende Betrachtung globaler Sicherheitsstandards für Verkehrssysteme. Automotive Safety & Security, Stuttgart, 2006.

[STÄ 10] Ständer, T.: Eine modellbasierte Methode zur Objektivierung der Risikoanalyse nach ISO 26262. Dissertation, Technische Universität Carolo-Wilhelmina zu Braunschweig, 2010.

[UTE 00] UTE C 80-810: RDF 2000: Reliability Data Handbook – A Universal Model For Reliability Prediction of Electronic Components, PCBs and Equipment. Union Technique de l'Electricité, 2000.

[VDA 08] VDA Auto Jahresbericht 2008. Verband der Automobilindustrie, Frankfurt am Main, 2008.

[VDI 11] VDI-Nachrichten: „Nicht alles, was zunächst cool oder hip ist, wird auch nachhaltig sein". VDI-Nachrichten, Nr. 18, 06.05.2011.

[WEI 03] Weidenhammer, P.: Elektronik treibt im Automobilbau die Innovationen weiter an. VDI- Nachrichten 24.10.2003.

[WRA 10] Wratil, P.; Kieviet, M.: Sicherheitstechnik für Komponenten und Systeme. 2. Auflage, Hüthig Verlag, Heidelberg, 2010.

Internetquellen

[elp 01] Hauptseite: www.elektronikpraxis.de
URL: http://www.elektronikpraxis.vogel.de/fachwissen/webcast/downloads/12632
Art der Quelle: Webcast.
(Abgerufen: 30.06. 2011)

[elp 02] Hauptseite: www.elektronikpraxis.de
URL: http://www.elektronikpraxis.vogel.de/themen/elektronikmanagement/rechtprodukthaftung/articles/248663/
Art der Quelle: Interview, 03.02.2010.
(Abgerufen: 15.08.2011)

[elp 03] Hauptseite: www.elektronikpraxis.de
URL: http://www.elektronikpraxis.vogel.de/themen/elektronikmanagement/projektqualitaetsmanagement/articles/242243/
Art der Quelle: Fachartikel
Sauler, J.; Kriso, S.: ISO 26262 – Die zukünftige Norm zur funktionalen Sicherheit von Straßenfahrzeugen. 31.08.2011.
(Abgerufen: 02.09.2011)

[elp 04] Hauptseite: www.elektronikpraxis.de
URL: http://www.elektronikpraxis.vogel.de/fachwissen/webcast/downloads/16250
Art der Quelle: Webcast.
(Abgerufen: 01.09.2011)

[elp 05] Hauptseite: www.elektronikpraxis.de
URL: http://www.elektronikpraxis.vogel.de/themen/embeddedsoftwareengineering/management/articles/185862/
Art der Quelle: Fachartikel
Winne, O.: Sicherheitskritische Systeme, Teil 1: Leitfaden für die Norm IEC 61508. 04.05.2009.
(Abgerufen: 01.12.2010)

[grs 01] Hauptseite: www.grs.de
URL: http://www.grs.de/begriff-der-woche-deutsche-risikostudie-kernkraftwerke
Art der Quelle: News der Woche.
(Abgerufen: 13.10.2011)

[lin 01] Hauptseite: http://www.uwe-lindenberg.de
URL: http://www.uwe-lindenberg.de/27-0-Folien.html
Art der Quelle: Folie.
(Abgerufen: 05.10.2011)

[wik 01] Hauptseite: www.wikipedia.de
URL: http://de.wikipedia.org/wiki/Abbreviated_Injury_Scale
Art der Quelle: Artikel.
(Abgerufen: 09.09.2010)

[wik 02] Hauptseite: www.wikipedia.de
URL: http://de.wikipedia.org/wiki/Commercial_off-the-shelf
Art der Quelle: Artikel.
(Abgerufen: 12.07.2009)

[wik 03] Hauptseite: www.wikipedia.de
URL: http://de.wikipedia.org/wiki/Fahrzeug-Identifizierungsnummer
Art der Quelle: Artikel.
(Abgerufen: 10.09.2011)

Anhang A

A1 Abkürzungsverzeichnis

ABS	Antiblockiersystem
ACE	Auto Club Europa
ADAC	Allgemeiner Deutscher Automobil-Club
AgPL	Agricultural Perfomance Level
AIS	Abbreviated Injury Scale
ALARP	As Low As Reasonably Practicable
AQ	Ausschlussquote
ASIL	Automotiver Sicherheits-Integritätslevel
BAK	Blutalkoholkonzentrationswert
CD	Committee Draft
CENELEC	Comité Européen de Normalisation Electrotechnique
COTS	Component-off-the-Shelf
DIN	Deutsches Institut für Normung
DIS	Draft International Standard
E/E	Elektrisch/elektronisch
E/E/PE	Elektrisch/elektronisch/programmierbar elektronisch
ECU	Electronic Control Unit
EN	Europäische Norm
ESP	Elektronisches Stabilitätsprogramm
EUC	Equipment Under Control
FAKRA	Fach-Normenausschuss Kraftfahrzeuge
FAS	Fahrerassistenzsystem
FBA	Fehlerbaumanalyse
FDIS	Final Draft International Standard
FIN	Fahrzeugidentifizierungsnummer
FLV	Fahrleistungsverteilung
FMEA	Fehler-Möglichkeits- und Einflussanalyse
FSK	Funktionales Sicherheitskonzept
FuSi	Funktionale Sicherheit
G+R	Gefahrenanalyse und Risikobewertung

GRS	Gesellschaft für Reaktorsicherheit
GSLZ	Gesamter Sicherheitslebenszyklus
GuK	Garantie und Kulanz
HSE	Health and Safety Executive
HW	Hardware
IEC	International Electrotechnical Commission
ISO	International Organisation For Standardization
KBA	Kraftfahrt-Bundesamt
KTA	Kerntechnischer Ausschuss
MCS	Monte-Carlo-Simulation
MLM	Maximum-Likelihood-Methode
MS	Microsoft®
MTTF	Mean Time To Failure
NAMUR	Normen- und Arbeitsgemeinschaft für Meß- und Regeltechnik
NE	NAMUR Empfehlung
OEM	Original Equipment Manufacturer
PES	Programmierbar elektronisches System
PFD	Probability of Failure on Demand
PFH_D	Probability of Dangerous Failure per Hour
PiU	Proven in Use
PL	Performance Level
PLT	Prozessleittechnik
PSA	Probabilistische Sicherheitsanalyse
QM	Qualitätsmanagement
Q-Q-Plot	Quantile-Quantile-Plot
RDF	Recueil de Données de Fiabilité
SAE	Society of Automotive Engineers
SIL	Sicherheits-Integritätslevel
SW	Software
THR	Tolerable Hazard Rate
Tkm	Tausendkilometer
TMF	Teilmarktfaktor
TR	Technical Report
TSK	Technisches Sicherheitskonzept

VDA	Verband der Automobilindustrie
VDE	Verband der Elektrotechnik Elektronik Informationstechnik
VDS	Vehicle Description Section
VIS	Vehicle Indicator Section
WMI	World Manufacturer Identification

A2 Fahrleistungsverteilungen der PiU-relevanten Baureihe

Nachfolgend werden die Ergebnisse der Ermittlungen der jährlichen Fahrleistungsverteilungen für die einzelnen Fahrzeugmodelle (insgesamt 49) sowie der einzelnen Cluster der PiU-relevanten Baureihe präsentiert. Hierbei wurde Deutschland sowohl als Vertriebs- als auch als Reparaturland gewählt. Die folgenden Ergebnisse beinhalten dabei jeweils:

- das untersuchte Fahrzeugmodell oder das untersuchte Cluster,
- die eingelesene und verwendete Datenmenge unter Angabe der aussortierten Datensätze,
- die graphische Darstellung der jährlichen FLV (empirisch (blaue Punkte mit roter Linie) und theoretisch (blaue Linie)),
- die Parameter (μ und σ) der an die empirischen Daten angepassten theoretischen Lognormal-Verteilungsfunktion,
- den Erwartungswert $E(S)$ der jährlichen Fahrleistungsverteilung,
- das Bestimmtheitsmaß der Anpassung.

Bei den Datenmengen wird zunächst angegeben, wie viele Datensätze überhaupt für das jeweilige Modell der Baureihe mit Deutschland als Vertriebs- und als Reparaturland in den GuK-Daten vorhanden sind (eingelesene Datensätze). Die verwendete Datenmenge entspricht den Datensätzen, aus denen die FLV letztendlich ermittelt worden ist. Diese Datenmenge ist um die Datensätze reduziert, bei denen entweder unplausible Datumsangaben (z.B. wenn das Reparaturdatum vor dem Produktionsdatum liegt) oder unplausible Kilometerangaben (z.B. bei einem Kilometerstand von 0 km oder wenn die jährliche Kilometerleistung außerhalb der vorgegeben Werte (<3 Tkm oder >150 Tkm) liegt) vorhanden sind.

A2.1 01-C-b

- Eingelesene Datensätze: 117, davon
  - 1 mit Datumsfehler und
  - 7 mit Fahrleistungsfehlern
- Verwendete Datensätze: 109

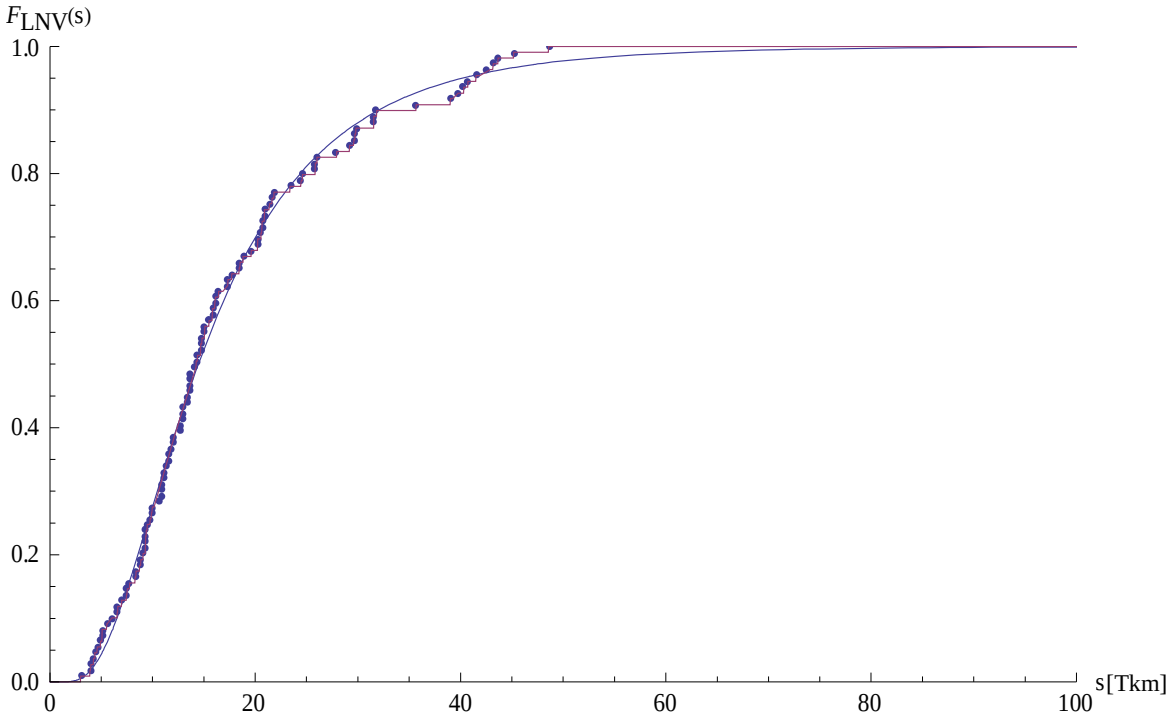


Bild A2-1: Jährliche Fahrleistungsverteilung für 01-C-b

- Parameter der Lognormal-Verteilung: $\mu = 2{,}6719$
  $\sigma = 0{,}62059$
- Erwartungswert der jährlichen FLV: $E(S) = 17{,}539\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99912$

A2.2 01-L-b/m

- Eingelesene Datensätze: 1.087, davon
  - 11 mit Datumsfehlern und
  - 25 mit Fahrleistungsfehlern
- Verwendete Datensätze: 1.051

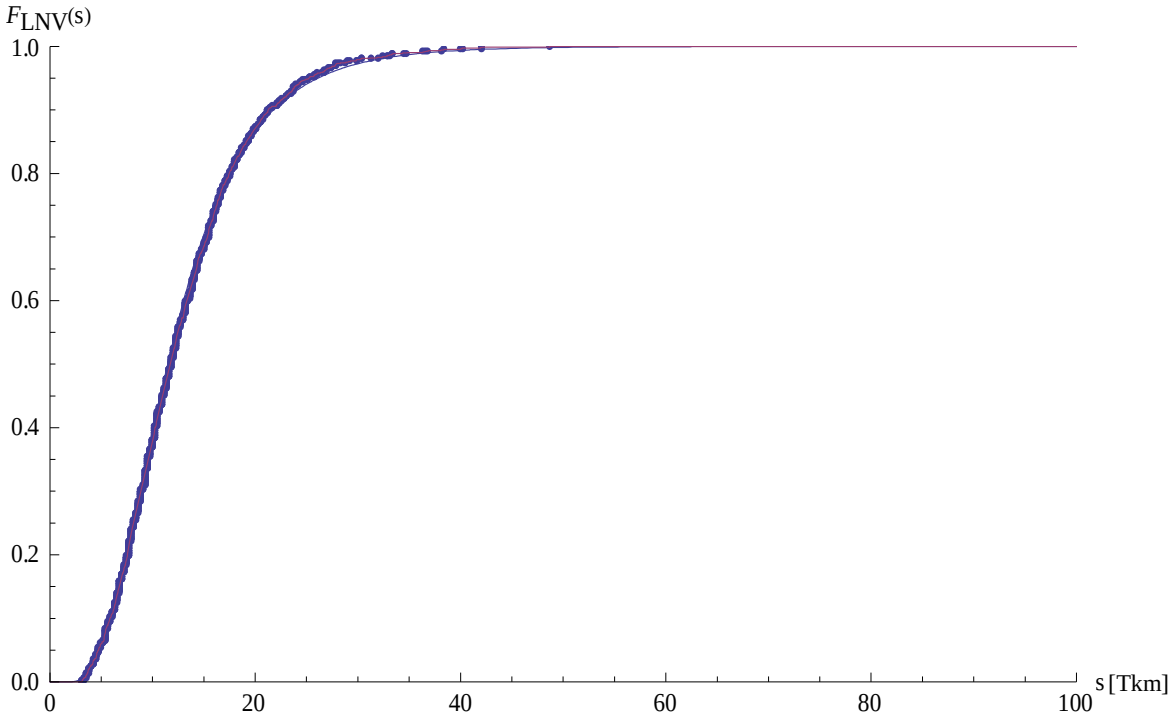


Bild A2-2: Jährliche Fahrleistungsverteilung für 01-L-b/m

- Parameter der Lognormal-Verteilung: $\mu = 2{,}4404$
  $\sigma = 0{,}49965$
- Erwartungswert der jährlichen FLV: $E(S) = 13{,}003\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99968$

A2.3 02-L-b

- Eingelesene Datensätze: 15.411, davon
  - 106 mit Datumsfehlern und
  - 158 mit Fahrleistungsfehlern
- Verwendete Datensätze: 15.147

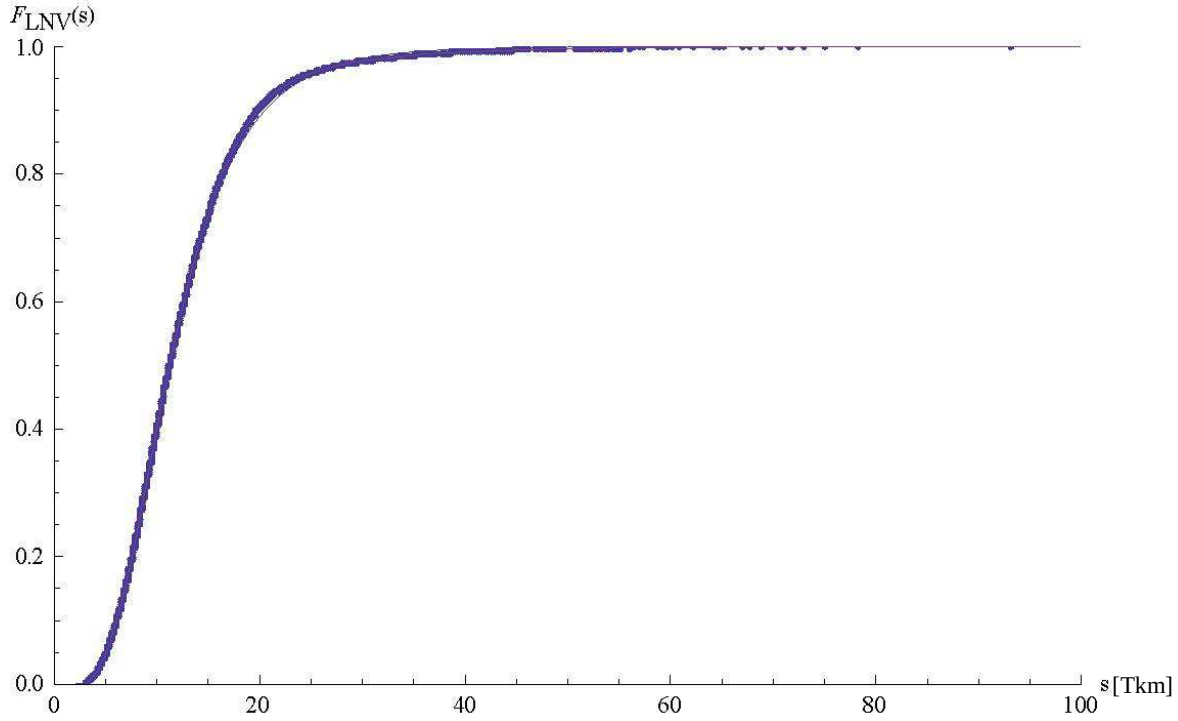


Bild A2-3: Jährliche Fahrleistungsverteilung für 02-L-b

- Parameter der Lognormal-Verteilung: $\mu = 2{,}4149$
  $\sigma = 0{,}4731$
- Erwartungswert der jährlichen FLV: $E(S) = 12{,}513\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99989$

A2.4 02-K-b

- Eingelesene Datensätze: 2.946, davon
  - 29 mit Datumsfehlern und
  - 12 mit Fahrleistungsfehlern
- Verwendete Datensätze: 2.905

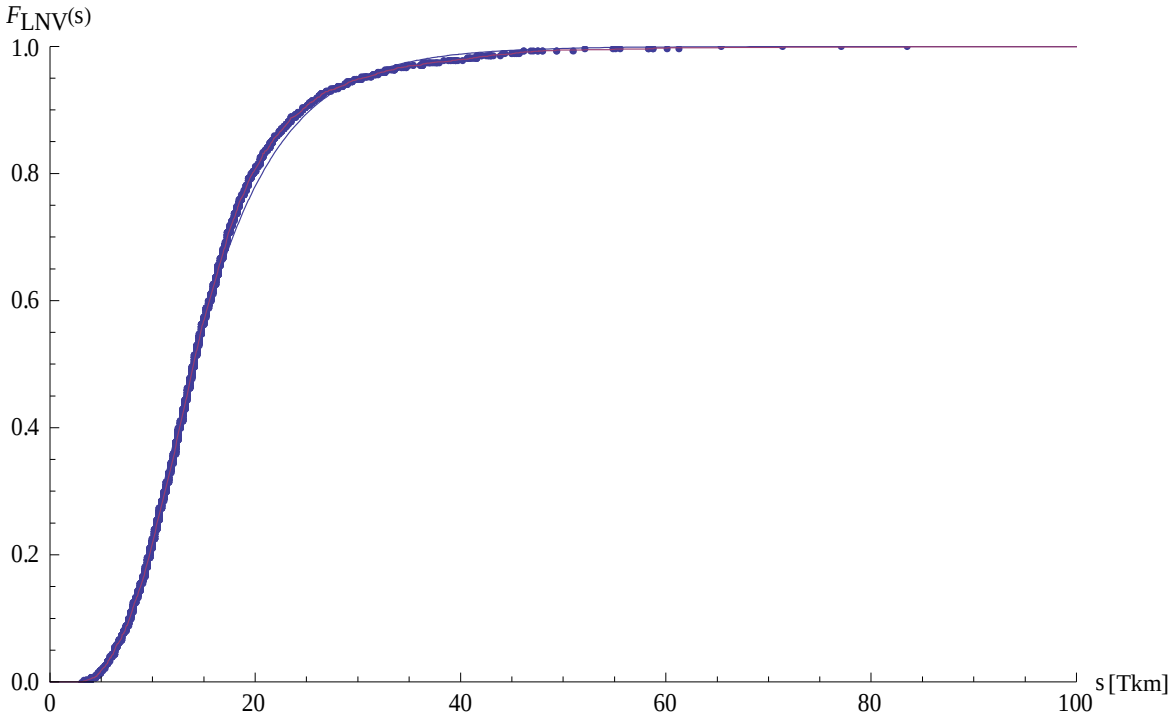


Bild A2-4: Jährliche Fahrleistungsverteilung für 02-K-b

- Parameter der Lognormal-Verteilung: $\mu = 2{,}6358$
  $\sigma = 0{,}46713$
- Erwartungswert der jährlichen FLV: $E(S) = 15{,}563\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99929$

A2.5 02-C-b/m

- Eingelesene Datensätze: 5.887, davon
  - 47 mit Datumsfehlern und
  - 69 mit Fahrleistungsfehlern
- Verwendete Datensätze: 5.771

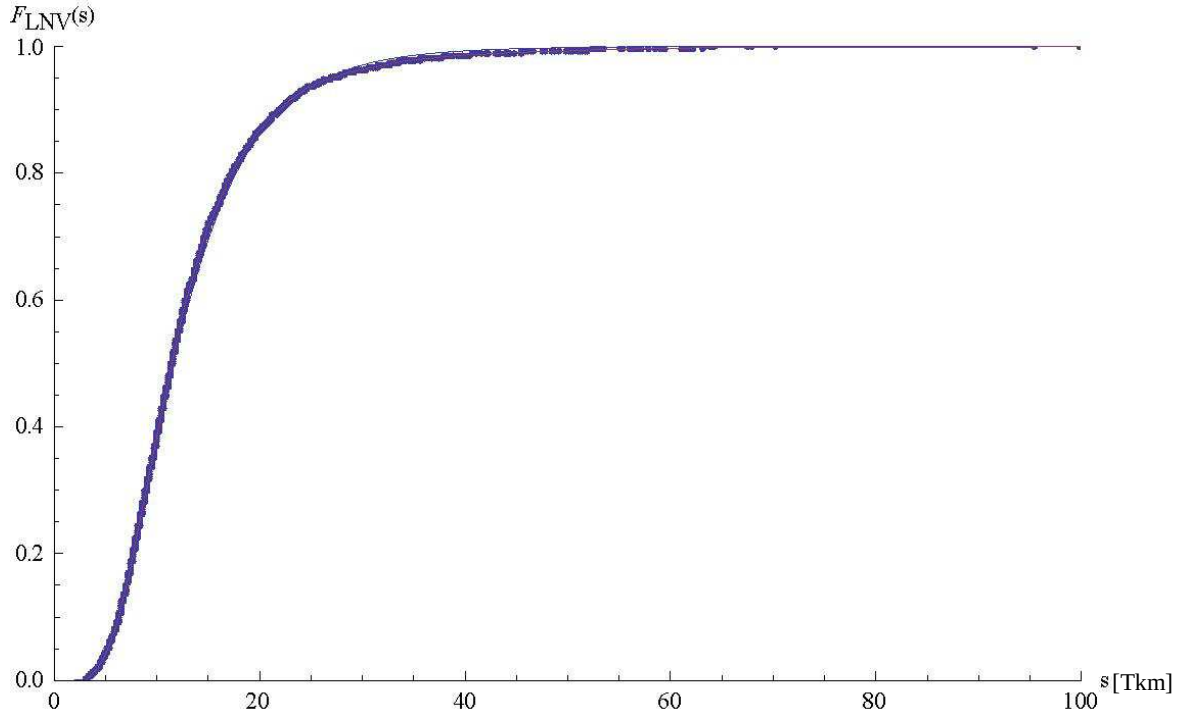


Bild A2-5: Jährliche Fahrleistungsverteilung für 02-C-b/m

- Parameter der Lognormal-Verteilung: $\mu = 2{,}4536$
  $\sigma = 0{,}50102$
- Erwartungswert der jährlichen FLV: $E(S) = 13{,}186\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99976$

A2.6 02-L-b/m

- Eingelesene Datensätze: 56.220, davon
  - 523 mit Datumsfehlern und
  - 781 mit Fahrleistungsfehlern
- Verwendete Datensätze: 54.916

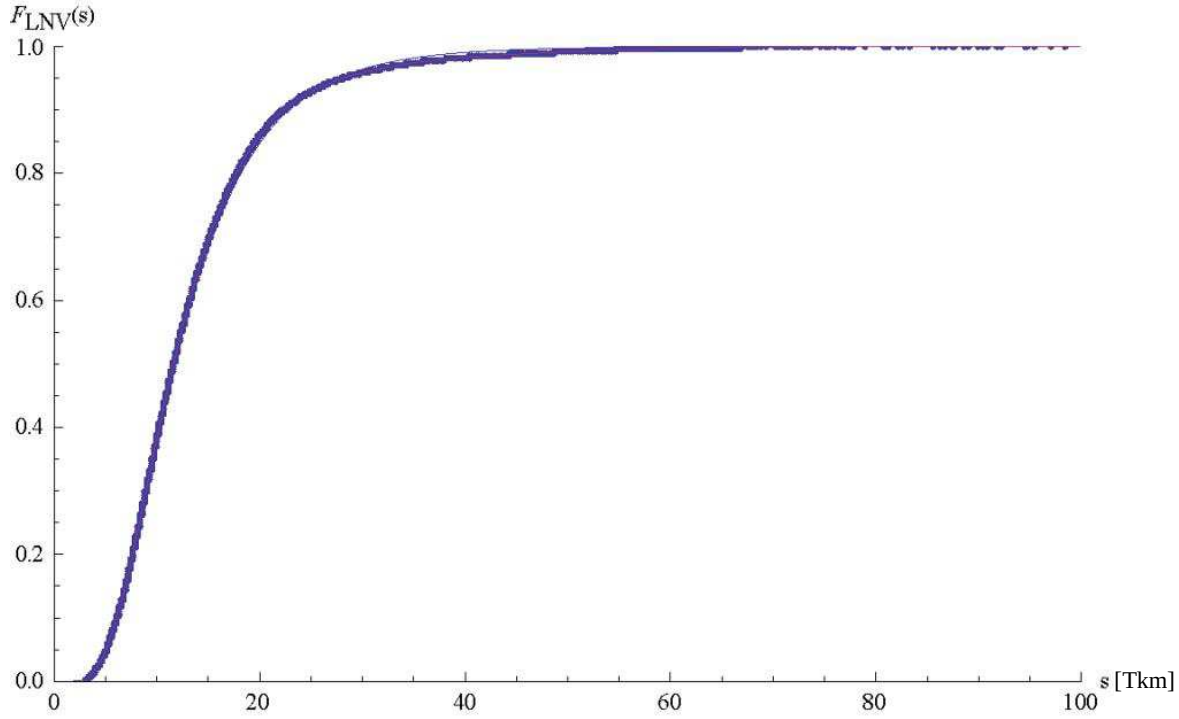


Bild A2-6: Jährliche Fahrleistungsverteilung für 02-L-b/m

- Parameter der Lognormal-Verteilung: $\mu = 2{,}4632$
  $\sigma = 0{,}52048$
- Erwartungswert der jährlichen FLV: $E(S) = 13{,}445\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99988$

A2.7 02-K-b/m

- Eingelesene Datensätze: 25.357, davon
  - 269 mit Datumsfehlern und
  - 161 mit Fahrleistungsfehlern
- Verwendete Datensätze: 24.927

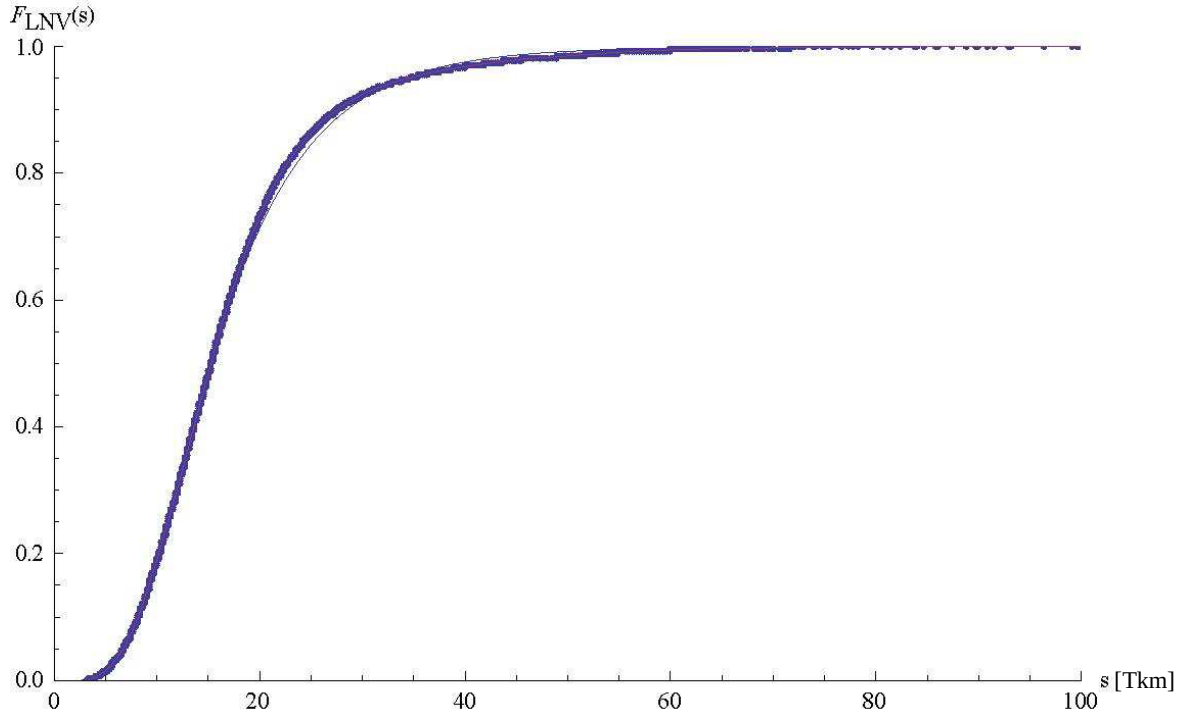


Bild A2-7: Jährliche Fahrleistungsverteilung für 02-K-b/m

- Parameter der Lognormal-Verteilung: $\mu = 2{,}719$
  $\sigma = 0{,}49246$
- Erwartungswert der jährlichen FLV: $E(S) = 17{,}12\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99959$

A2.8 03-C-b/m

- Eingelesene Datensätze: 1.282, davon
  - 6 mit Datumsfehlern und
  - 31 mit Fahrleistungsfehlern
- Verwendete Datensätze: 1.245

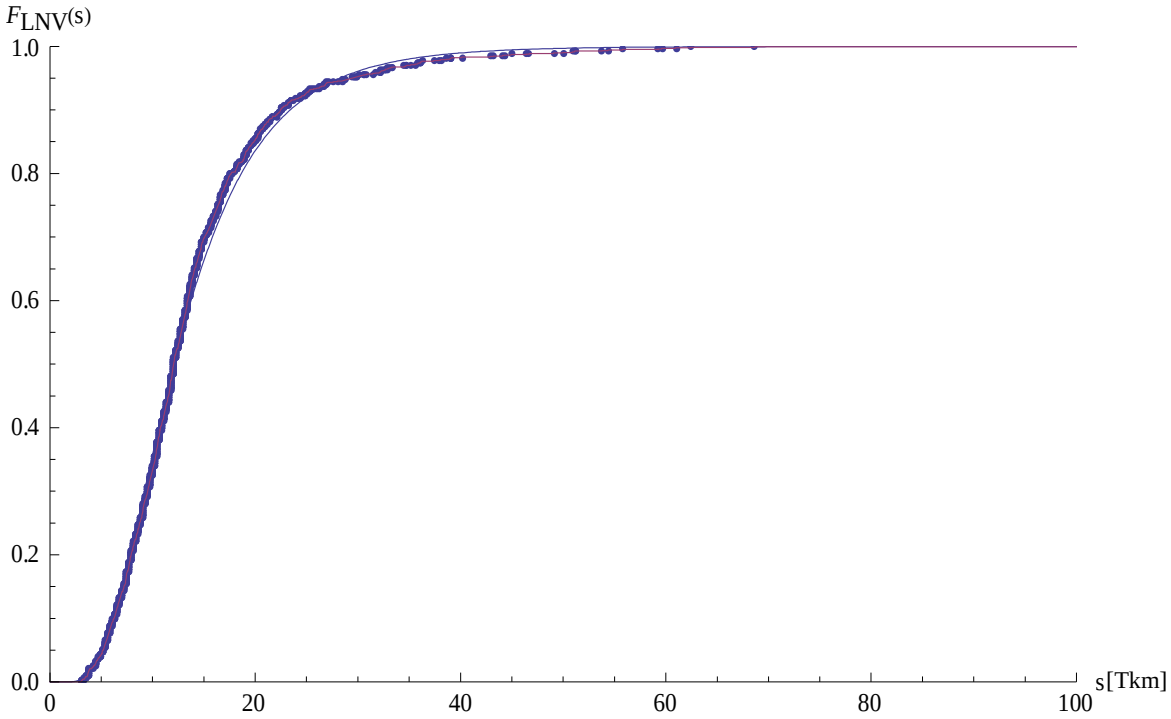


Bild A2-8: Jährliche Fahrleistungsverteilung für 03-C-b/m

- Parameter der Lognormal-Verteilung: $\mu = 2{,}4909$
  $\sigma = 0{,}51692$
- Erwartungswert der jährlichen FLV: $E(S) = 13{,}789\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99918$

A2.9 03-L-b/m

- Eingelesene Datensätze: 38.777, davon
  - 489 mit Datumsfehlern und
  - 452 mit Fahrleistungsfehlern
- Verwendete Datensätze: 37.836

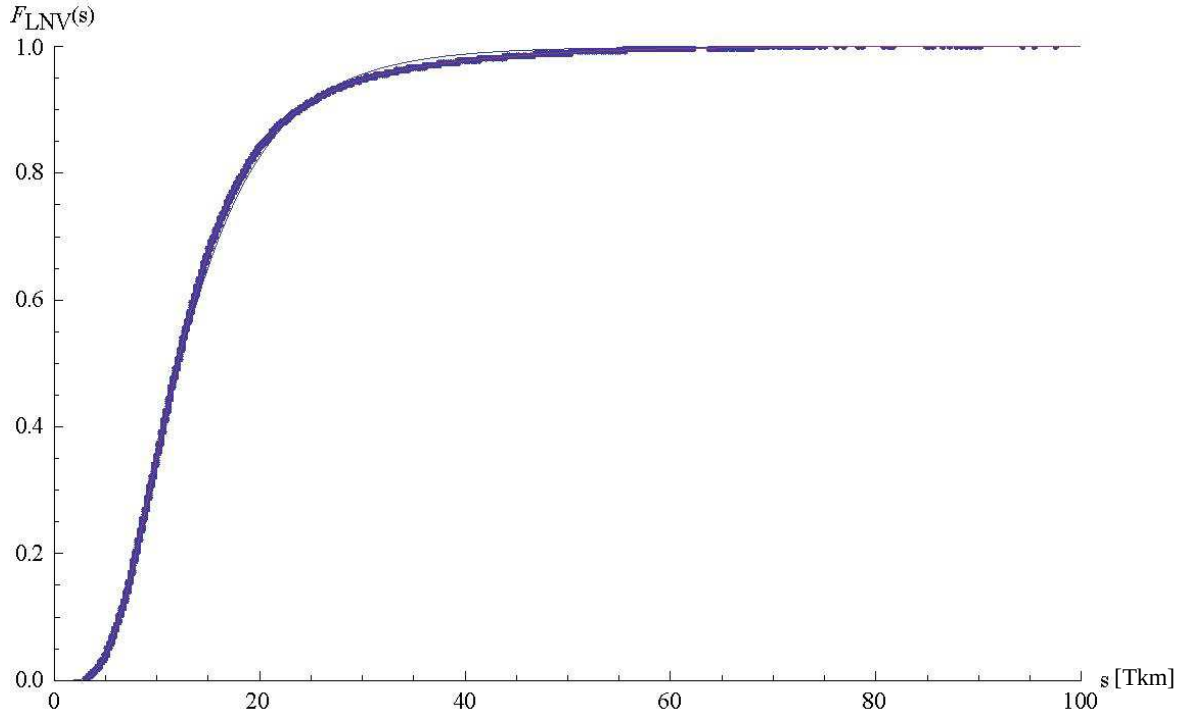


Bild A2-9: Jährliche Fahrleistungsverteilung für 03-L-b/m

- Parameter der Lognormal-Verteilung: $\mu = 2{,}5034$
  $\sigma = 0{,}52545$
- Erwartungswert der jährlichen FLV: $E(S) = 14{,}034\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99968$

A2.10 03-K-b/m

- Eingelesene Datensätze: 15.949, davon
  - 262 mit Datumsfehlern und
  - 69 mit Fahrleistungsfehlern
- Verwendete Datensätze: 15.618

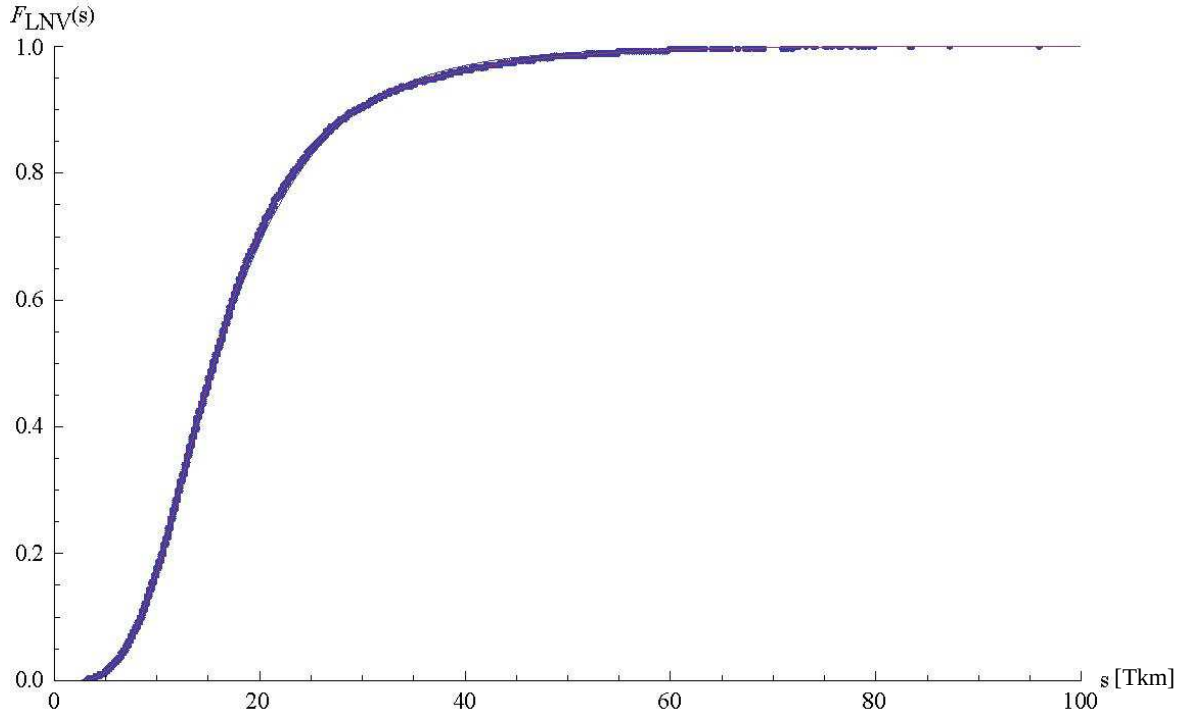


Bild A2-10: Jährliche Fahrleistungsverteilung für 03-K-b/m

- Parameter der Lognormal-Verteilung: $\mu = 2{,}7494$
  $\sigma = 0{,}49987$
- Erwartungswert der jährlichen FLV: $E(S) = 17{,}713\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99973$

A2.11 03-L-b/e/m

- Eingelesene Datensätze: 300, davon
  - 11 mit Datumsfehlern
- Verwendete Datensätze: 289

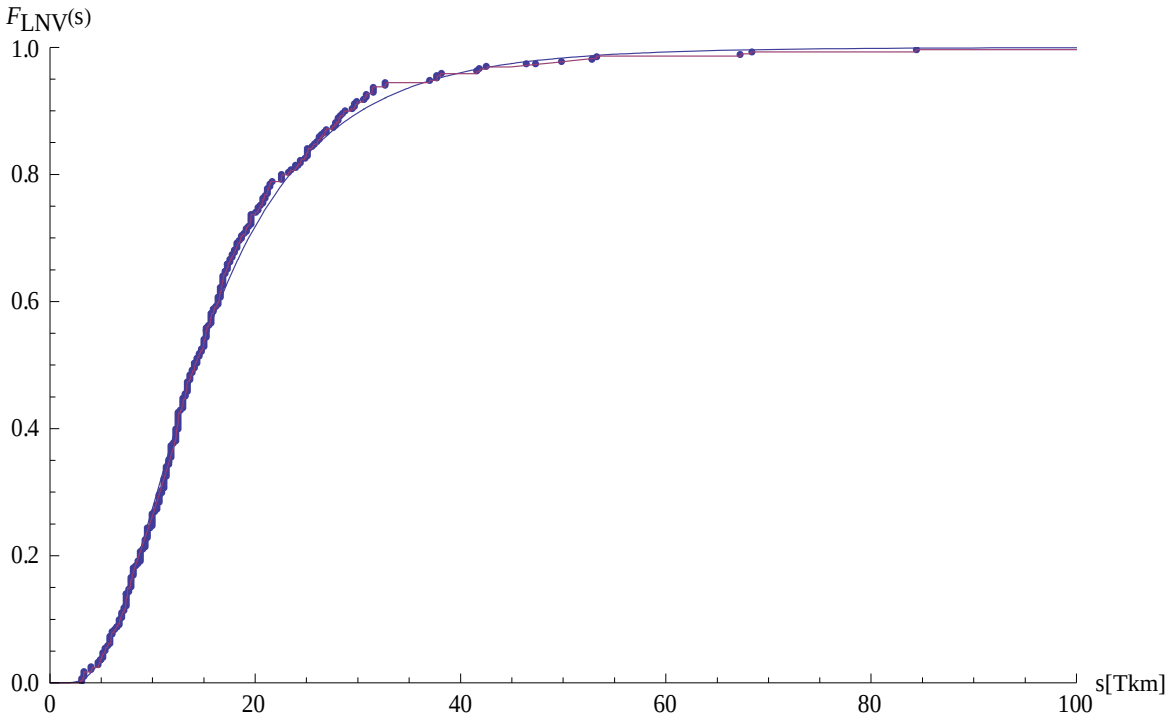


Bild A2-11: Jährliche Fahrleistungsverteilung für 03-L-b/e/m

- Parameter der Lognormal-Verteilung: $\mu = 2{,}6547$
  $\sigma = 0{,}59031$
- Erwartungswert der jährlichen FLV: $E(S) = 16{,}928\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99954$

A2.12 03-K-b/e/m

- Eingelesene Datensätze: 106, davon
  - 3 mit Datumsfehlern und
  - 2 mit Fahrleistungsfehlern
- Verwendete Datensätze: 101

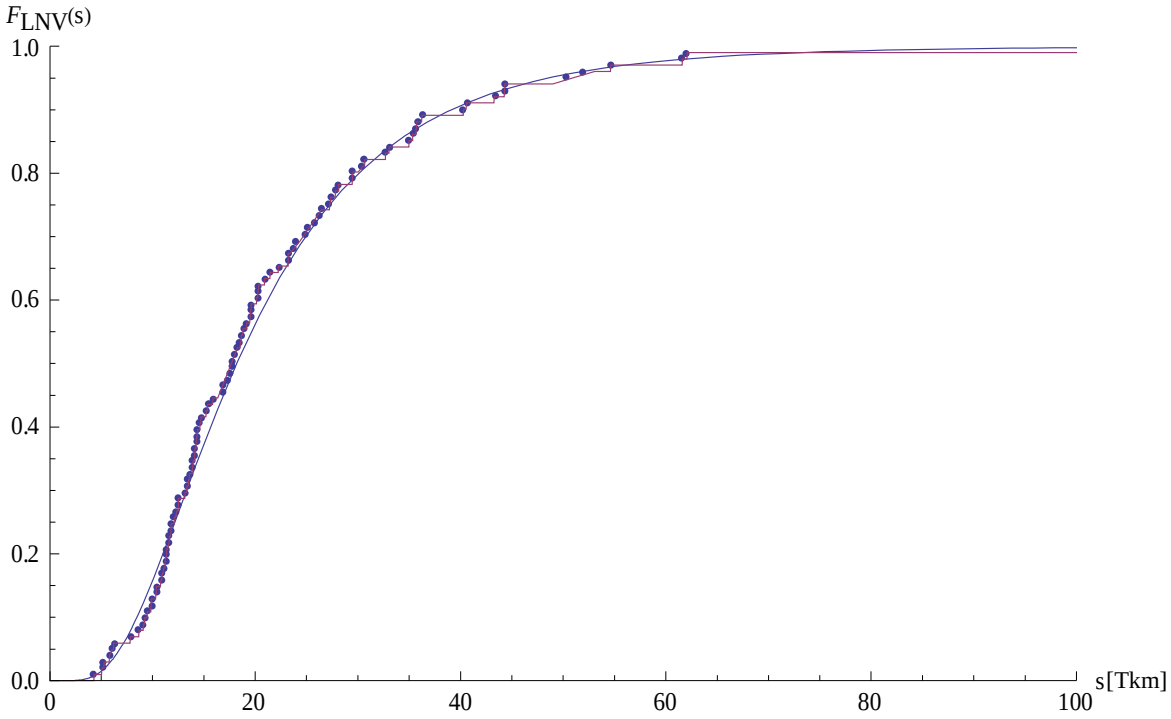


Bild A2-12: Jährliche Fahrleistungsverteilung für 03-K-b/e/m

- Parameter der Lognormal-Verteilung: $\mu = 2{,}9018$
  $\sigma = 0{,}5963$
- Erwartungswert der jährlichen FLV: $E(S) = 21{,}75\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99874$

A2.13 03-C-d

- Eingelesene Datensätze: 1.006, davon
  - 12 mit Datumsfehlern und
  - 2 mit Fahrleistungsfehlern
- Verwendete Datensätze: 992

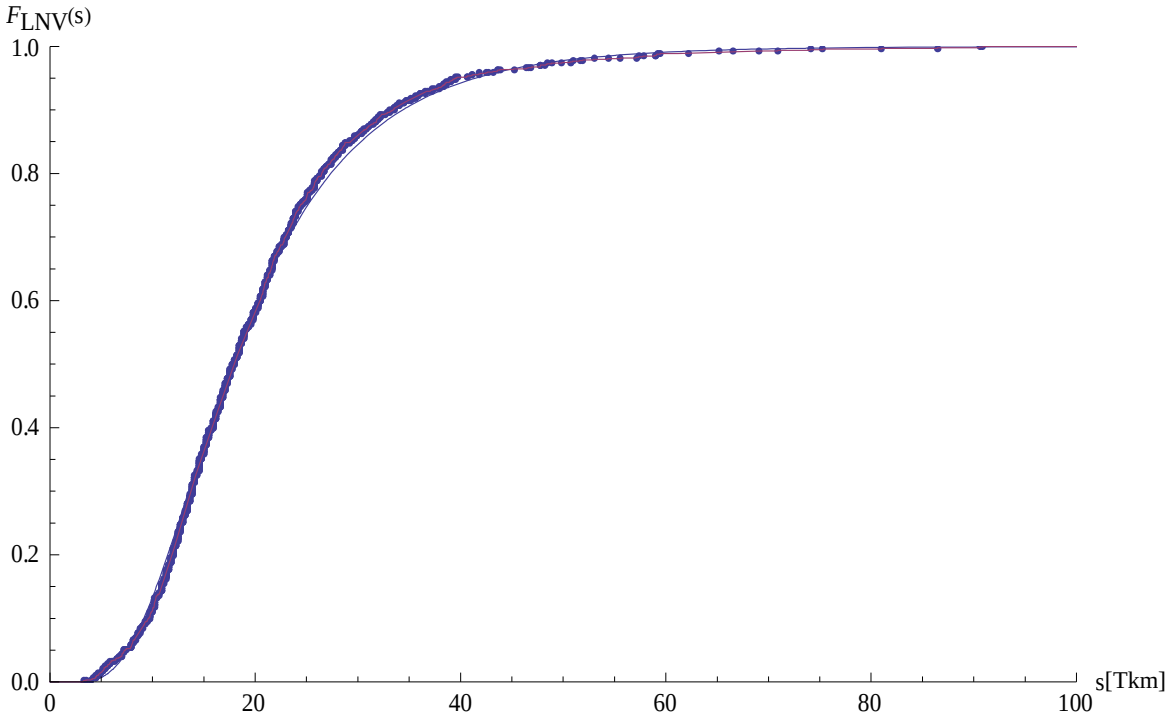


Bild A2-13: Jährliche Fahrleistungsverteilung für 03-C-d

- Parameter der Lognormal-Verteilung: $\mu = 2{,}8755$
  $\sigma = 0{,}51614$
- Erwartungswert der jährlichen FLV: $E(S) = 20{,}261\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99952$

A2.14 03-L-d

- Eingelesene Datensätze: 37.300, davon
  - 315 mit Datumsfehlern und
  - 230 mit Fahrleistungsfehlern
- Verwendete Datensätze: 36.755

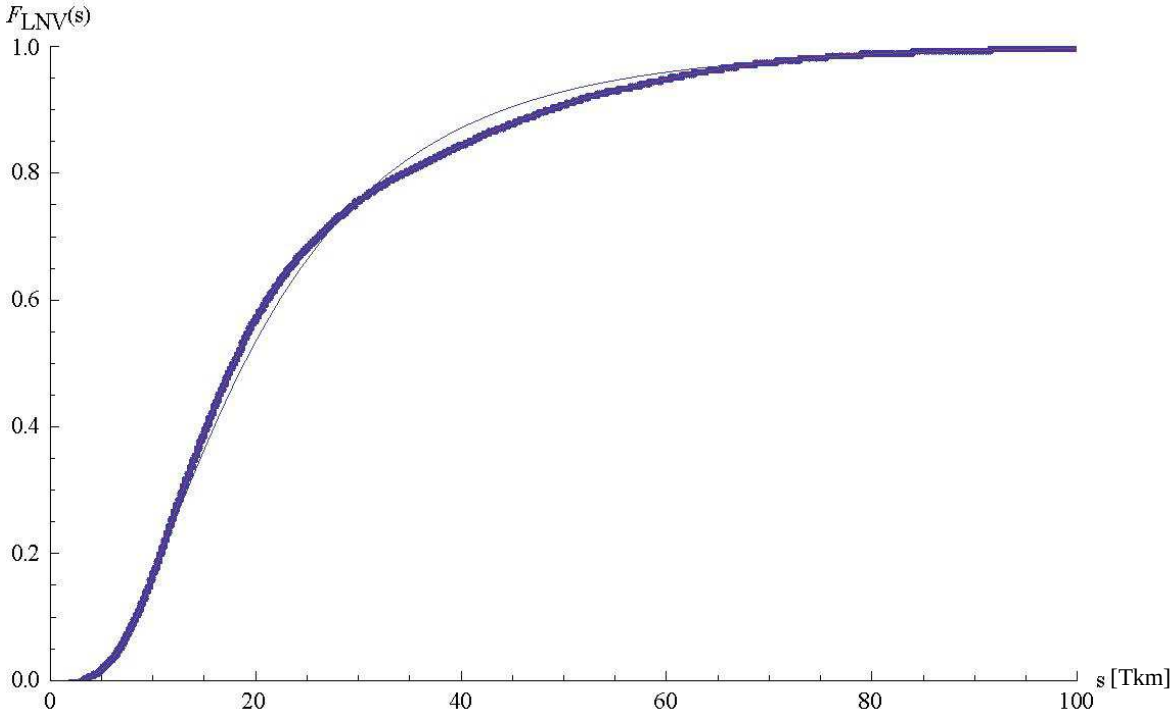


Bild A2-14: Jährliche Fahrleistungsverteilung für 03-L-d

- Parameter der Lognormal-Verteilung: $\mu = 2{,}9379$
  $\sigma = 0{,}66263$
- Erwartungswert der jährlichen FLV: $E(S) = 23{,}511\,Tkm$
- Bestimmtheitsmaß: $B = 0{,}99872$

A2.15 03-K-d

- Eingelesene Datensätze: 28.278, davon
  - 233 mit Datumsfehlern und
  - 93 mit Fahrleistungsfehlern
- Verwendete Datensätze: 27.952

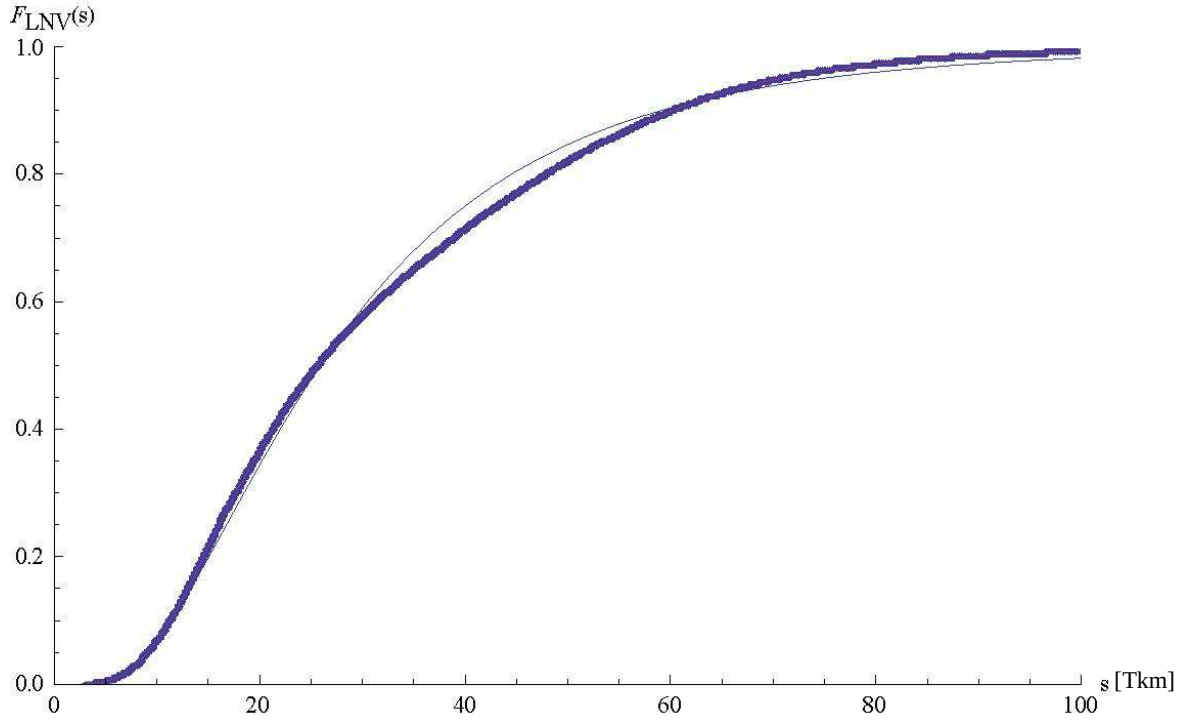


Bild A2-15: Jährliche Fahrleistungsverteilung für 03-K-d

- Parameter der Lognormal-Verteilung: $\mu = 3{,}2544$
  $\sigma = 0{,}64328$
- Erwartungswert der jährlichen FLV: $E(S) = 31{,}859\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99899$

A2.16 04-C-d

- Eingelesene Datensätze: 2.221, davon
  - 23 mit Datumsfehlern und
  - 7 mit Fahrleistungsfehlern
- Verwendete Datensätze: 2.191

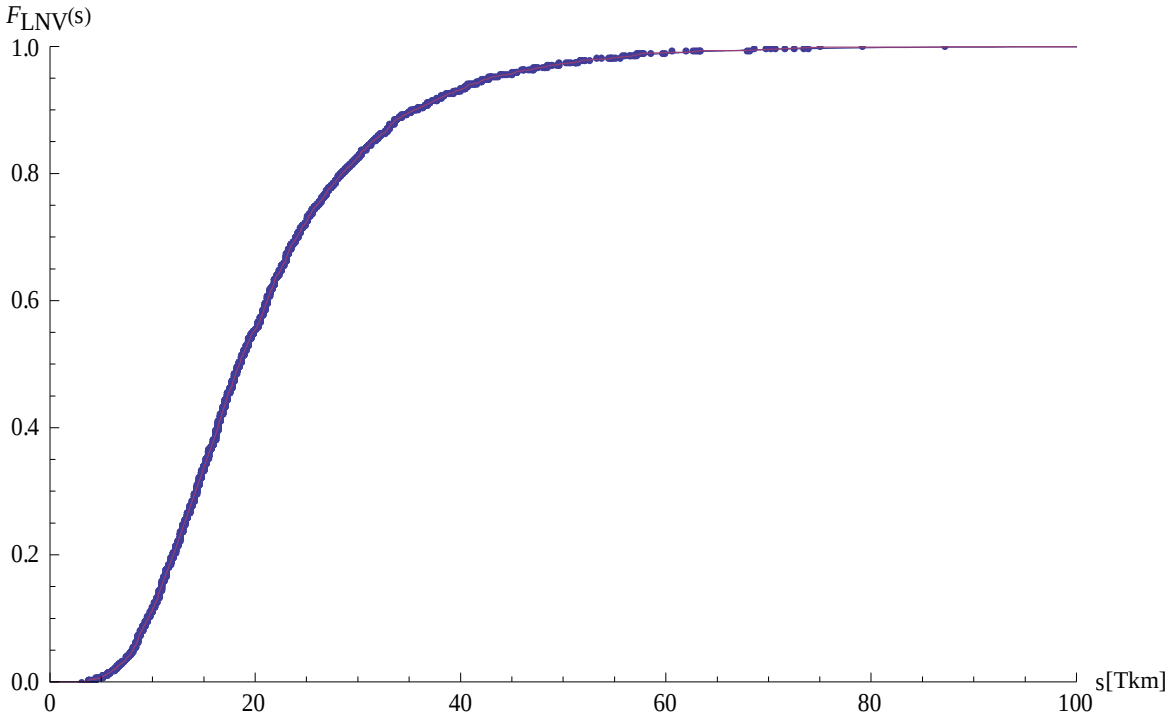


Bild A2-16: Jährliche Fahrleistungsverteilung für 04-C-d

- Parameter der Lognormal-Verteilung: $\mu = 2{,}9169$
  $\sigma = 0{,}51378$
- Erwartungswert der jährlichen FLV: $E(S) = 21{,}091\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99996$

A2.17 04-L-d

- Eingelesene Datensätze: 57.378, davon
  - 436 mit Datumsfehlern und
  - 283 mit Fahrleistungsfehlern
- Verwendete Datensätze: 56.659

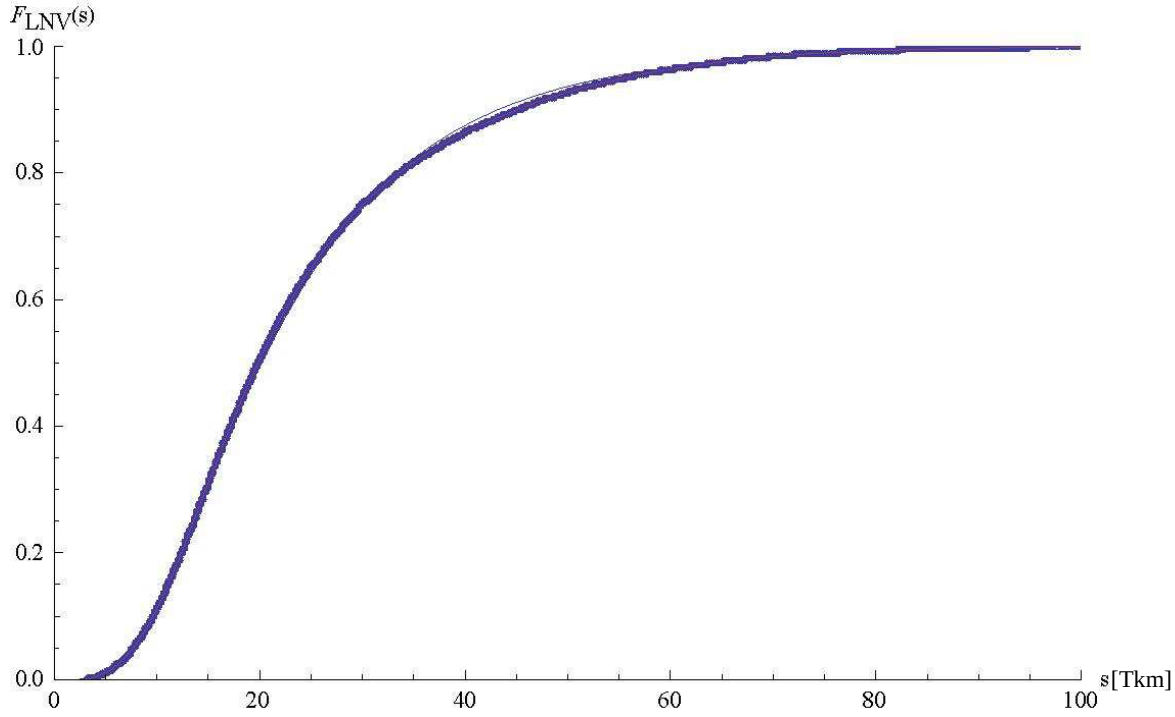


Bild A2-17: Jährliche Fahrleistungsverteilung für 04-L-d

- Parameter der Lognormal-Verteilung: $\mu = 3{,}0058$
  $\sigma = 0{,}59278$
- Erwartungswert der jährlichen FLV: $E(S) = 24{,}081\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99982$

A2.18 04-K-d

- Eingelesene Datensätze: 52.032, davon
  - 510 mit Datumsfehlern und
  - 109 mit Fahrleistungsfehlern
- Verwendete Datensätze: 51.413

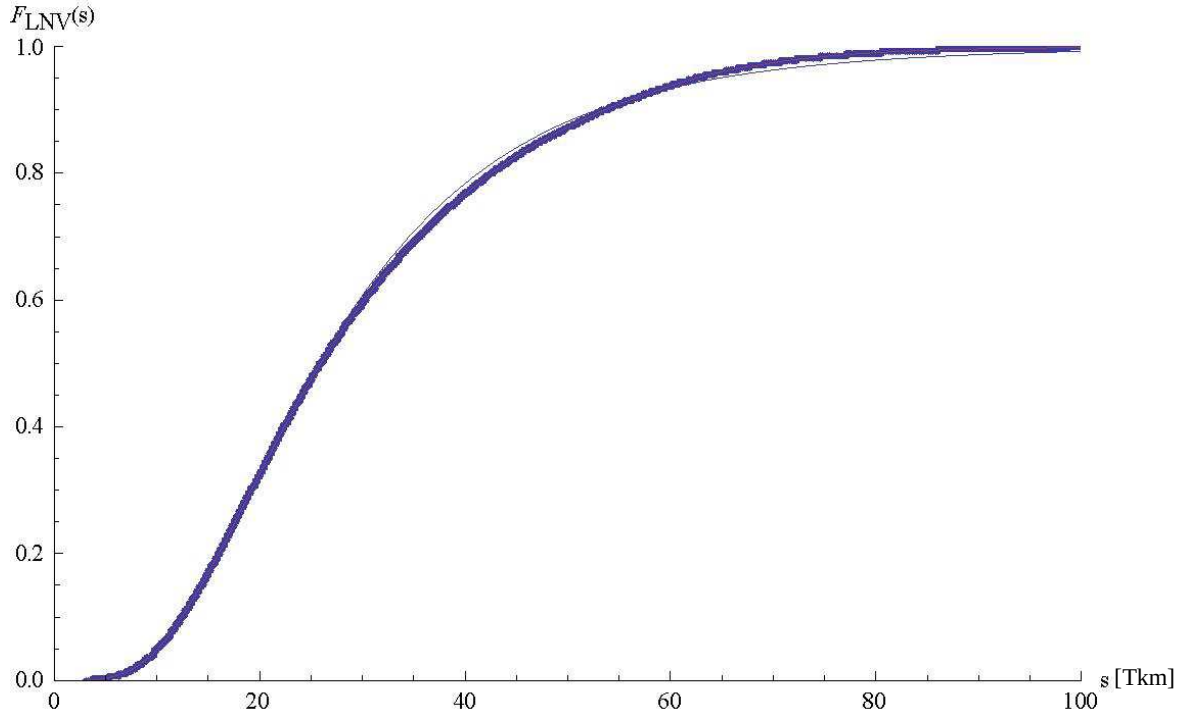


Bild A2-18: Jährliche Fahrleistungsverteilung für 04-K-d

- Parameter der Lognormal-Verteilung: $\mu = 3{,}2485$
  $\sigma = 0{,}56017$
- Erwartungswert der jährlichen FLV: $E(S) = 30{,}125\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99986$

A2.19 05-C-b

- Eingelesene Datensätze: 1.186, davon
  - 45 mit Datumsfehlern und
  - 37 mit Fahrleistungsfehlern
- Verwendete Datensätze: 1.104

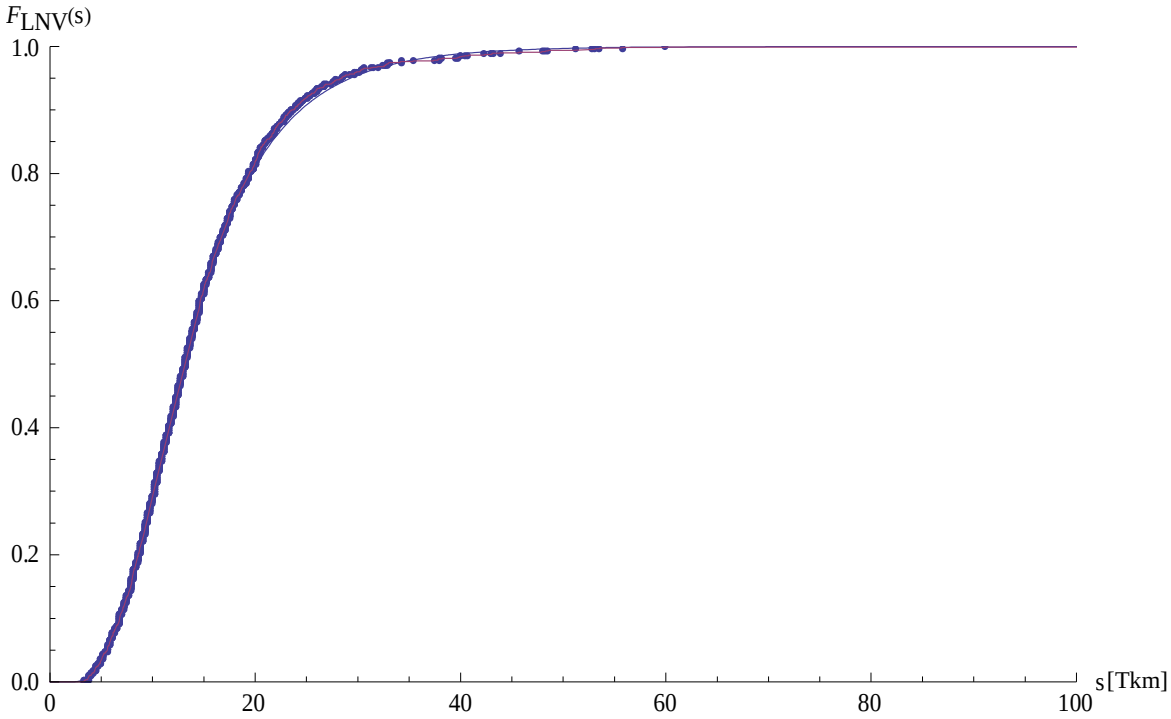


Bild A2-19: Jährliche Fahrleistungsverteilung für 05-C-b

- Parameter der Lognormal-Verteilung: $\mu = 2{,}5599$
  $\sigma = 0{,}49665$
- Erwartungswert der jährlichen FLV: $E(S) = 14{,}632\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99976$

A2.20 05-L-b

- Eingelesene Datensätze: 1.333, davon
  - 41 mit Datumsfehlern und
  - 18 mit Fahrleistungsfehlern
- Verwendete Datensätze: 1.274

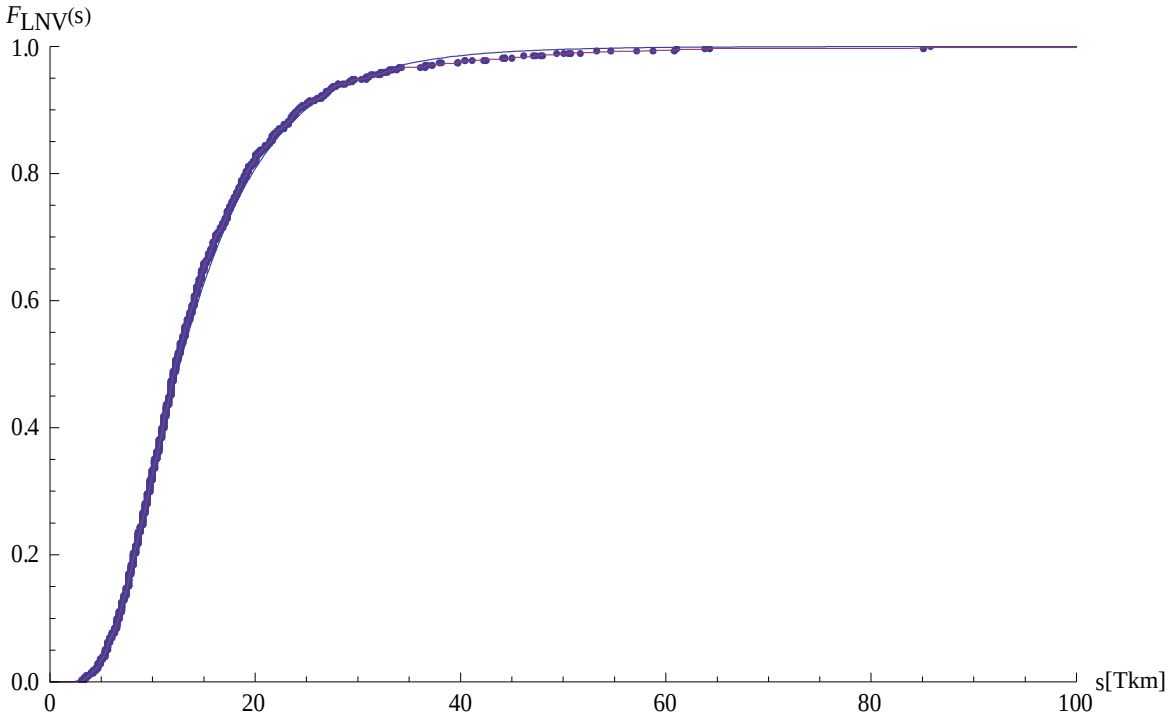


Bild A2-20: Jährliche Fahrleistungsverteilung für 05-L-b

- Parameter der Lognormal-Verteilung: $\mu = 2{,}5381$
  $\sigma = 0{,}52728$
- Erwartungswert der jährlichen FLV: $E(S) = 14{,}543\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99965$

A2.21 05-K-b

- Eingelesene Datensätze: 1.309, davon
  - 59 mit Datumsfehlern und
  - 7 mit Fahrleistungsfehlern
- Verwendete Datensätze: 1.243

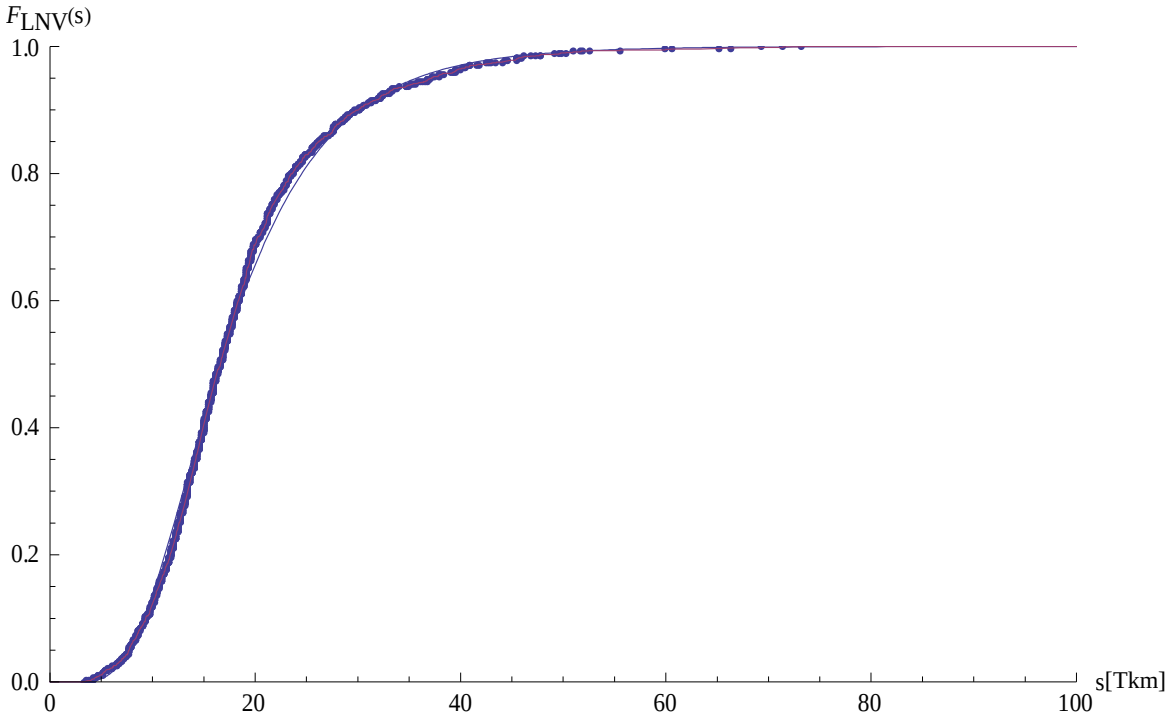


Bild A2-21: Jährliche Fahrleistungsverteilung für 05-K-b

- Parameter der Lognormal-Verteilung: $\mu = 2{,}8083$
  $\sigma = 0{,}46605$
- Erwartungswert der jährlichen FLV: $E(S) = 18{,}484\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99907$

A2.22 05-L-b/m

- Eingelesene Datensätze: 3.540, davon
  - 77 mit Datumsfehlern und
  - 26 mit Fahrleistungsfehlern
- Verwendete Datensätze: 3.437

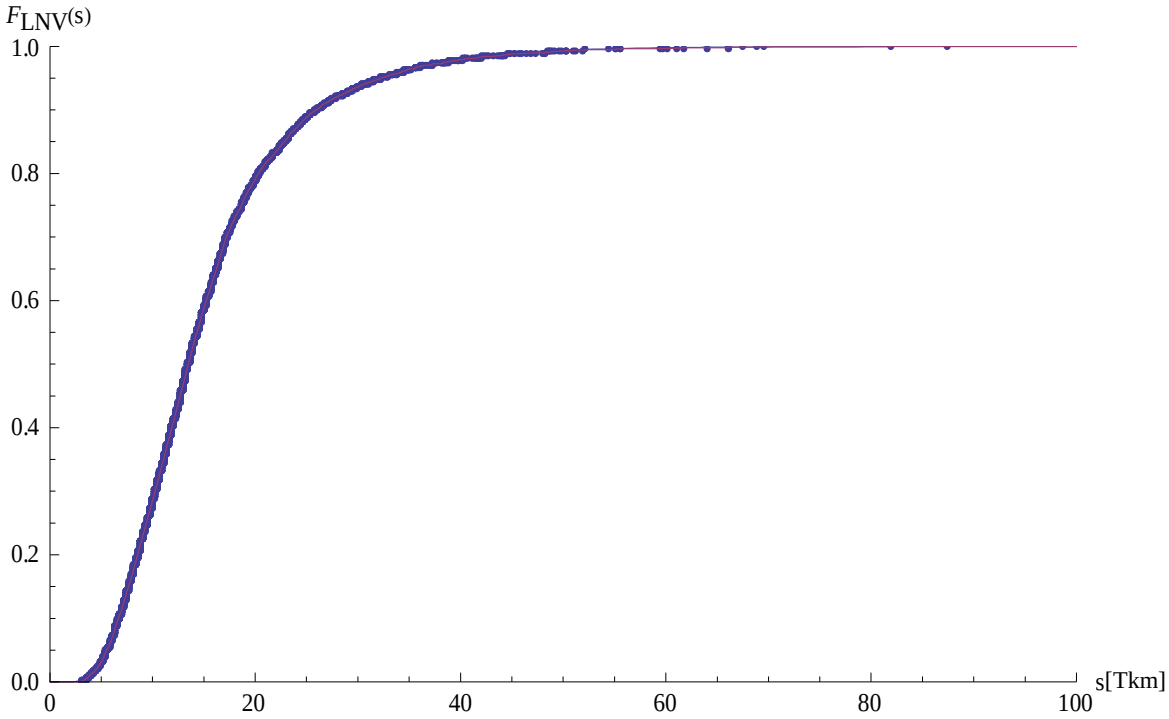


Bild A2-22: Jährliche Fahrleistungsverteilung für 05-L-b/m

- Parameter der Lognormal-Verteilung: $\mu = 2{,}5908$
  $\sigma = 0{,}52587$
- Erwartungswert der jährlichen FLV: $E(S) = 15{,}319\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99982$

A2.23 05-K-b/m

- Eingelesene Datensätze: 592, davon
  - 22 mit Datumsfehlern und
  - 3 mit Fahrleistungsfehlern
- Verwendete Datensätze: 567

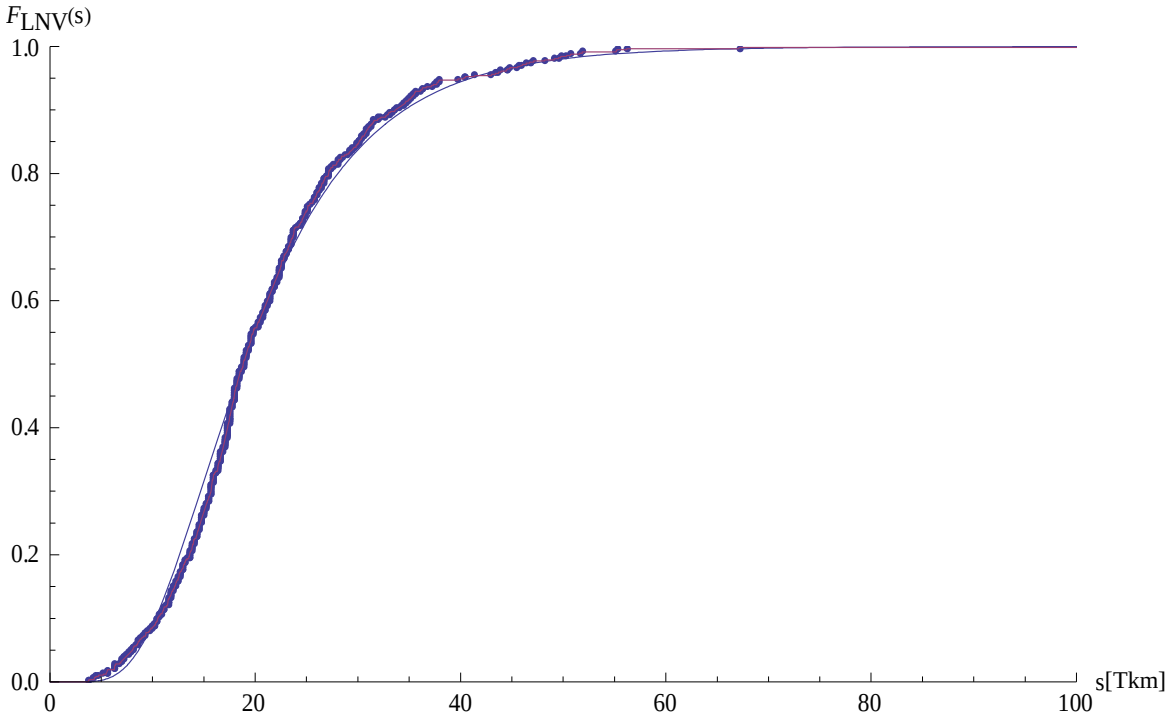


Bild A2-23: Jährliche Fahrleistungsverteilung für 05-K-b/m

- Parameter der Lognormal-Verteilung: $\mu = 2{,}9358$
  $\sigma = 0{,}4733$
- Erwartungswert der jährlichen FLV: $E(S) = 21{,}069\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99829$

A2.24 06-L-b

- Eingelesene Datensätze: 3.195, davon
  - 31 mit Datumsfehlern und
  - 41 mit Fahrleistungsfehlern
- Verwendete Datensätze: 3.123

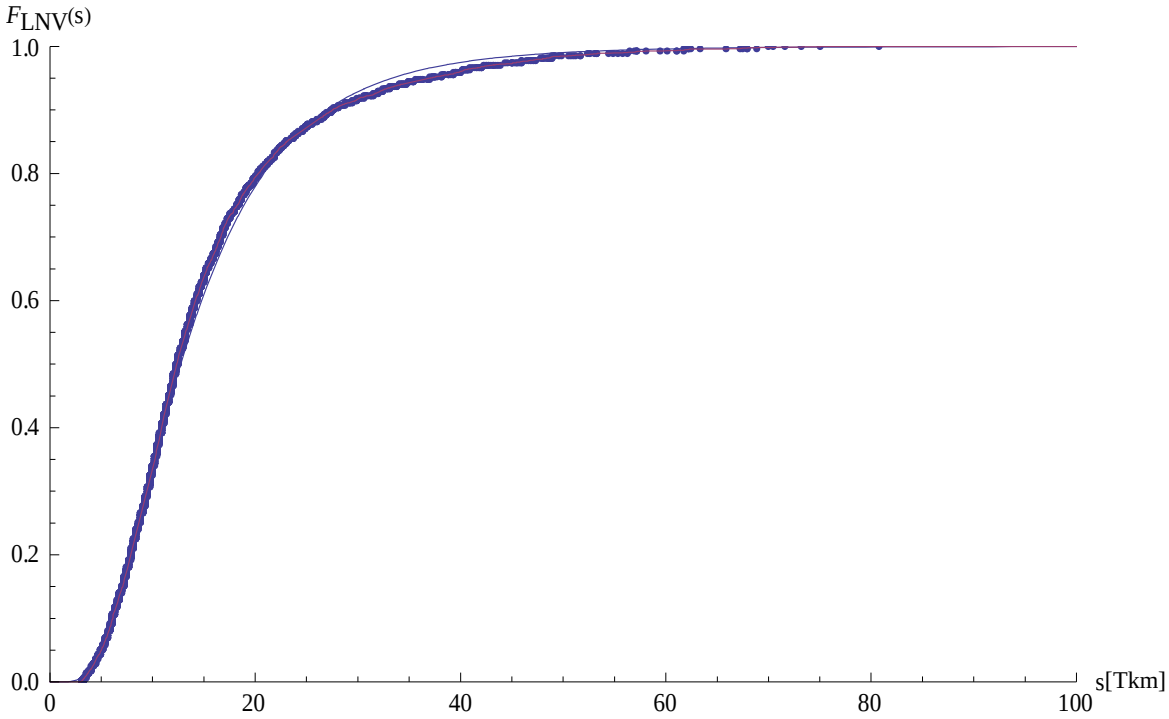


Bild A2-24: Jährliche Fahrleistungsverteilung für 06-L-b

- Parameter der Lognormal-Verteilung: $\mu = 2{,}5462$
  $\sigma = 0{,}58343$
- Erwartungswert der jährlichen FLV: $E(S) = 15{,}125\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99949$

A2.25 06-K-b

- Eingelesene Datensätze: 1.418, davon
  - 27 mit Datumsfehlern und
  - 10 mit Fahrleistungsfehlern
- Verwendete Datensätze: 1.381

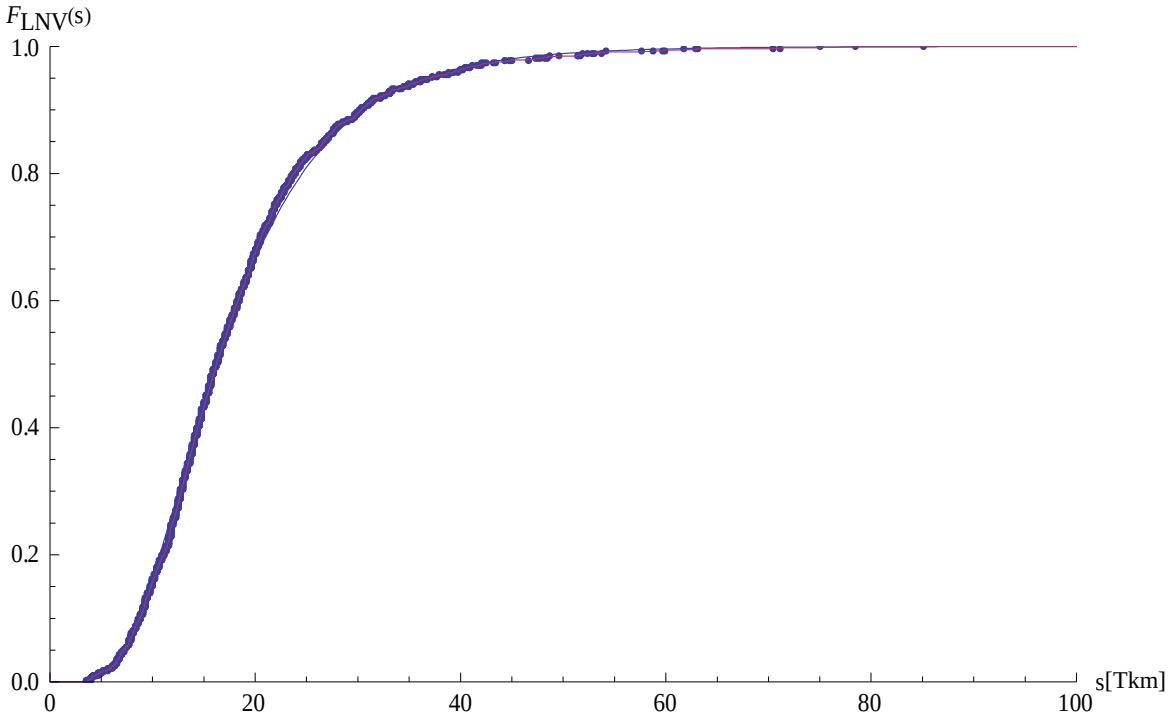


Bild A2-25: Jährliche Fahrleistungsverteilung für 06-K-b

- Parameter der Lognormal-Verteilung: $\mu = 2{,}7867$
  $\sigma = 0{,}49344$
- Erwartungswert der jährlichen FLV: $E(S) = 18{,}328\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99969$

A2.26 06-L-b/a

- Eingelesene Datensätze: 355, davon
  - 1 mit Datumsfehler und
  - 1 mit Fahrleistungsfehler
- Verwendete Datensätze: 353

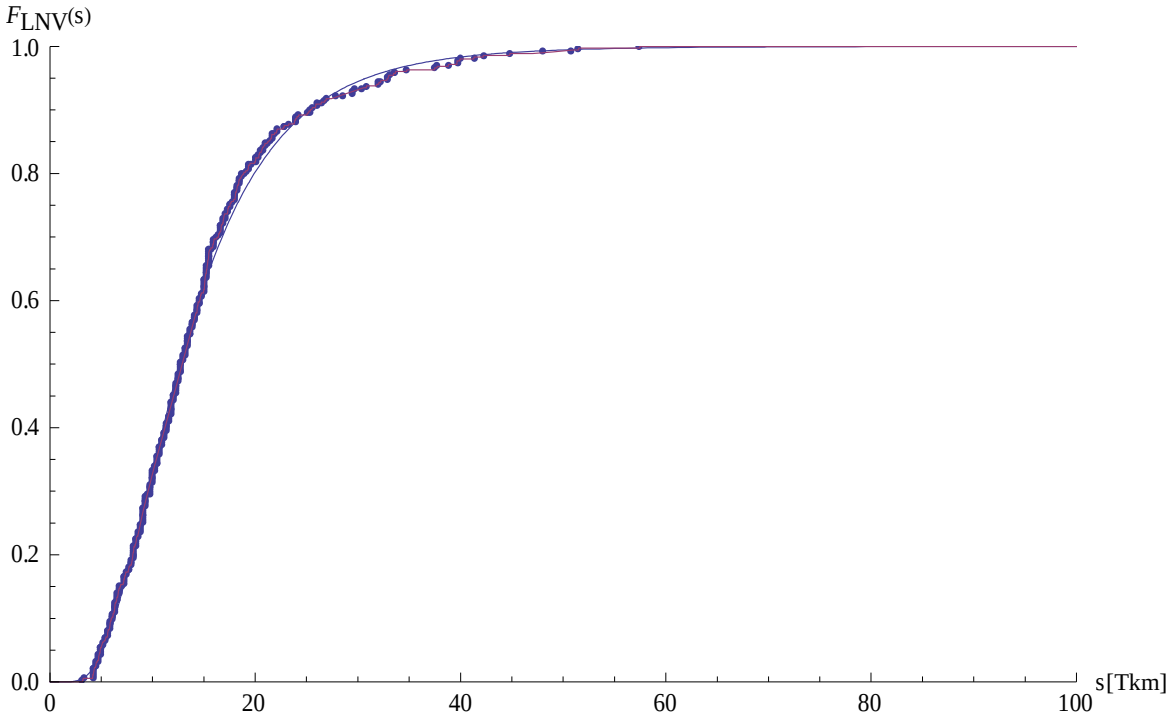


Bild A2-26: Jährliche Fahrleistungsverteilung für 06-L-b/a

- Parameter der Lognormal-Verteilung: $\mu = 2{,}5355$
  $\sigma = 0{,}54233$
- Erwartungswert der jährlichen FLV: $E(S) = 14{,}622\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}9994$

A2.27 06-K-b/a

- Eingelesene Datensätze: 332, davon
  - 1 mit Datumsfehler und
  - 1 mit Fahrleistungsfehler
- Verwendete Datensätze: 330

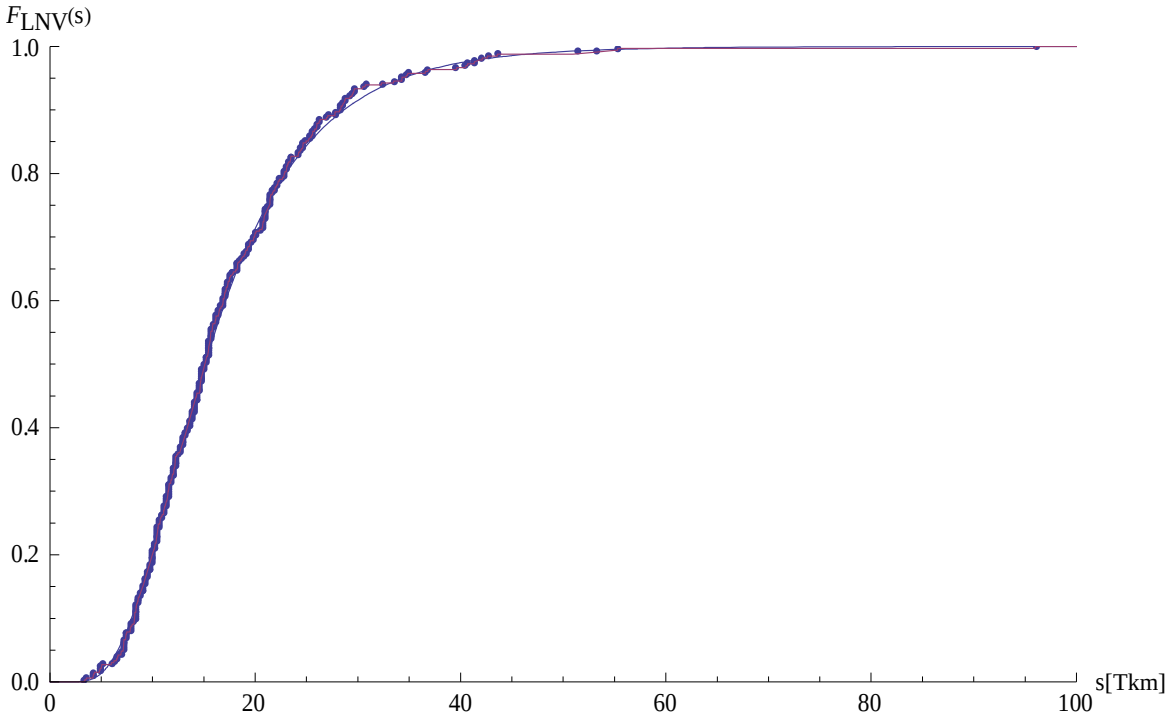


Bild A2-27: Jährliche Fahrleistungsverteilung für 06-K-b/a

- Parameter der Lognormal-Verteilung: $\mu = 2{,}7136$
  $\sigma = 0{,}5003$
- Erwartungswert der jährlichen FLV: $E(S) = 17{,}095\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99976$

A2.28 07-L-d

- Eingelesene Datensätze: 6.773, davon
  - 77 mit Datumsfehlern und
  - 20 mit Fahrleistungsfehlern
- Verwendete Datensätze: 6.676

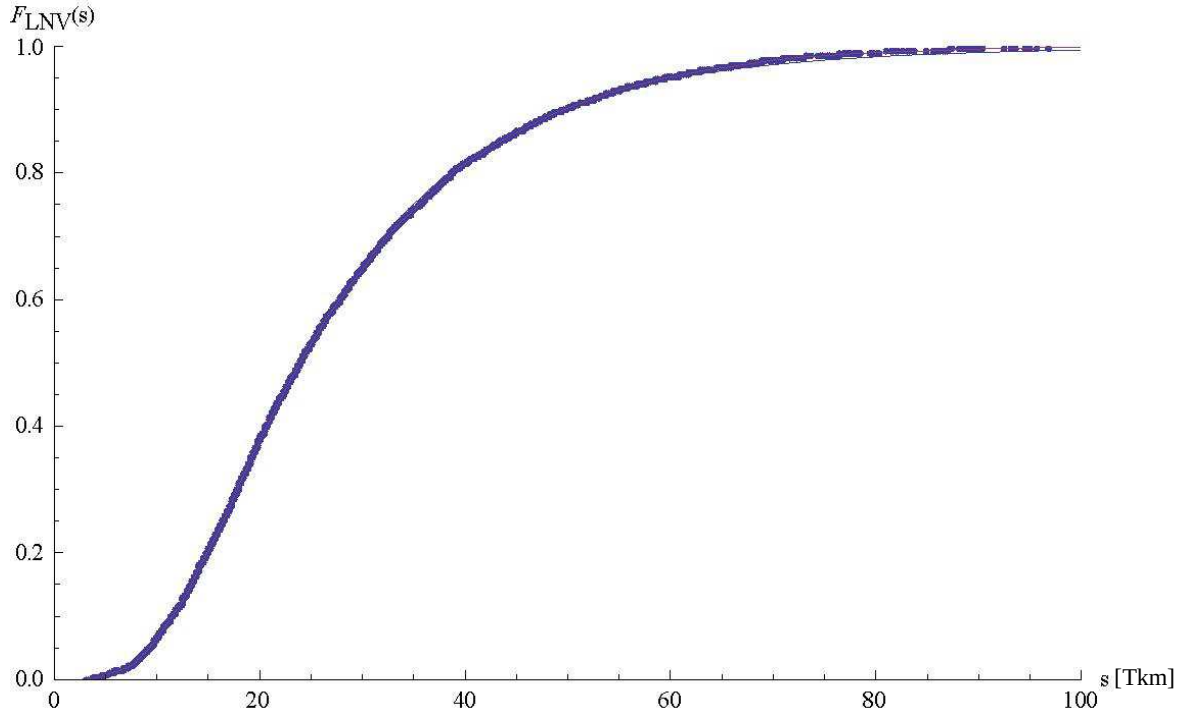


Bild A2-28: Jährliche Fahrleistungsverteilung für 07-L-d

- Parameter der Lognormal-Verteilung: $\mu = 3{,}1713$
  $\sigma = 0{,}56695$
- Erwartungswert der jährlichen FLV: $E(S) = 27{,}995\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99995$

A2.29 07-K-d

- Eingelesene Datensätze: 9.187, davon
  - 99 mit Datumsfehlern und
  - 16 mit Fahrleistungsfehlern
- Verwendete Datensätze: 9.072

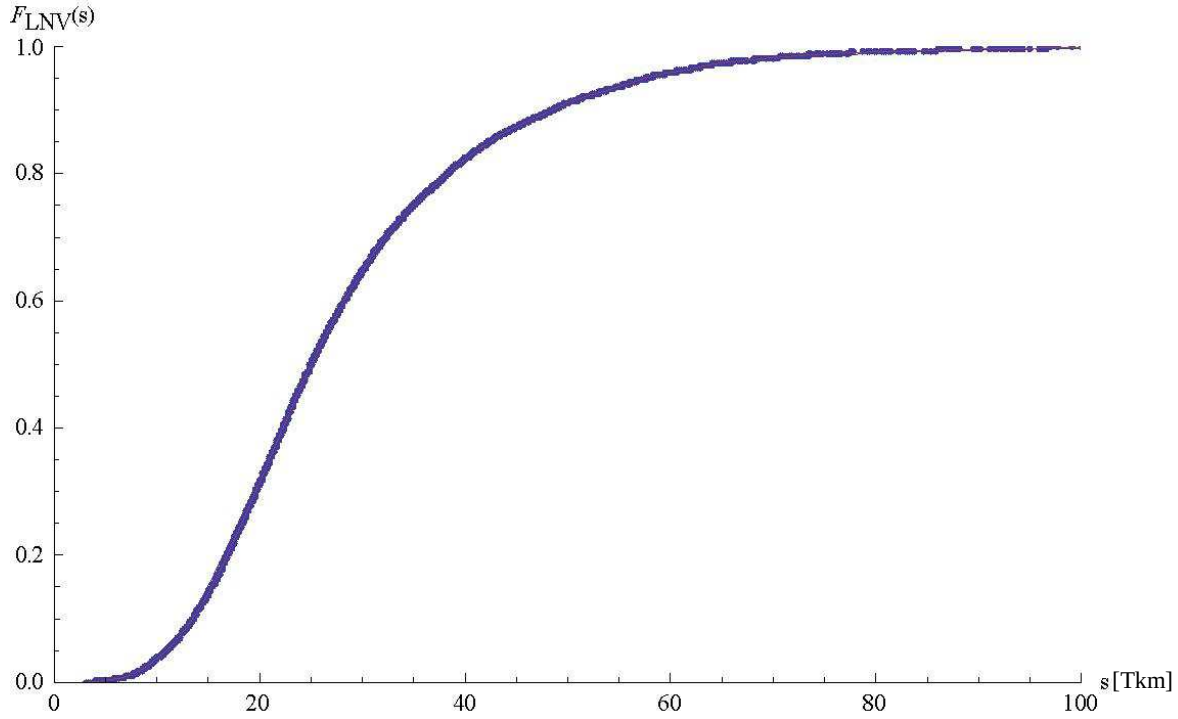


Bild A2-29: Jährliche Fahrleistungsverteilung für 07-K-d

- Parameter der Lognormal-Verteilung: $\mu = 3{,}1713$
  $\sigma = 0{,}56695$
- Erwartungswert der jährlichen FLV: $E(S) = 27{,}995\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99995$

A2.30 08-L-b

- Eingelesene Datensätze: 687, davon
  - 34 mit Datumsfehlern und
  - 10 mit Fahrleistungsfehlern
- Verwendete Datensätze: 643

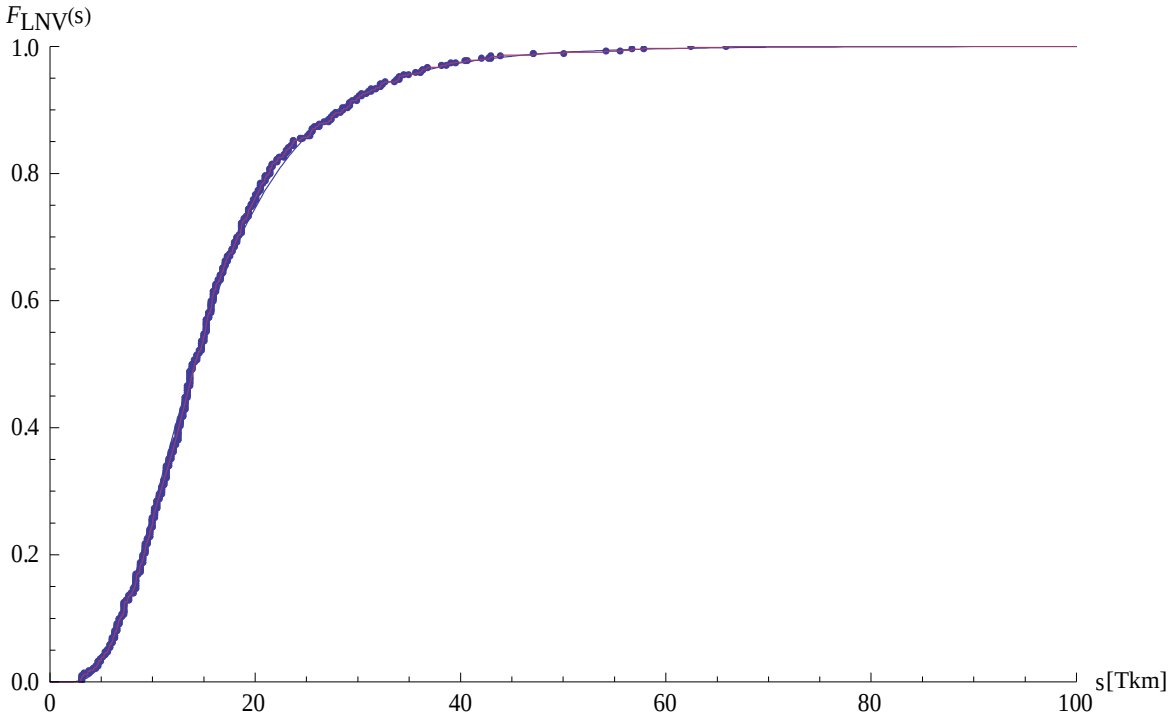


Bild A2-30: Jährliche Fahrleistungsverteilung für 08-L-b

Parameter der Lognormal-Verteilung: $\mu = 2{,}637$

$\sigma = 0{,}54166$

Erwartungswert der jährlichen FLV: $E(S) = 16{,}179\ Tkm$

Bestimmtheitsmaß: $B = 0{,}99947$

A2.31 08-K-b

- Eingelesene Datensätze: 1.140, davon
  - 71 mit Datumsfehlern und
  - 1 mit Fahrleistungsfehler
- Verwendete Datensätze: 1.068

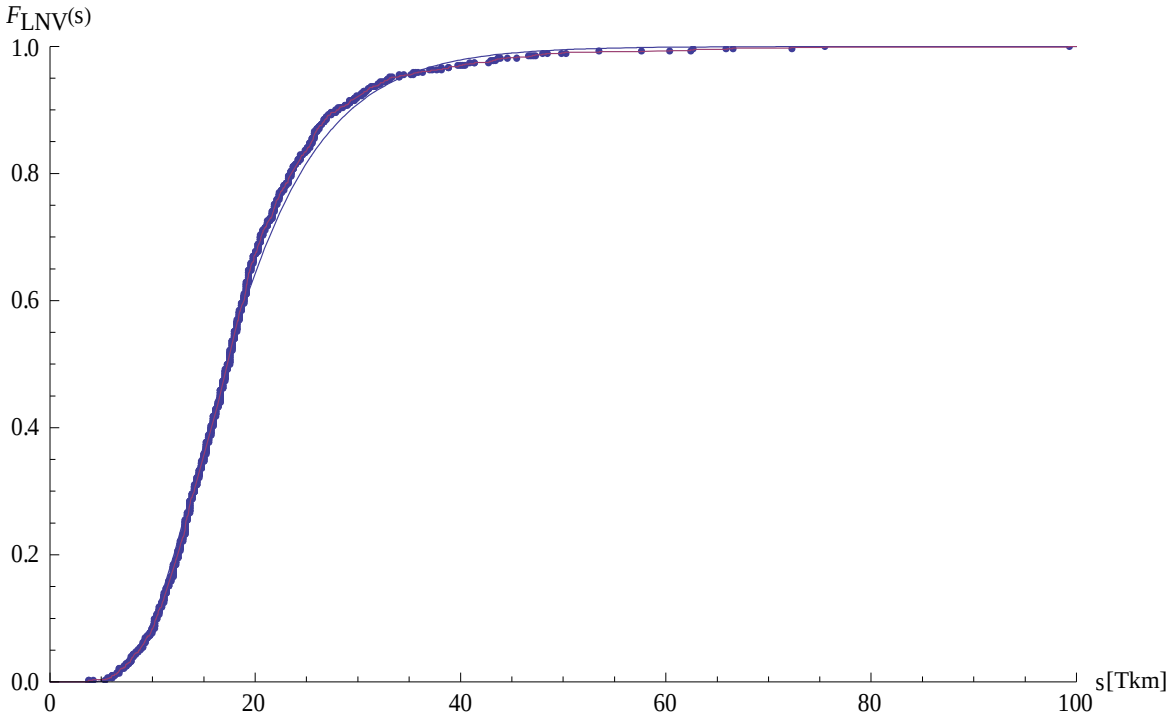


Bild A2-31: Jährliche Fahrleistungsverteilung für 08-K-b

- Parameter der Lognormal-Verteilung: $\mu = 2{,}8431$
  $\sigma = 0{,}41722$
- Erwartungswert der jährlichen FLV: $E(S) = 18{,}73\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99908$

A2.32 08-L-b/a

- Eingelesene Datensätze: 219, davon
  - 5 mit Fahrleistungsfehlern
- Verwendete Datensätze: 214

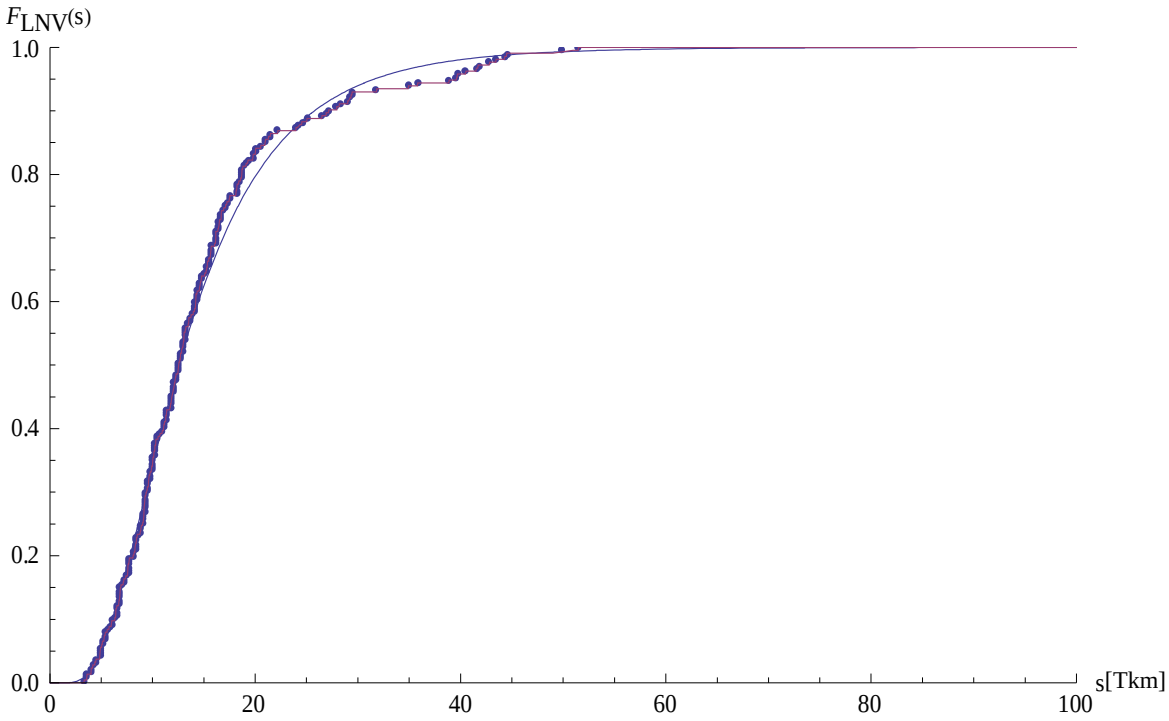


Bild A2-32: Jährliche Fahrleistungsverteilung für 08-L-b/a

- Parameter der Lognormal-Verteilung: $\mu = 2{,}5303$
  $\sigma = 0{,}56089$
- Erwartungswert der jährlichen FLV: $E(S) = 14{,}697\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99902$

A2.33 08-K-b/a

- Eingelesene Datensätze: 313, davon
  - 13 mit Datumsfehlern
- Verwendete Datensätze: 300

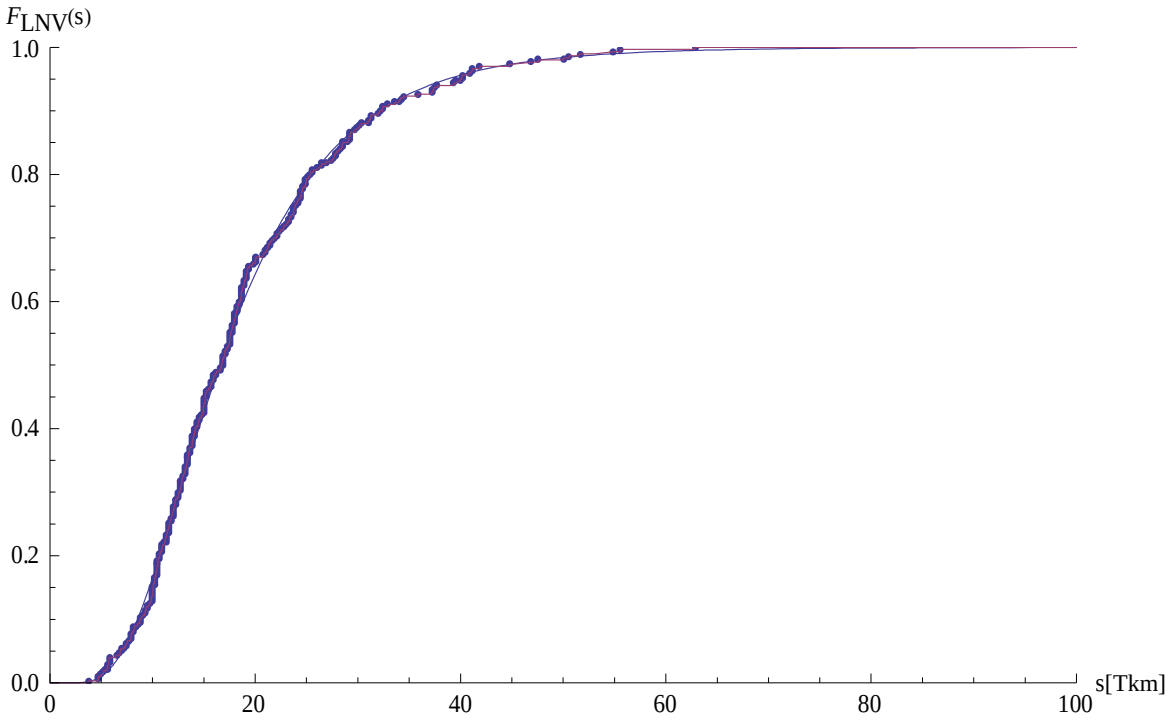


Bild A2-33: Jährliche Fahrleistungsverteilung für 08-K-b/a

- Parameter der Lognormal-Verteilung: $\mu = 2{,}8058$
  $\sigma = 0{,}51645$
- Erwartungswert der jährlichen FLV: $E(S) = 18{,}901\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99959$

A2.34 09-L-d/t

- Eingelesene Datensätze: 339, davon
  - 13 mit Datumsfehlern und
  - 5 mit Fahrleistungsfehlern
- Verwendete Datensätze: 321

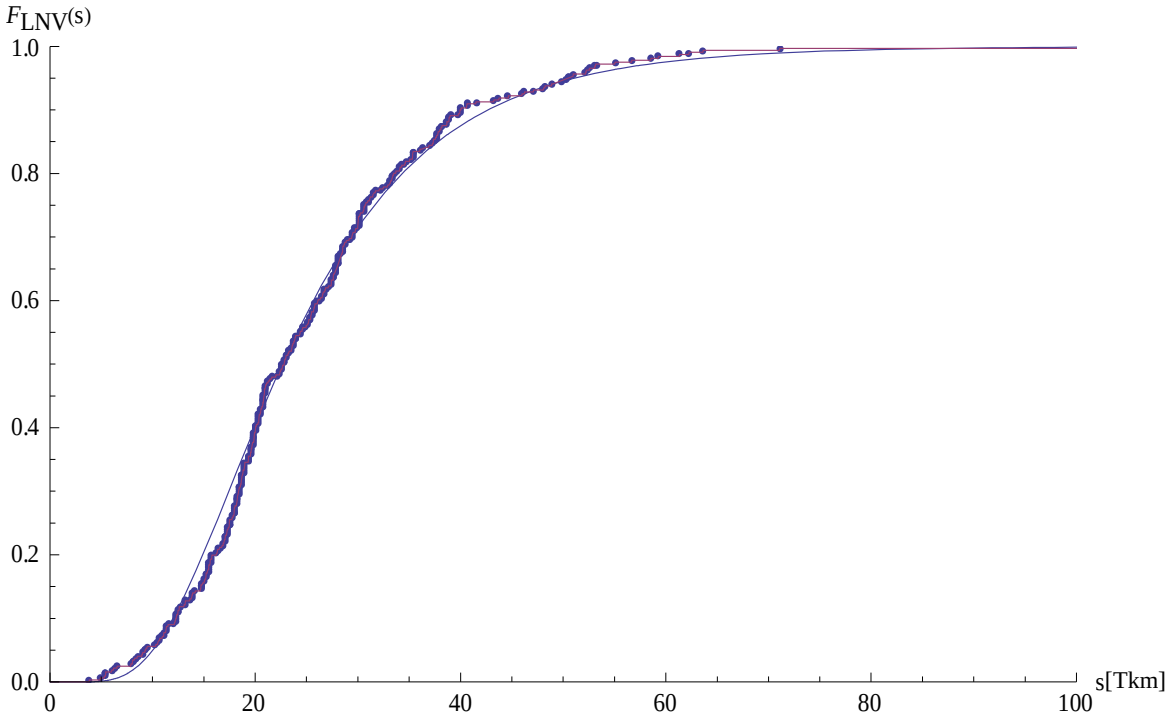


Bild A2-34: Jährliche Fahrleistungsverteilung für 09-L-d/t

- Parameter der Lognormal-Verteilung: $\mu = 3{,}1191$
  $\sigma = 0{,}49514$
- Erwartungswert der jährlichen FLV: $E(S) = 25{,}576\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99841$

A2.35 09-K-d/t

- Eingelesene Datensätze: 286, davon
  - 10 mit Datumsfehlern
- Verwendete Datensätze: 276

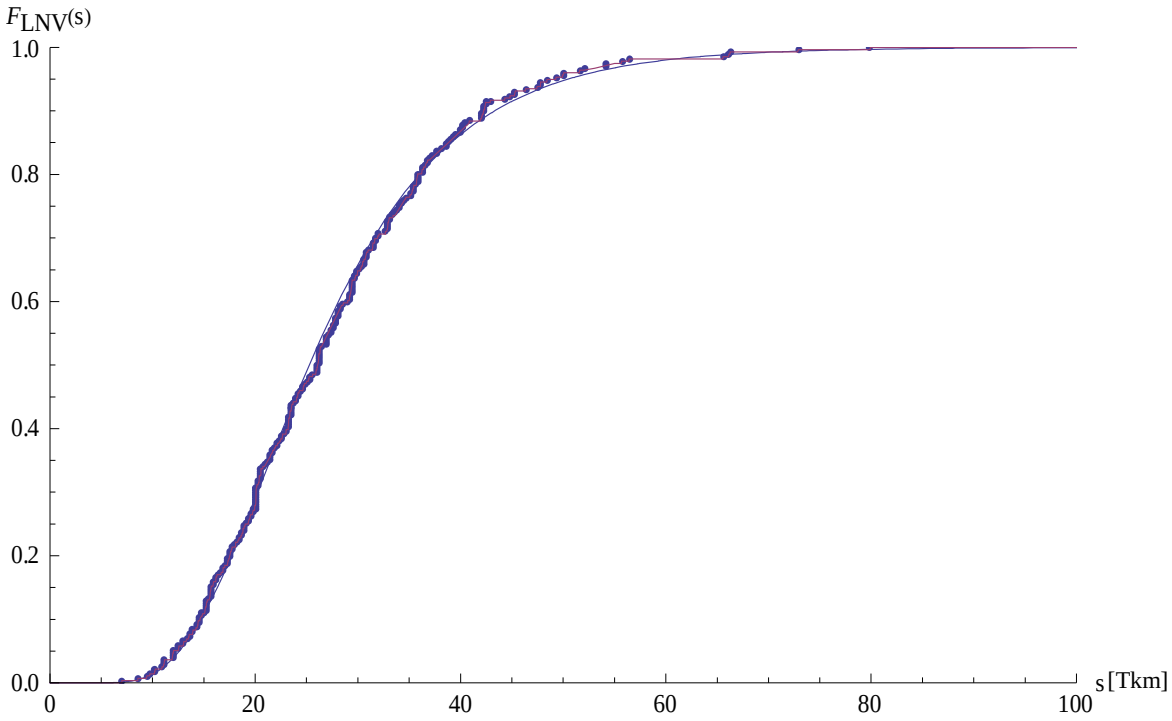


Bild A2-35: Jährliche Fahrleistungsverteilung für 09-K-d/t

- Parameter der Lognormal-Verteilung: $\mu = 3{,}2286$
  $\sigma = 0{,}42146$
- Erwartungswert der jährlichen FLV: $E(S) = 27{,}588\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99953$

A2.36 10-L-b

- Eingelesene Datensätze: 1.872, davon
  - 51 mit Datumsfehlern und
  - 18 mit Fahrleistungsfehlern
- Verwendete Datensätze: 1.803

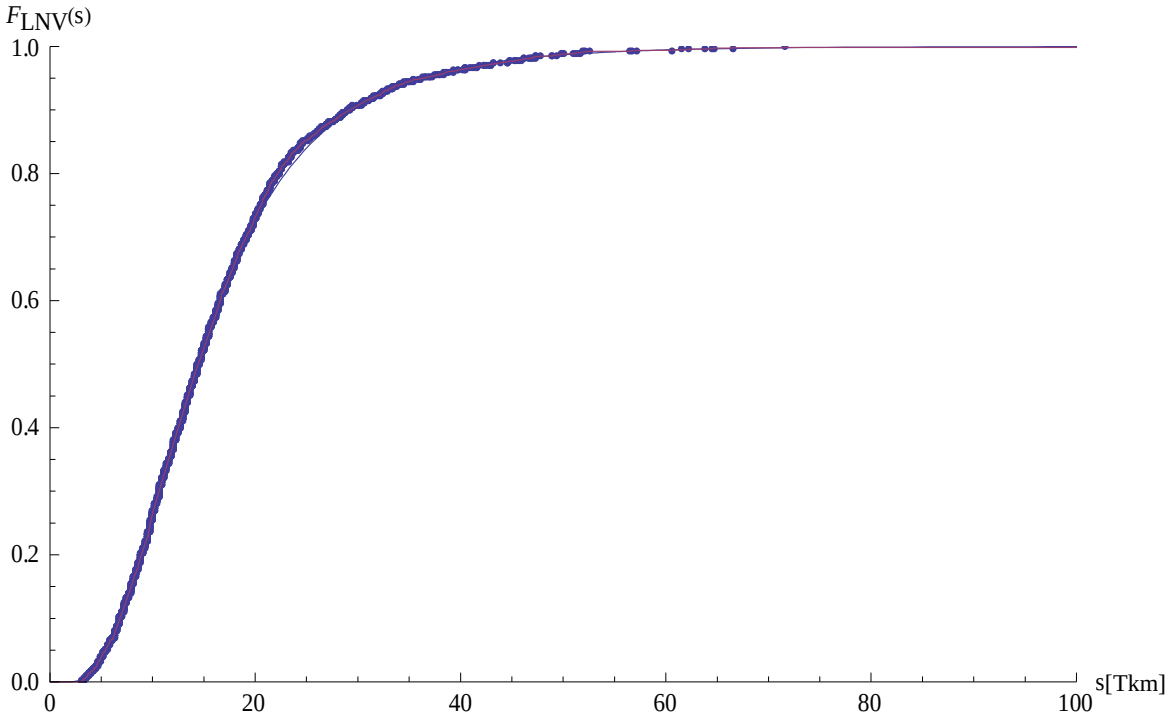


Bild A2-36: Jährliche Fahrleistungsverteilung für 10-L-b

- Parameter der Lognormal-Verteilung: $\mu = 2{,}656$
  $\sigma = 0{,}56638$
- Erwartungswert der jährlichen FLV: $E(S) = 16{,}717\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}9998$

A2.37 10-K-b

- Eingelesene Datensätze: 811, davon
  - 23 mit Datumsfehlern
- Verwendete Datensätze: 788

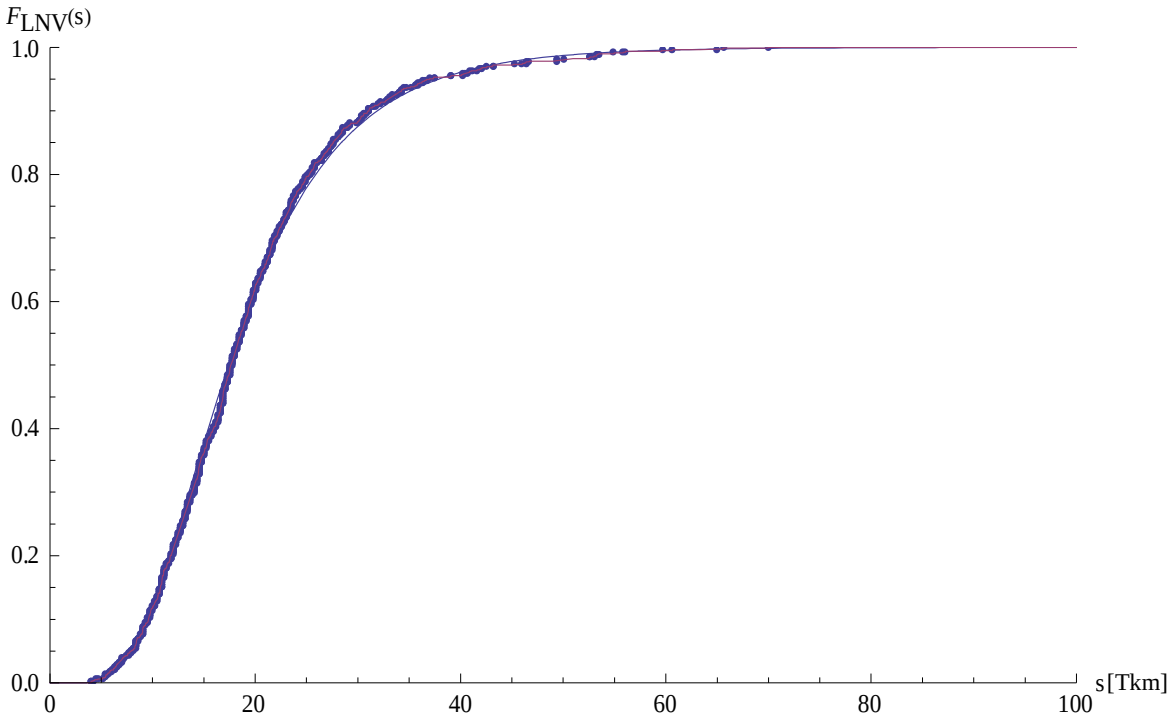


Bild A2-37: Jährliche Fahrleistungsverteilung für 10-K-b

- Parameter der Lognormal-Verteilung: $\mu = 2{,}8556$
  $\sigma = 0{,}47343$
- Erwartungswert der jährlichen FLV: $E(S) = 19{,}446\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}9995$

A2.38 10-L-b/a

- Eingelesene Datensätze: 378, davon
  - 6 mit Datumsfehlern und
  - 9 mit Fahrleistungsfehlern
- Verwendete Datensätze: 363

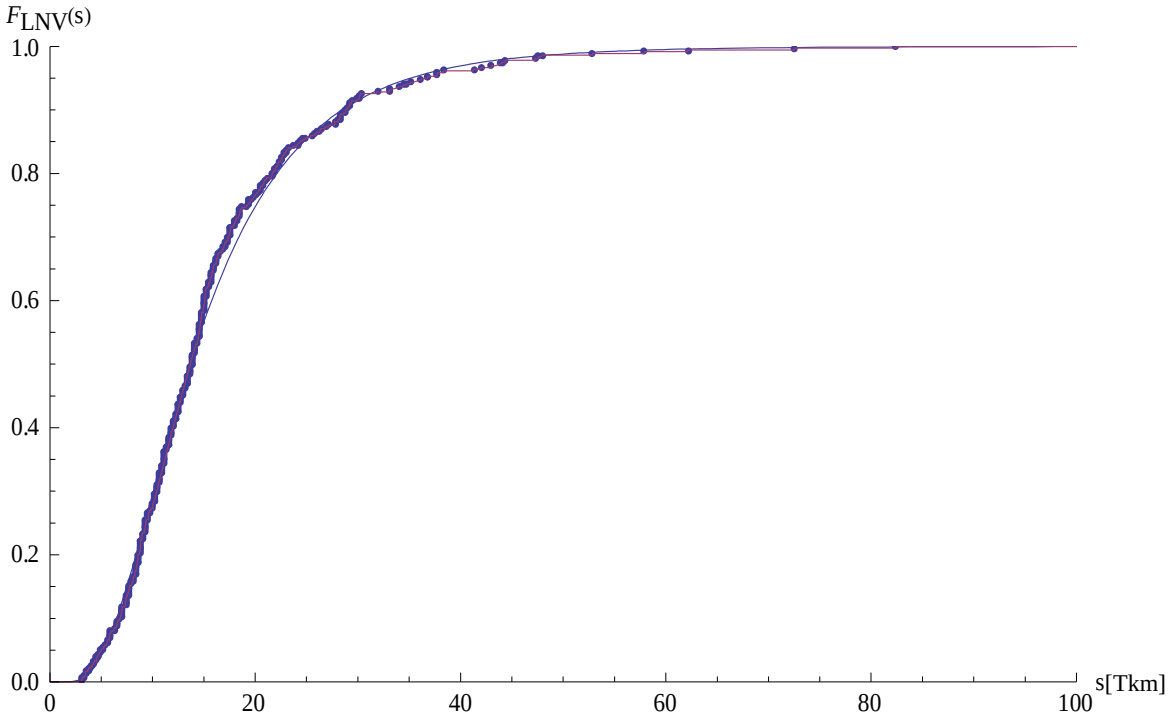


Bild A2-38: Jährliche Fahrleistungsverteilung für 10-L-b/a

- Parameter der Lognormal-Verteilung: $\mu = 2{,}6114$
  $\sigma = 0{,}57551$
- Erwartungswert der jährlichen FLV: $E(S) = 16{,}071\,Tkm$
- Bestimmtheitsmaß: $B = 0{,}99902$

A2.39 10-K-b/a

- Eingelesene Datensätze: 354, davon
  - 5 mit Datumsfehlern und
  - 1 mit Fahrleistungsfehler
- Verwendete Datensätze: 348

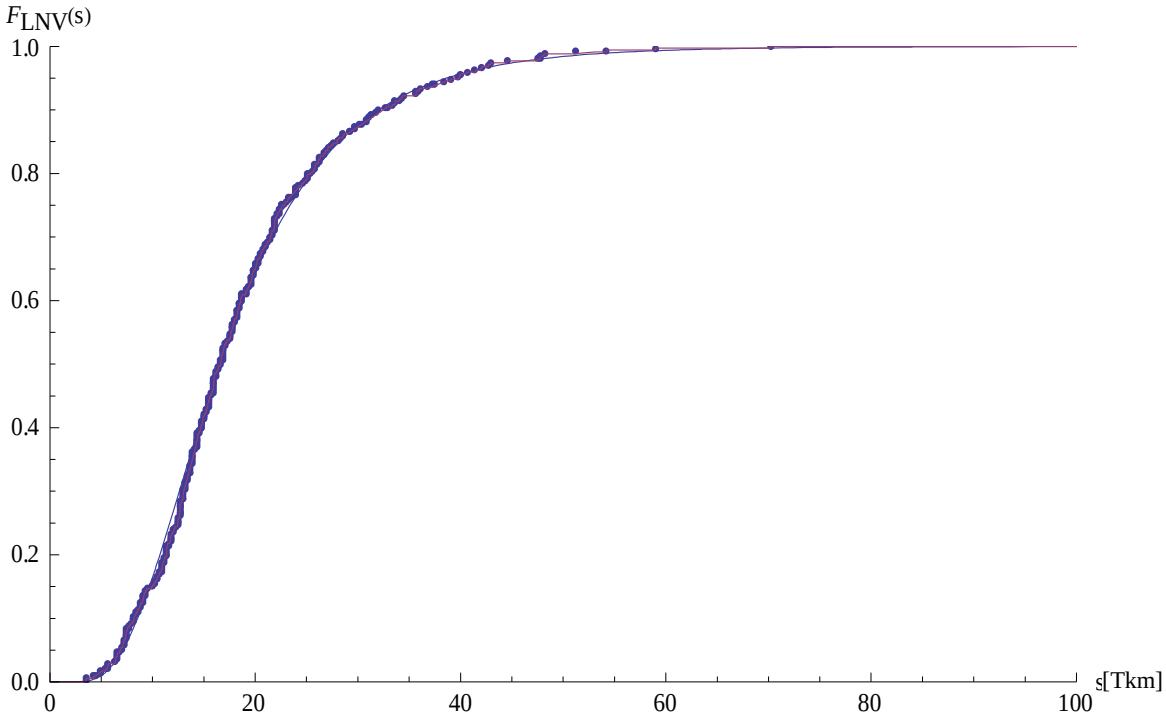


Bild A2-39: Jährliche Fahrleistungsverteilung für 10-K-b/a

- Parameter der Lognormal-Verteilung: $\mu = 2{,}8054$
  $\sigma = 0{,}51531$
- Erwartungswert der jährlichen FLV: $E(S) = 18{,}881\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99939$

A2.40 10-L-b/m/t

- Eingelesene Datensätze: 346, davon
  - 17 mit Datumsfehlern und
  - 2 mit Fahrleistungsfehlern
- Verwendete Datensätze: 327

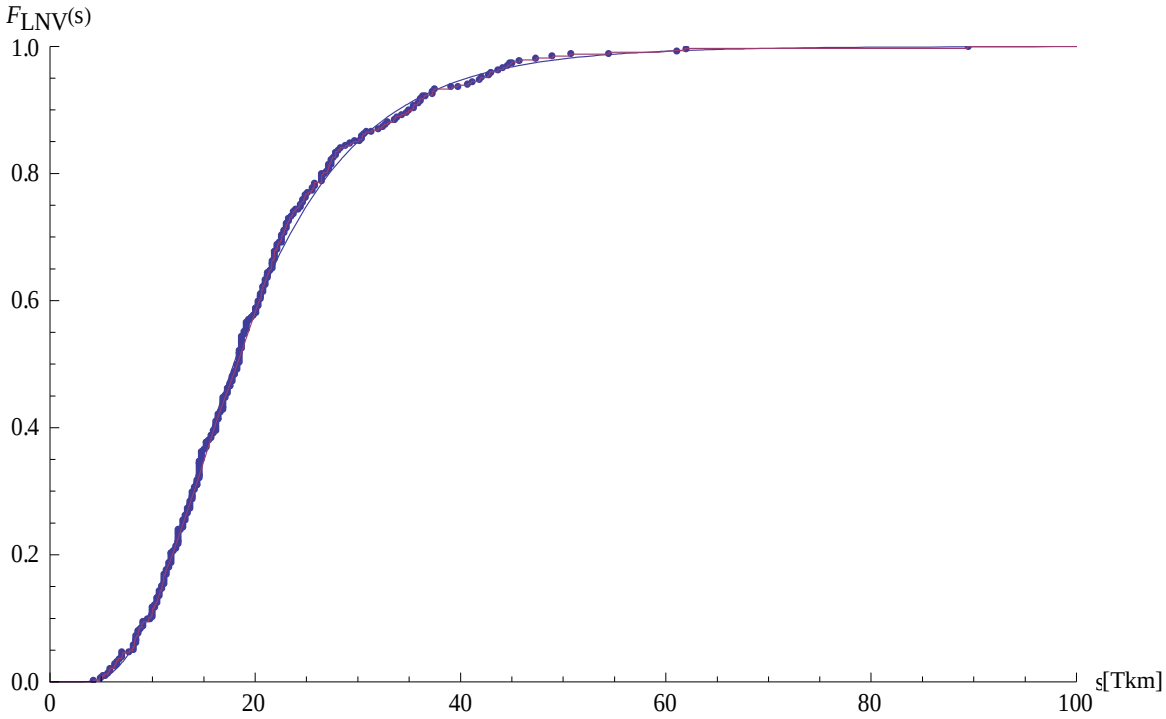


Bild A2-40: Jährliche Fahrleistungsverteilung für 10-L-b/m/t

- Parameter der Lognormal-Verteilung: $\mu = 2{,}8846$
  $\sigma = 0{,}49848$
- Erwartungswert der jährlichen FLV: $E(S) = 20{,}265\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99961$

A2.41 10-K-b/m/t

- Eingelesene Datensätze: 425, davon
  - 17 mit Datumsfehlern und
  - 2 mit Fahrleistungsfehlern
- Verwendete Datensätze: 406

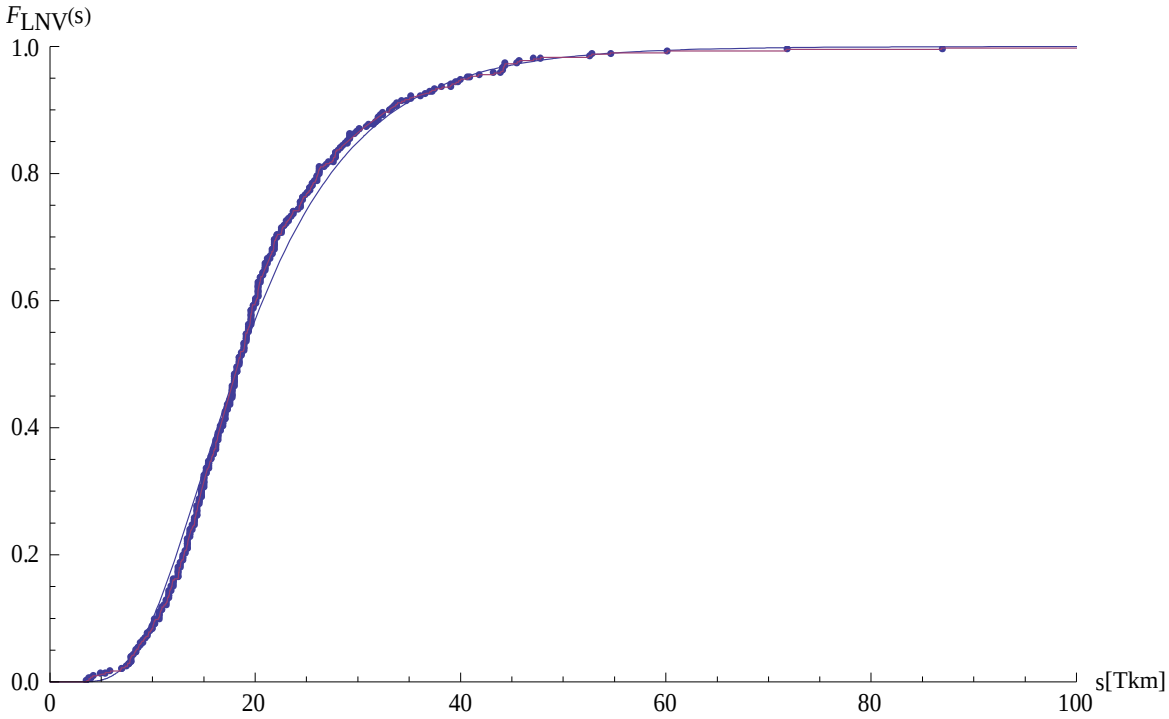


Bild A2-41: Jährliche Fahrleistungsverteilung für 10-K-b/m/t

- Parameter der Lognormal-Verteilung: $\mu = 2{,}911$
  $\sigma = 0{,}47358$
- Erwartungswert der jährlichen FLV: $E(S) = 20{,}556\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99841$

A2.42 10-L-d

- Eingelesene Datensätze: 1.549, davon
  - 101 mit Datumsfehlern und
  - 1 mit Fahrleistungsfehler
- Verwendete Datensätze: 1.447

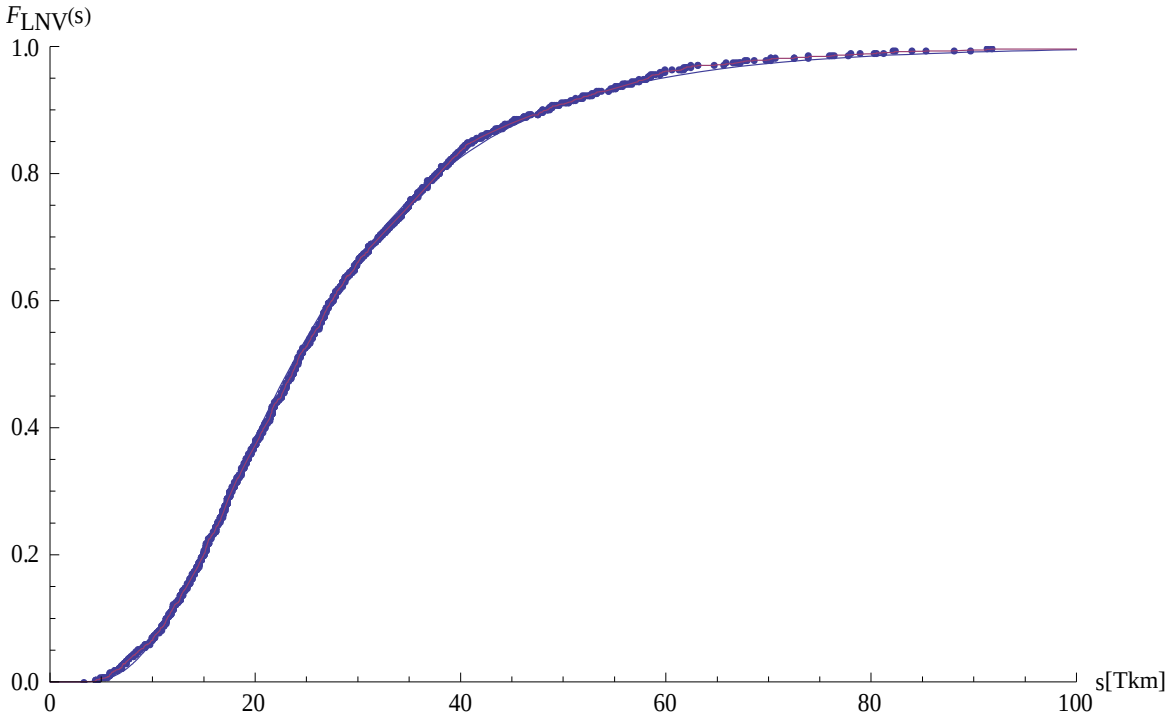


Bild A2-42: Jährliche Fahrleistungsverteilung für 10-L-d

- Parameter der Lognormal-Verteilung: $\mu = 3{,}1598$
  $\sigma = 0{,}564511$
- Erwartungswert der jährlichen FLV: $E(S) = 27{,}636\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99979$

A2.43 10-K-d

- Eingelesene Datensätze: 2.939, davon
  - 133 mit Datumsfehlern und
  - 2 mit Fahrleistungsfehlern
- Verwendete Datensätze: 2.804

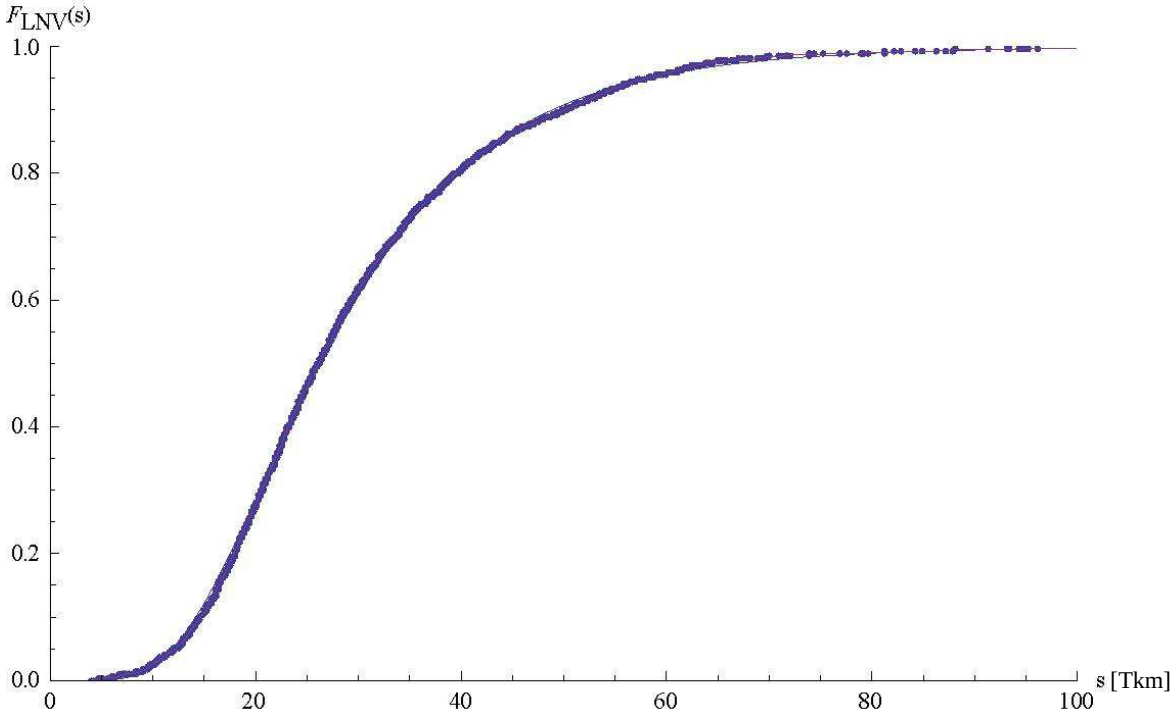


Bild A2-43: Jährliche Fahrleistungsverteilung für 10-K-d

- Parameter der Lognormal-Verteilung: $\mu = 3{,}2706$
  $\sigma = 0{,}48242$
- Erwartungswert der jährlichen FLV: $E(S) = 29{,}577\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99981$

A2.44 11-C-b

- Eingelesene Datensätze: 519, davon
  - 17 mit Datumsfehlern und
  - 21 mit Fahrleistungsfehlern
- Verwendete Datensätze: 481

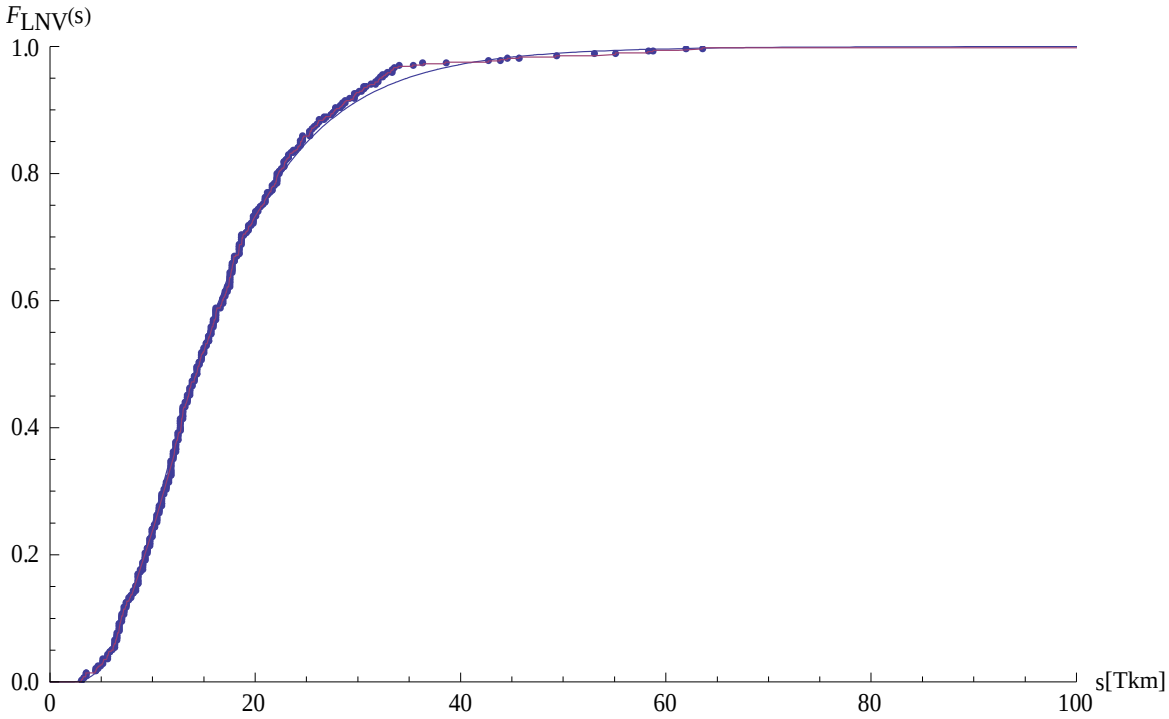


Bild A2-44: Jährliche Fahrleistungsverteilung für 11-C-b

- Parameter der Lognormal-Verteilung: $\mu = 2{,}6654$
  $\sigma = 0{,}53732$
- Erwartungswert der jährlichen FLV: $E(S) = 16{,}606\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99965$

A2.45 11-L-b

- Eingelesene Datensätze: 246, davon
  - 21 mit Datumsfehlern und
  - 2 mit Fahrleistungsfehlern
- Verwendete Datensätze: 223

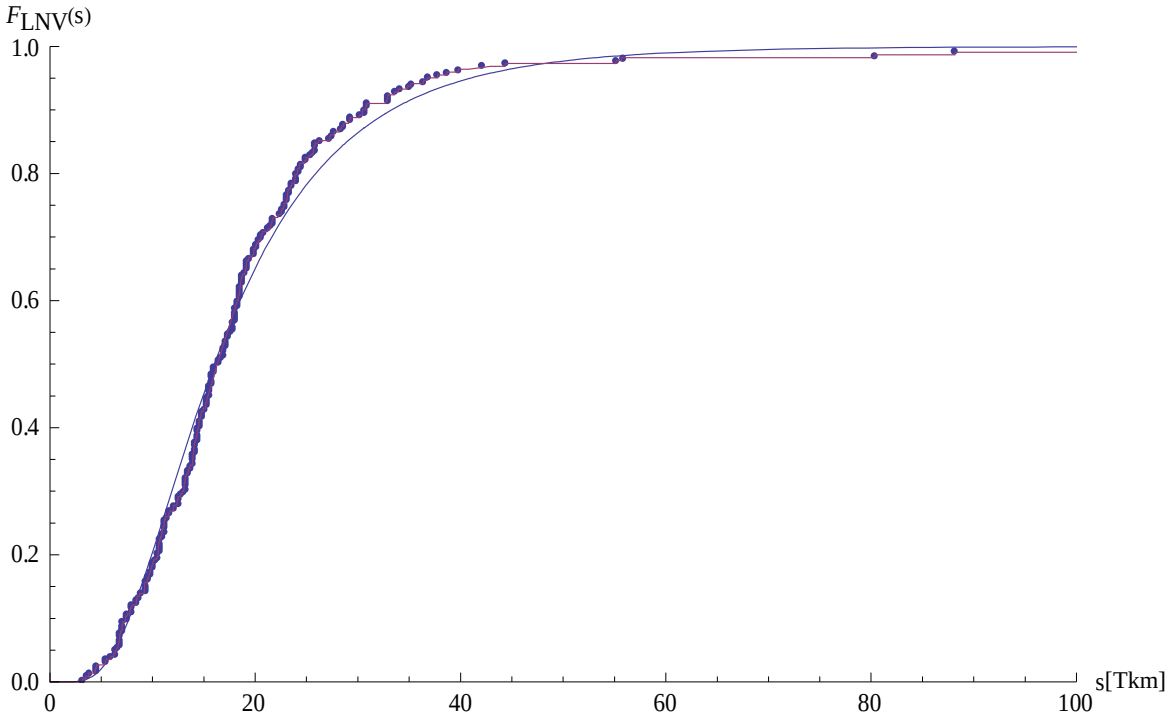


Bild A2-45: Jährliche Fahrleistungsverteilung für 11-L-b

- Parameter der Lognormal-Verteilung: $\mu = 2{,}7738$
  $\sigma = 0{,}57062$
- Erwartungswert der jährlichen FLV: $E(S) = 18{,}851\,Tkm$
- Bestimmtheitsmaß: $B = 0{,}99811$

A2.46 11-K-b

- Eingelesene Datensätze: 302, davon
  - 23 mit Datumsfehlern und
  - 1 mit Fahrleistungsfehler
- Verwendete Datensätze: 278

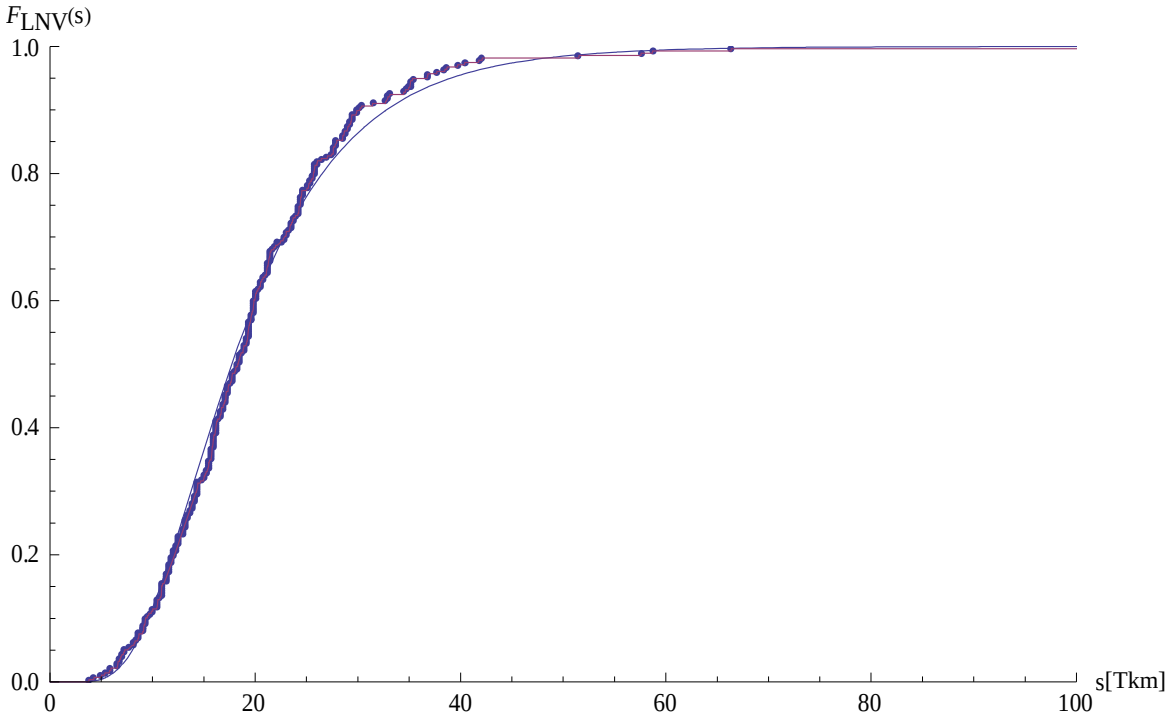


Bild A2-46: Jährliche Fahrleistungsverteilung für 11-K-b

- Parameter der Lognormal-Verteilung: $\mu = 2{,}8744$
  $\sigma = 0{,}48025$
- Erwartungswert der jährlichen FLV: $E(S) = 19{,}88\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99875$

A2.47 11-L-b/a

- Eingelesene Datensätze: 45, davon
  - 2 mit Datumsfehlern und
  - 1 mit Fahrleistungsfehler
- Verwendete Datensätze: 42

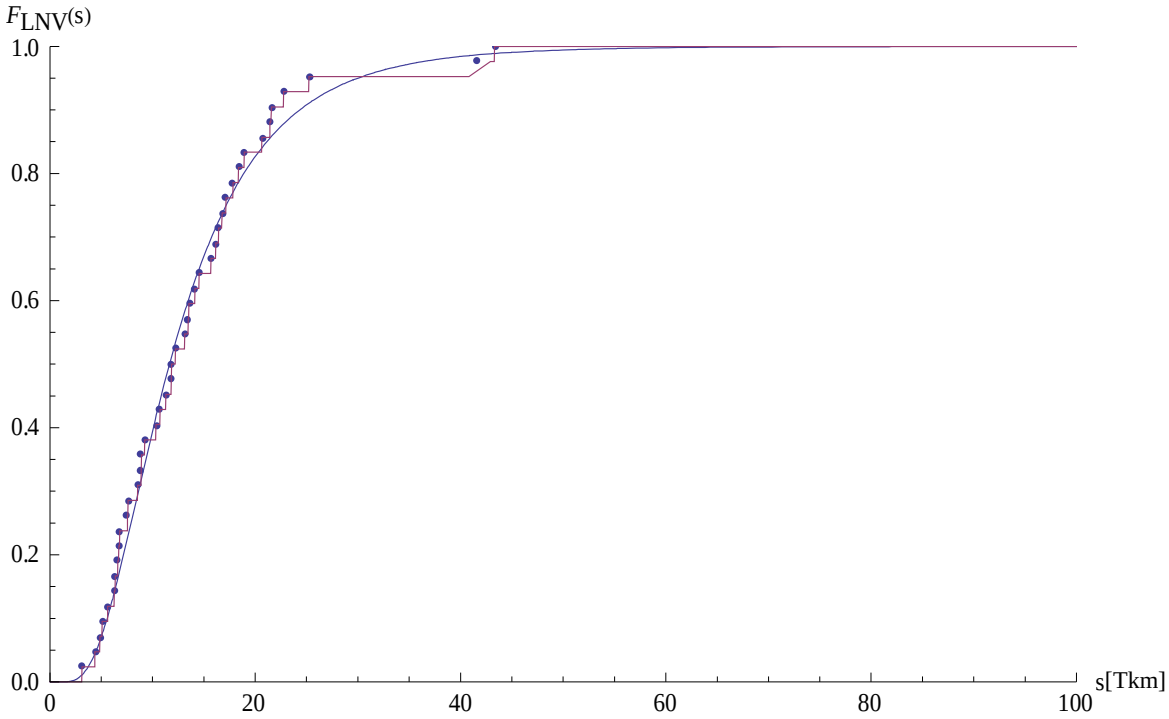


Bild A2-47: Jährliche Fahrleistungsverteilung für 11-L-b/a

- Parameter der Lognormal-Verteilung: $\mu = 2{,}4557$
  $\sigma = 0{,}57445$
- Erwartungswert der jährlichen FLV: $E(S) = 13{,}745\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99789$

A2.48 11-K-b/a

- Eingelesene Datensätze: 117, davon
  - 5 mit Datumsfehlern
- Verwendete Datensätze: 112

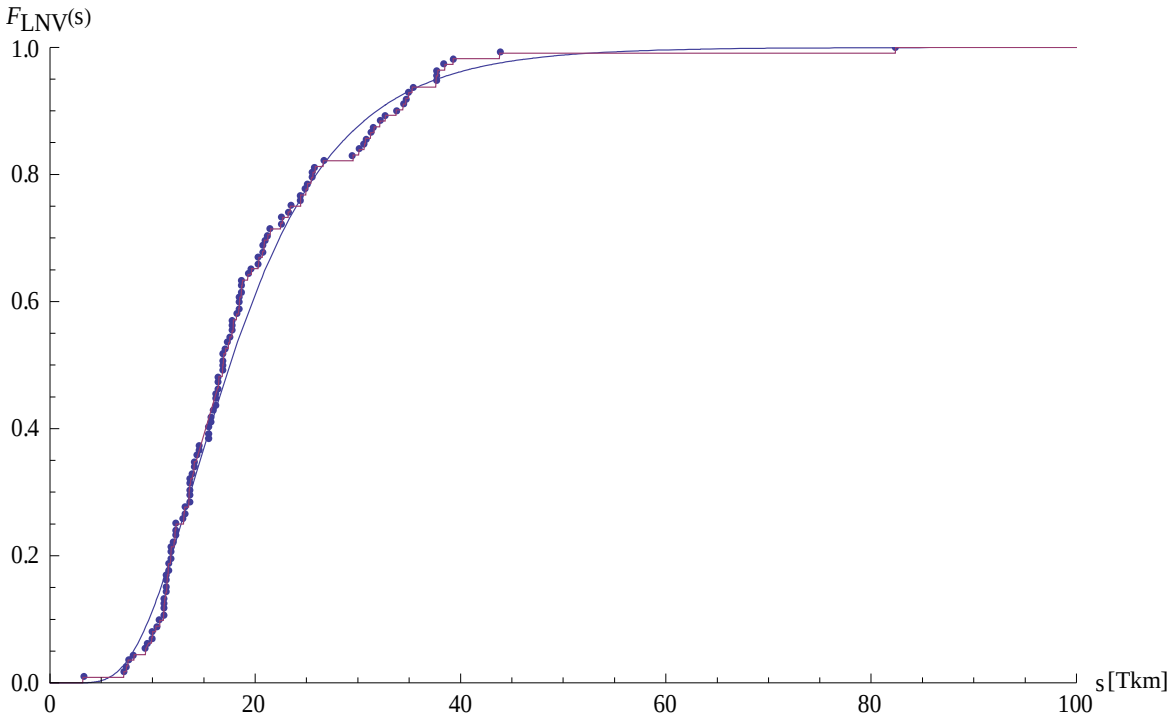


Bild A2-48: Jährliche Fahrleistungsverteilung für 11-K-b/a

- Parameter der Lognormal-Verteilung: $\mu = 2{,}8638$
  $\sigma = 0{,}46584$
- Erwartungswert der jährlichen FLV: $E(S) = 19{,}536\ Tkm$
- Bestimmtheitsmaß: $B = 0{,}99757$

A2.49 12-L-b/t

- Eingelesene Datensätze: 462, davon
  - 65 mit Datumsfehlern und
  - 2 mit Fahrleistungsfehlern
- Verwendete Datensätze: 395

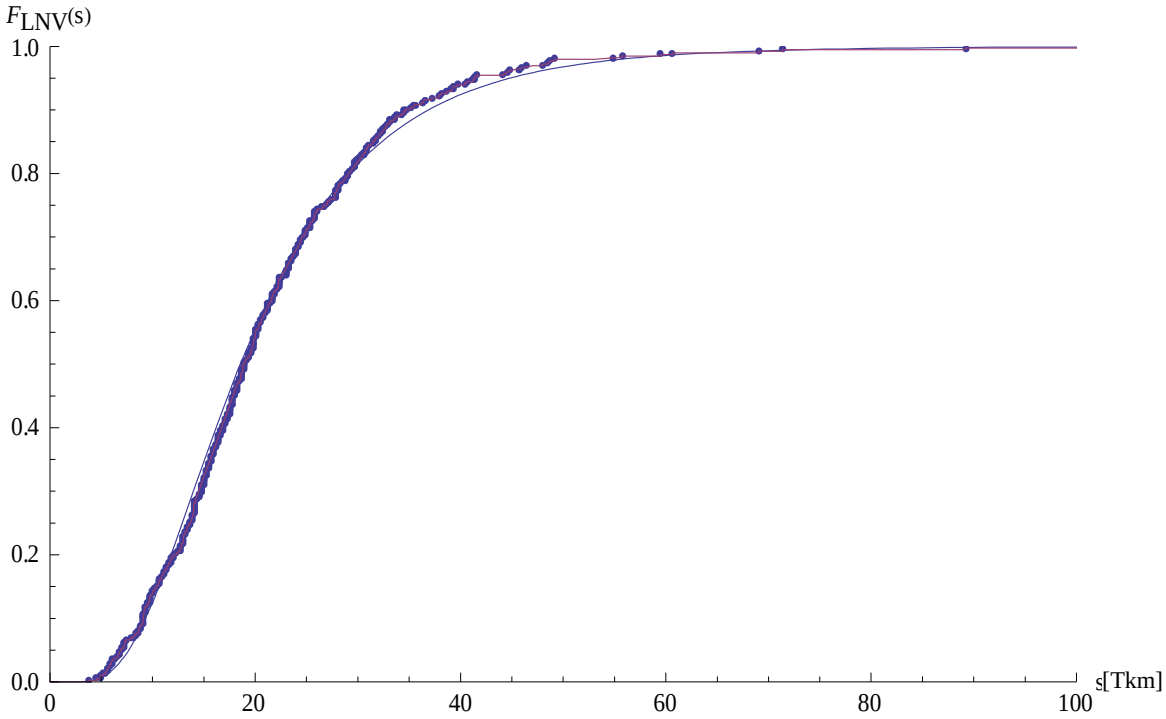


Bild A2-49: Jährliche Fahrleistungsverteilung für 12-L-b/t

- Parameter der Lognormal-Verteilung: $\mu = 2{,}9201$
  $\sigma = 0{,}53631$
- Erwartungswert der jährlichen FLV: $E(S) = 21{,}411\,Tkm$
- Bestimmtheitsmaß: $B = 0{,}99909$

A2.50 Cluster Limousinen mit Allradantrieb (L-a)

- Parameter der Lognormal-Verteilung: $\mu = 2{,}5594$

  $\sigma = 0{,}56203$

- Erwartungswert der jährlichen FLV: $E(S) = 15{,}14\ Tkm$

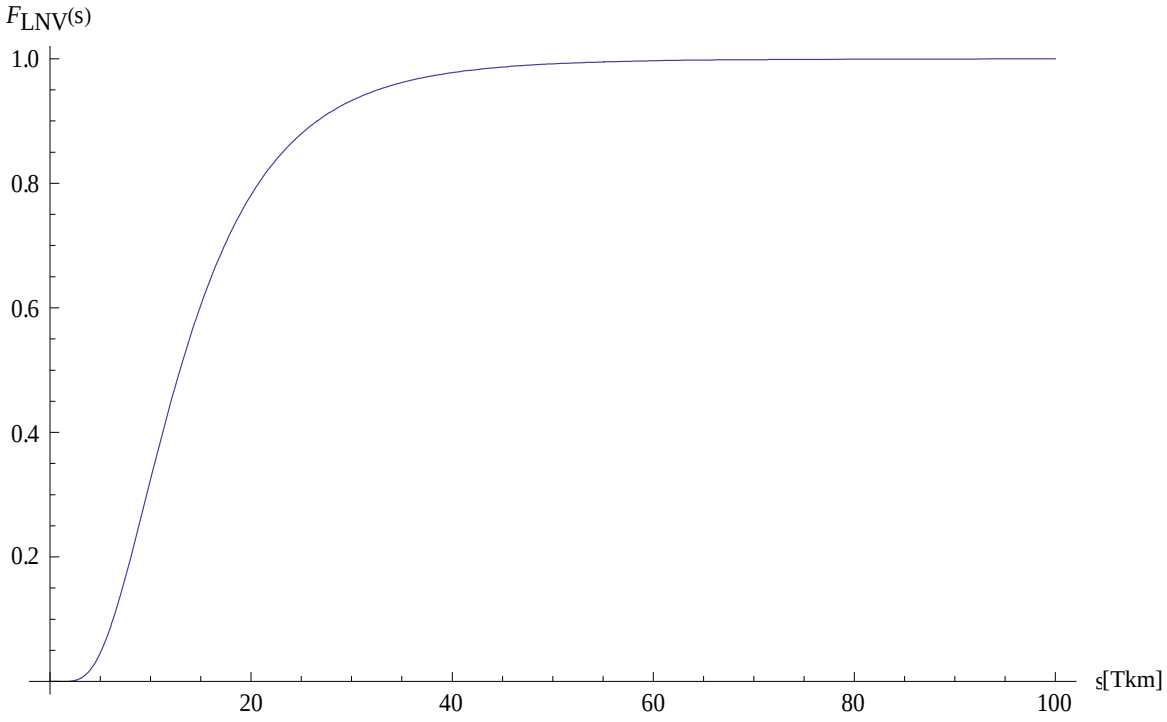


Bild A2-50: Jährliche Fahrleistungsverteilung für Cluster L-a

A2.51 Cluster Kombifahrzeuge mit Allradantrieb (K-a)

- Parameter der Lognormal-Verteilung: $\mu = 2{,}7837$

  $\sigma = 0{,}50861$

- Erwartungswert der jährlichen FLV: $E(S) = 18{,}41\ Tkm$

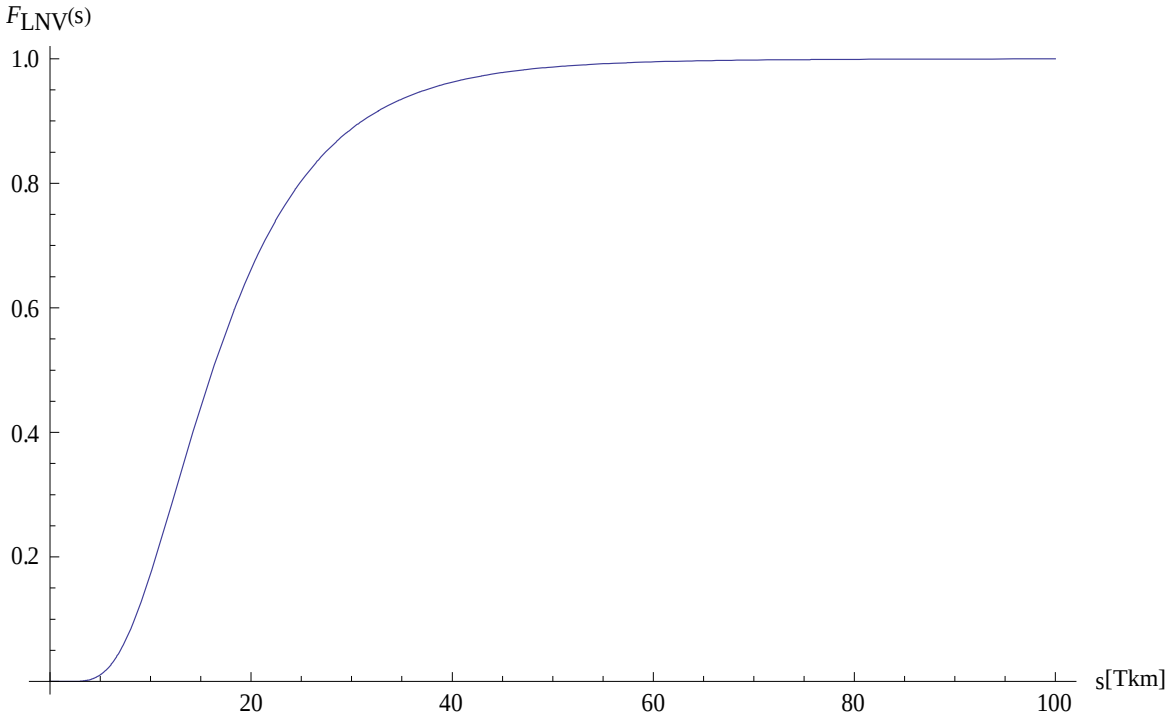


Bild A2-51: Jährliche Fahrleistungsverteilung für Cluster K-a

A2.52 Cluster Fahrzeuge mit Allradantrieb gesamt (a)

- Parameter der Lognormal-Verteilung: $\mu = 2{,}6779$

  $\sigma = 0{,}54597$

- Erwartungswert der jährlichen FLV: $E(S) = 16{,}89\ Tkm$

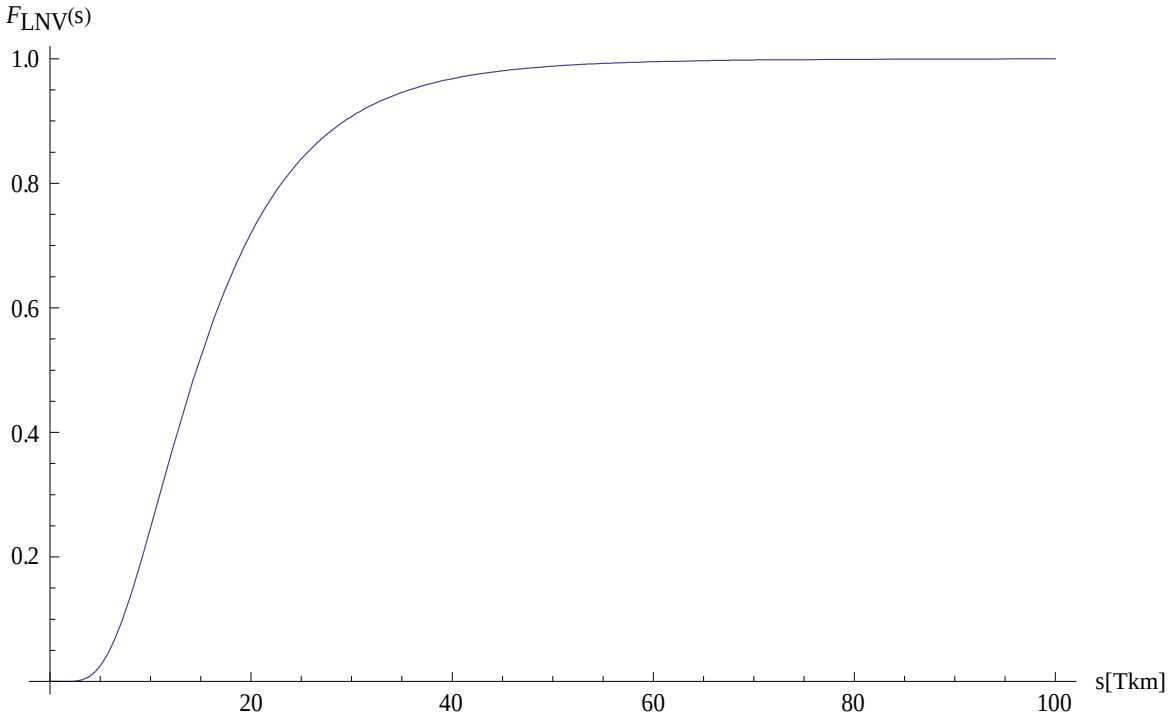


Bild A2-52: Jährliche Fahrleistungsverteilung für Cluster a

A2.53 Cluster Tuningfahrzeuge (t)

- Parameter der Lognormal-Verteilung: $\mu = 2{,}9975$

  $\sigma = 0{,}50664$

- Erwartungswert der jährlichen FLV: $E(S) = 22{,}78\ Tkm$

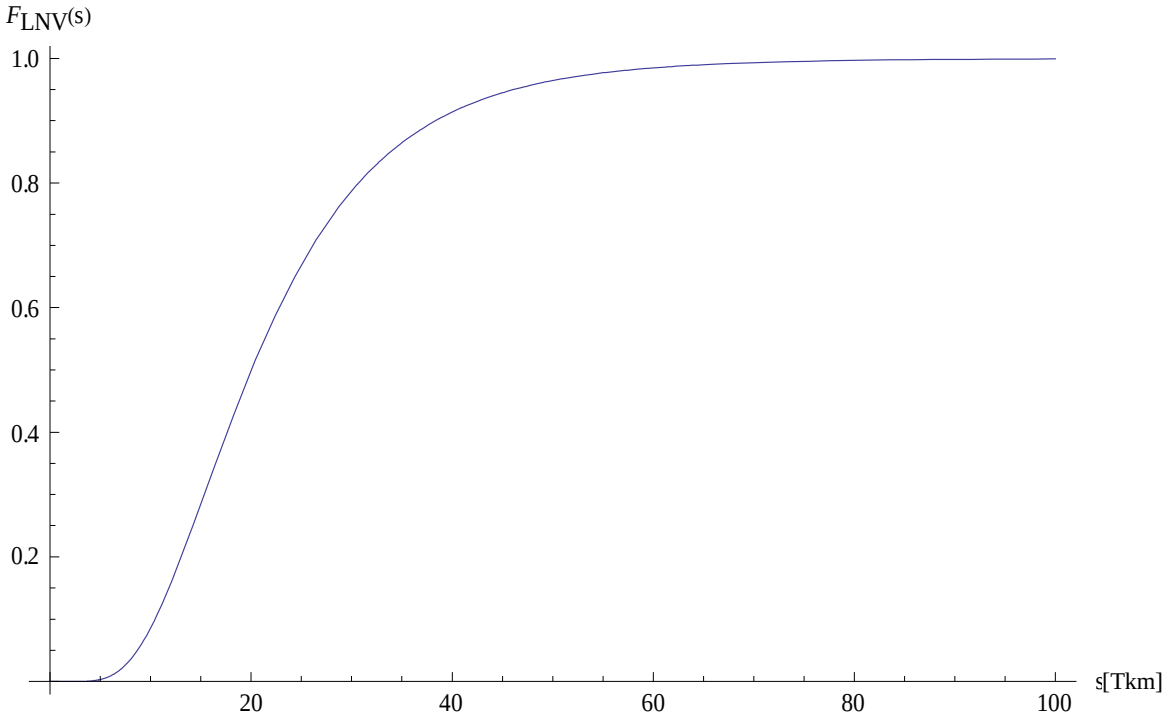


Bild A2-53: Jährliche Fahrleistungsverteilung für Cluster t

A2.54 Cluster Limousinen mit Dieselmotor (L-d)

- Parameter der Lognormal-Verteilung: $\mu = 2{,}9946$

  $\sigma = 0{,}61976$

- Erwartungswert der jährlichen FLV: $E(S) = 24{,}21\ Tkm$

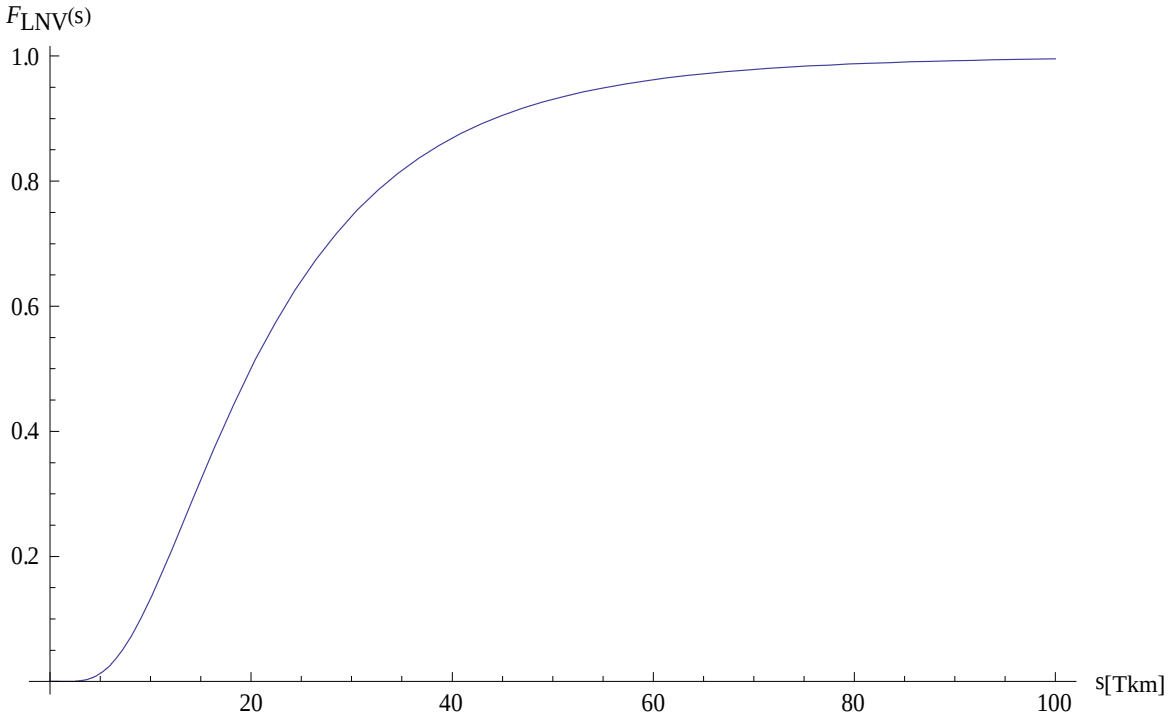


Bild A2-54: Jährliche Fahrleistungsverteilung für Cluster L-d

A2.55 Cluster Kombifahrzeuge mit Dieselmotor (K-d)

- Parameter der Lognormal-Verteilung: $\mu = 3{,}2486$

  $\sigma = 0{,}57910$
- Erwartungswert der jährlichen FLV: $E(S) = 30{,}46\ Tkm$

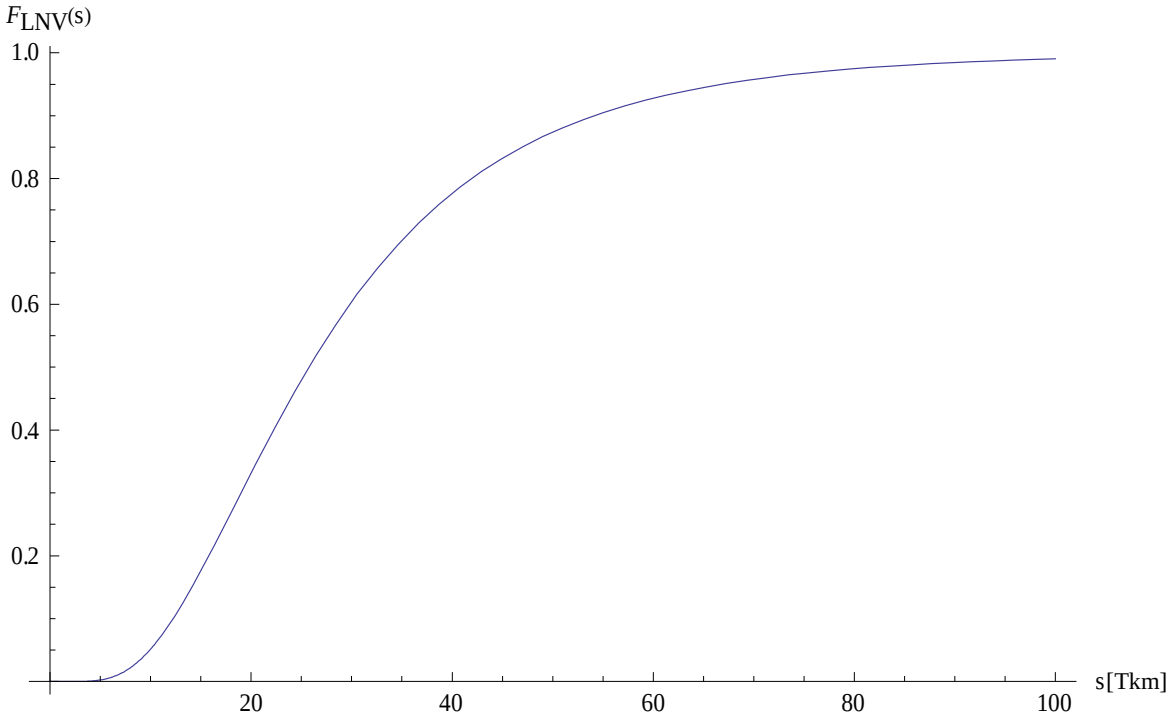


Bild A2-55: Jährliche Fahrleistungsverteilung für Cluster K-d

A2.56 Cluster Fahrzeuge mit Dieselmotor gesamt (d)

- Parameter der Lognormal-Verteilung: $\mu = 3{,}1149$

  $\sigma = 0{,}61413$

- Erwartungswert der jährlichen FLV: $E(S) = 27{,}21\ Tkm$

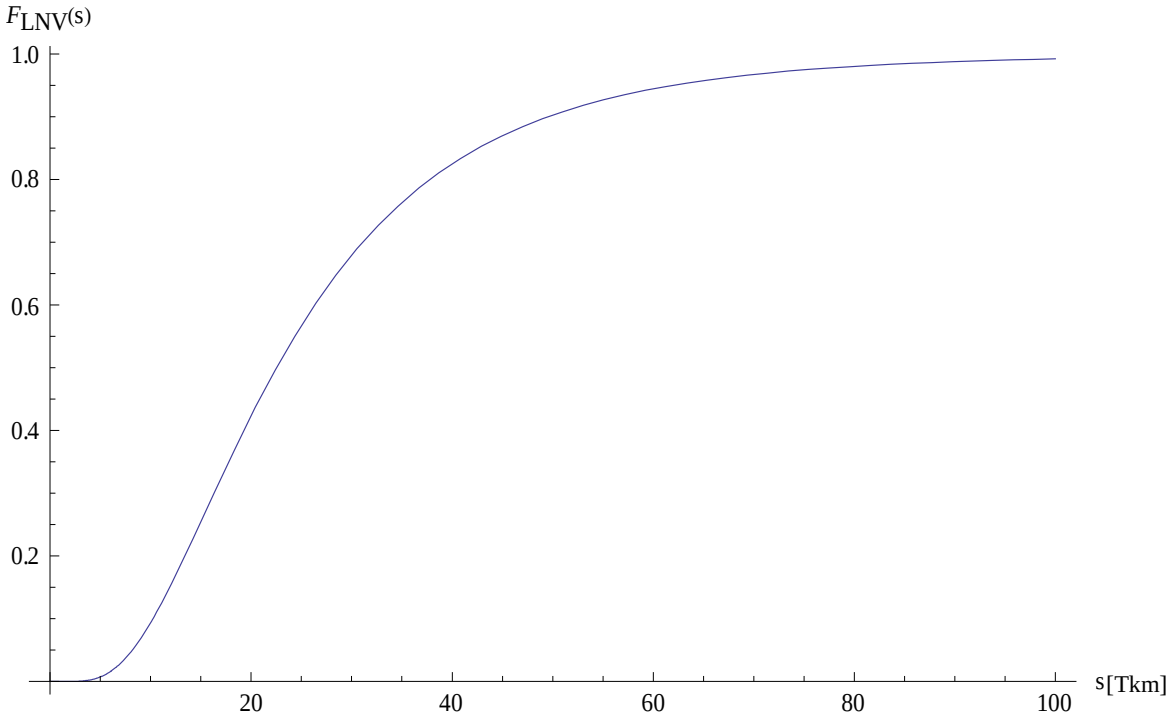


Bild A2-56: Jährliche Fahrleistungsverteilung für Cluster d

A2.57 Cluster Limousinen mit Motoraufladung (L-m)

- Parameter der Lognormal-Verteilung: $\mu = 2{,}4819$

  $\sigma = 0{,}522246$

- Erwartungswert der jährlichen FLV: $E(S) = 13{,}71\ Tkm$

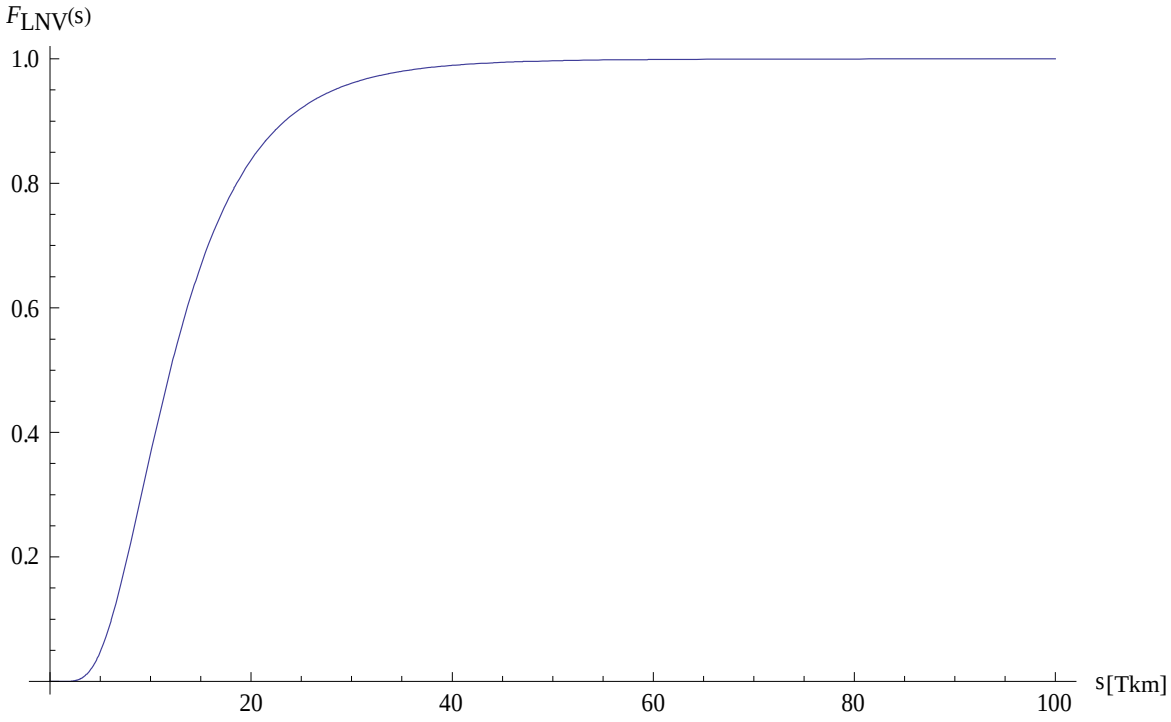


Bild A2-57: Jährliche Fahrleistungsverteilung für Cluster L-m

A2.58 Cluster Kombifahrzeuge mit Motoraufladung (K-m)

- Parameter der Lognormal-Verteilung: $\mu = 2{,}7340$

  $\sigma = 0{,}49626$

- Erwartungswert der jährlichen FLV: $E(S) = 17{,}41\ Tkm$

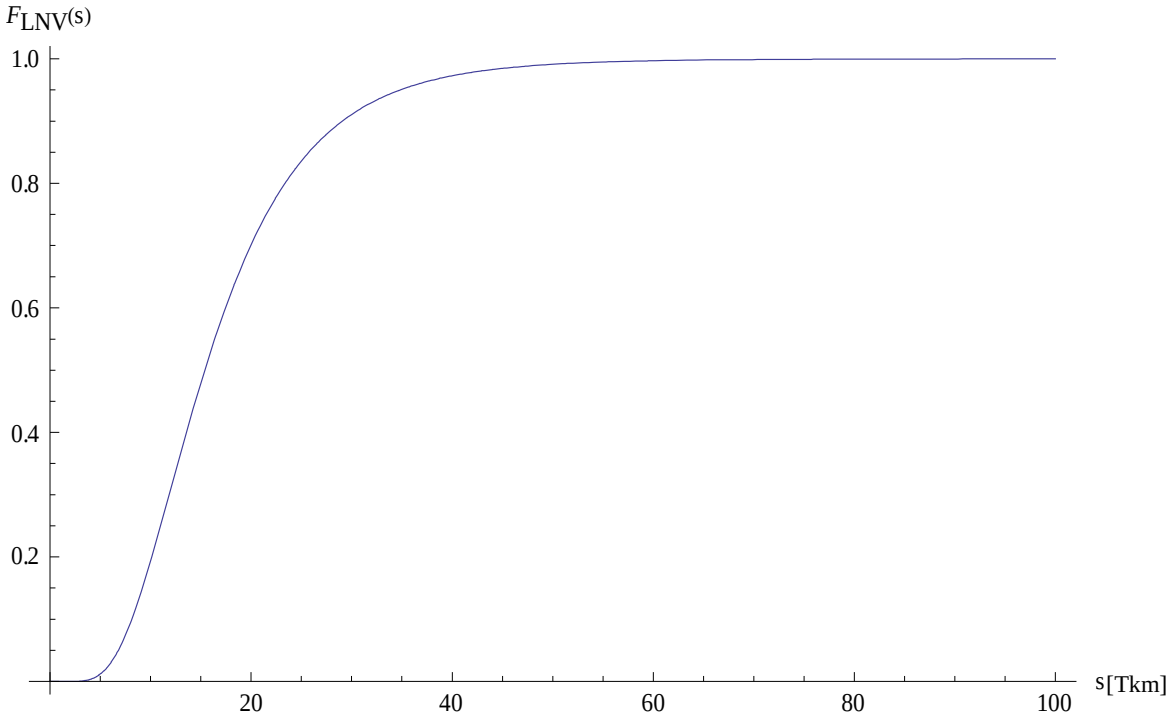


Bild A2-58: Jährliche Fahrleistungsverteilung für Cluster K-m

A2.59 Cluster Fahrzeuge mit Motoraufladung gesamt (m)

- Parameter der Lognormal-Verteilung: $\mu = 2{,}5533$

  $\sigma = 0{,}52749$
- Erwartungswert der jährlichen FLV: $E(S) = 14{,}77\ Tkm$

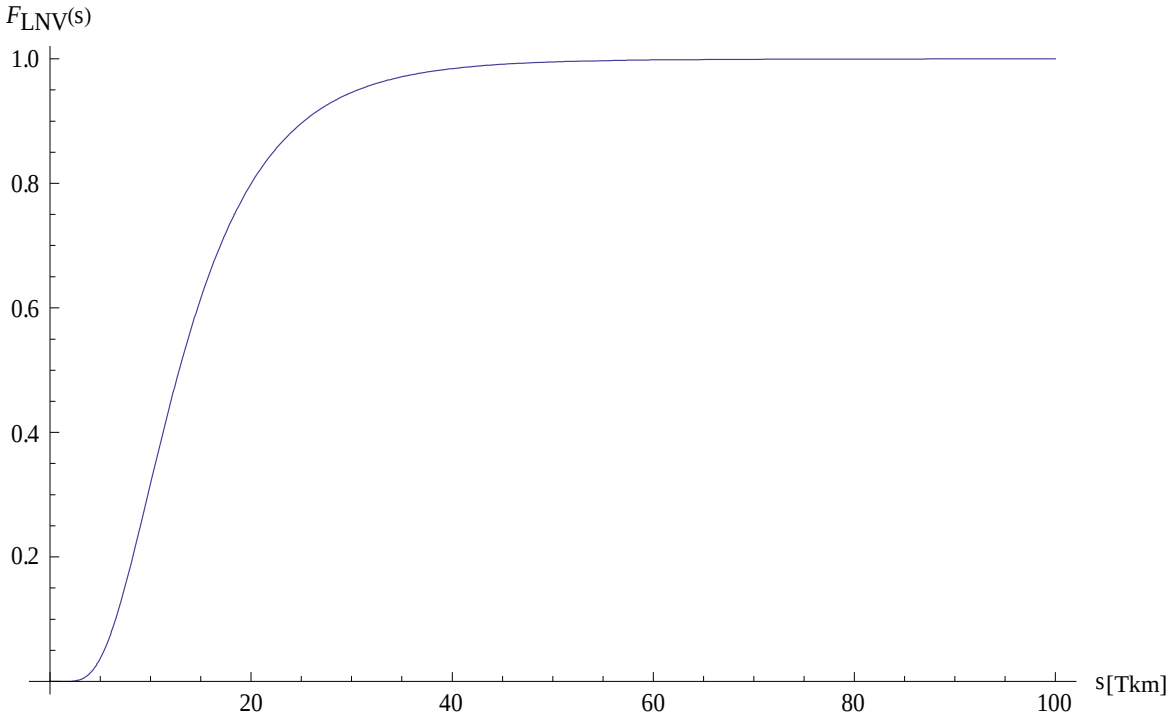


Bild A2-59: Jährliche Fahrleistungsverteilung für Cluster m

A2.60 Cluster gesamte Baureihe

- Parameter der Lognormal-Verteilung: $\mu = 2{,}8452$

  $\sigma = 0{,}636599$

- Erwartungswert der jährlichen FLV: $E(S) = 21{,}07\ Tkm$

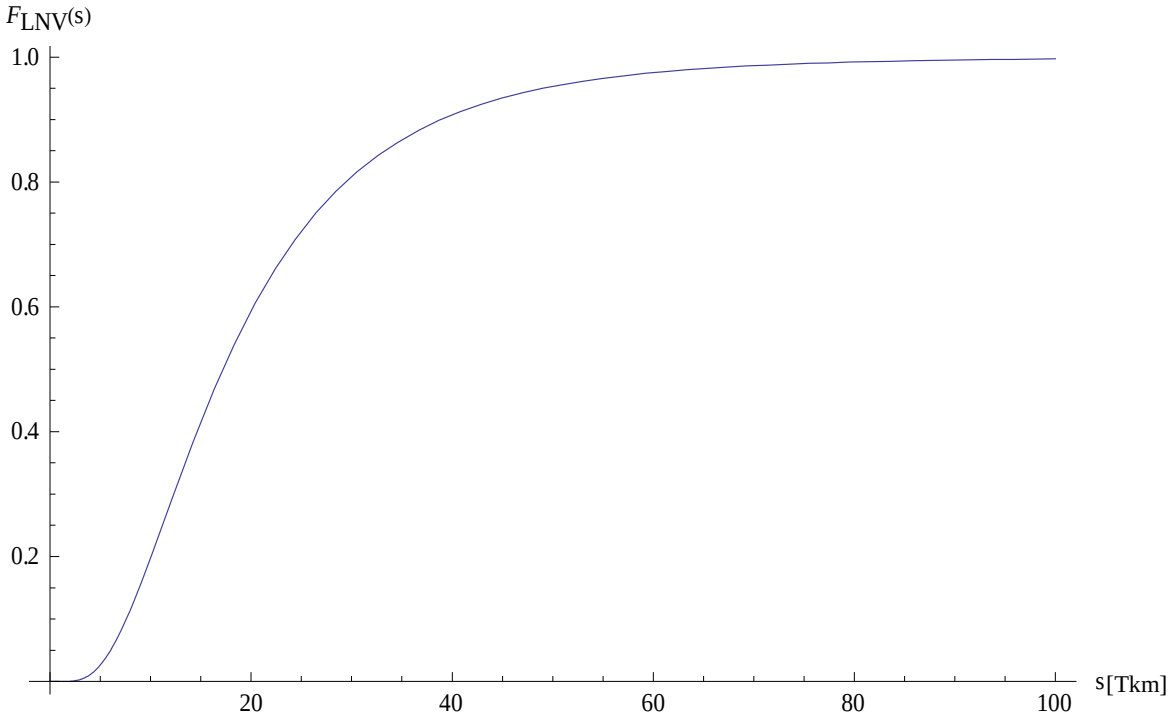


Bild A2-60: Jährliche Fahrleistungsverteilung für Cluster gesamte Baureihe

A3 Verteilungsfunktionen der Analysemenge

In nachfolgender Tabelle A3-1 werden die Parameter der ermittelten Verteilungsfunktionen für die Analysemenge dargestellt (s. Abschnitt 6.3.2.1). Berücksichtigt werden dabei die jeweilige Weibull-verteilte kilometerabhängige sowie die Weibull-verteilte zeitabhängige Verteilungsfunktion. Angegeben werden die entsprechenden Parameter α und β sowie der Anpassungsfaktor w. Bei der km-abhängigen Verteilungsfunktion wird außerdem das jeweilige Bestimmtheitsmaß B mit angegeben. Betrachtet werden hierbei die vier Fälle:

- unkorrigiert ohne Berücksichtigung des Anpassungsfaktors,
- unkorrigiert mit Berücksichtigung des Anpassungsfaktors,
- korrigiert ohne Berücksichtigung des Anpassungsfaktors und
- korrigiert mit Berücksichtigung des Anpassungsfaktors.

Tabelle A3-1: Zusammenstellung der Ergebnisse der Verteilungsfunktionen für die Analysemenge

Km-abhängige Verteilungsfunktion (Weibull-verteilt) Maßeinheit: Tkm				
Parameter	Unkorrigiert ohne w	Unkorrigiert mit w	Korrigiert ohne w	Korrigiert mit w
α	$20{,}5619 \cdot 10^{-6}$	$68{,}3452 \cdot 10^{-6}$	$6{,}74394 \cdot 10^{-6}$	$1{,}45866 \cdot 10^{-3}$
β	0,616798	2,69608	1,0163	1,34715
w	-	$334{,}266 \cdot 10^{-6}$	-	$1{,}50563 \cdot 10^{-3}$
B	0,9430	0,9964	0,9828	0,9880
Zeitabhängige Verteilungsfunktion (Weibull-verteilt) Maßeinheit: Jahr				
Parameter	Unkorrigiert ohne w	Unkorrigiert mit w	Korrigiert ohne w	Korrigiert mit w
α	$149{,}664 \cdot 10^{-6}$	$477{,}097 \cdot 10^{-3}$	$193{,}173 \cdot 10^{-6}$	$163{,}006 \cdot 10^{-3}$
β	0,616783	1,42118	1,01614	1,25163
w	-	$322{,}399 \cdot 10^{-6}$	-	$1{,}20874 \cdot 10^{-3}$

In folgender Tabelle A3-2 sind die gleichen Angaben wie in Tabelle A3-1 enthalten, nun jedoch für den Fall, dass die Ausschlussquote AQ mit berücksichtigt worden ist.

Tabelle A3-2: Zusammenstellung der Ergebnisse der Verteilungsfunktionen für die Analysemenge mit Berücksichtigung der Ausschlussquote

Km-abhängige Verteilungsfunktion (Weibull-verteilt) Maßeinheit: Tkm				
Parameter	Unkorrigiert ohne w	Unkorrigiert mit w	Korrigiert ohne w	Korrigiert mit w
α	$21{,}4963 \cdot 10^{-6}$	$68{,}3452 \cdot 10^{-6}$	$7{,}05016 \cdot 10^{-6}$	$1{,}45866 \cdot 10^{-3}$
β	0,616802	2,69608	1,01632	1,34715
w	-	$349{,}46 \cdot 10^{-6}$	-	$1{,}57407 \cdot 10^{-3}$
B	0,9430	0,9964	0,9828	0,9880
Zeitabhängige Verteilungsfunktion (Weibull-verteilt) Maßeinheit: Jahr				
Parameter	Unkorrigiert ohne w	Unkorrigiert mit w	Korrigiert ohne w	Korrigiert mit w
α	$156{,}467 \cdot 10^{-6}$	$477{,}097 \cdot 10^{-3}$	$201{,}955 \cdot 10^{-6}$	$163{,}006 \cdot 10^{-3}$
β	0,616787	1,42118	1,01614	1,25163
w	-	$337{,}053 \cdot 10^{-6}$	-	$1{,}26368 \cdot 10^{-3}$

A4 Verteilungsfunktionen der zeitbezogenen Zerlegung der Analysemenge

In nachfolgenden Tabellen werden die Parameter der ermittelten Verteilungsfunktionen für die zeitbezogene Zerlegung des Produktionszeitraums der Analysemenge dargestellt. Berücksichtigt werden dabei die Weibull-verteilte kilometerabhängige sowie die Weibull-verteilte zeitabhängige Verteilungsfunktion. Angegeben werden die entsprechenden Parameter α und β sowie der Anpassungsfaktor w. Bei der km-abhängigen Verteilungsfunktion wird außerdem das jeweilige Bestimmtheitsmaß B mit angegeben. Betrachtet werden hierbei wiederum die vier Fälle:

- unkorrigiert ohne Berücksichtigung des Anpassungsfaktors,
- unkorrigiert mit Berücksichtigung des Anpassungsfaktors,
- korrigiert ohne Berücksichtigung des Anpassungsfaktors und
- korrigiert mit Berücksichtigung des Anpassungsfaktors.

In Tabelle A4-1 sind zunächst die Ergebnisse für die Zeitmenge 1 (Produktionszeitraum von Dezember Jahr 1 bis Dezember Jahr 2) dargestellt. Eine Berücksichtigung der Ausschlussquote war hierbei nicht erforderlich, da alle Datensätze verwendet wurden.

Tabelle A4-1: Zusammenstellung der Ergebnisse der Verteilungsfunktionen für die Zeitmenge 1

Km-abhängige Verteilungsfunktion (Weibull-verteilt) Maßeinheit: Tkm				
Parameter	Unkorrigiert ohne w	Unkorrigiert mit w	Korrigiert ohne w	Korrigiert mit w
α	$6{,}532 \cdot 10^{-6}$	$2{,}14309 \cdot 10^{-8}$	$2{,}73091 \cdot 10^{-6}$	$201{,}982 \cdot 10^{-6}$
β	0,837159	5,09026	1,17188	2,18105
w	-	$233{,}202 \cdot 10^{-6}$	-	$502{,}955 \cdot 10^{-6}$
B	0,9319	0,9964	0,9612	0,9739
Zeitabhängige Verteilungsfunktion (Weibull-verteilt) Maßeinheit: Jahr				
Parameter	Unkorrigiert ohne w	Unkorrigiert mit w	Korrigiert ohne w	Korrigiert mit w
α	$99{,}0263 \cdot 10^{-6}$	$439{,}428 \cdot 10^{-3}$	$132{,}579 \cdot 10^{-6}$	$312{,}609 \cdot 10^{-3}$
β	0,837127	1,6312	1,17166	1,47365
w	-	$226{,}525 \cdot 10^{-6}$	-	$467{,}03 \cdot 10^{-3}$

In Tabelle A4-2 sind die Ergebnisse für die Zeitmenge 2 (Produktionszeitraum von Dezember Jahr 1 bis September Jahr 3) unter Berücksichtigung der Ausschlussquote dargestellt.

Tabelle A4-2: Zusammenstellung der Ergebnisse der Verteilungsfunktionen für die Zeitmenge 2

Km-abhängige Verteilungsfunktion (Weibull-verteilt) Maßeinheit: Tkm				
Parameter	Unkorrigiert ohne w	Unkorrigiert mit w	Korrigiert ohne w	Korrigiert mit w
α	$8{,}05692 \cdot 10^{-6}$	$6{,}4936 \cdot 10^{-8}$	$3{,}20475 \cdot 10^{-6}$	$74{,}3638 \cdot 10^{-6}$
β	0,844225	4,6888	1,18852	2,43731
w	-	$296{,}991 \cdot 10^{-6}$	-	$639{,}174 \cdot 10^{-6}$
B	0,9407	0,9943	0,9644	0,9819
Zeitabhängige Verteilungsfunktion (Weibull-verteilt) Maßeinheit: Jahr				
Parameter	Unkorrigiert ohne w	Unkorrigiert mit w	Korrigiert ohne w	Korrigiert mit w
α	$125{,}315 \cdot 10^{-6}$	$403{,}354 \cdot 10^{-3}$	$164{,}362 \cdot 10^{-6}$	$288{,}128 \cdot 10^{-3}$
β	0,844186	1,69347	1,18825	1,57594
w	-	$288{,}185 \cdot 10^{-6}$	-	$595{,}971 \cdot 10^{-3}$

Die Ergebnisse der Zeitmenge 3 entsprechen denen der gesamten Analysemenge, welche in Tabelle A3-2 bereits dargestellt sind.

A5 Verteilungsfunktionen der fahrzeugbezogenen Zerlegung der Analysemenge

In nachfolgenden Tabellen werden die Parameter der ermittelten Verteilungsfunktionen für die fahrzeugbezogene Zerlegung der Analysemenge dargestellt. Berücksichtigt werden dabei die Weibull-verteilte kilometerabhängige sowie die Weibull-verteilte zeitabhängige Verteilungsfunktion. Angegeben werden die entsprechenden Parameter α und β sowie der Anpassungsfaktor w. Bei der km-abhängigen Verteilungsfunktion wird außerdem das jeweilige Bestimmtheitsmaß B mit angegeben. Betrachtet werden hierbei wiederum die vier Fälle:

- unkorrigiert ohne Berücksichtigung des Anpassungsfaktors,
- unkorrigiert mit Berücksichtigung des Anpassungsfaktors,
- korrigiert ohne Berücksichtigung des Anpassungsfaktors und
- korrigiert mit Berücksichtigung des Anpassungsfaktors.

Außerdem werden die Ergebnisse sowohl für den Fall, dass die Fahrleistungsverteilung bestimmt wurde, als auch für den Fall, dass die FLV übergeben wurde, angegeben.

In Tabelle A5-1 sind zunächst die Ergebnisse für das Cluster der Diesel-Fahrzeuge dargestellt. Eine Berücksichtigung der Ausschlussquote war hierbei nicht erforderlich, da alle Datensätze verwendet werden konnten. Die km-abhängigen Verteilungsfunktionen sind für beide Fälle identisch.

Tabelle A5-1: Zusammenstellung der Ergebnisse der Verteilungsfunktionen für das Cluster Diesel

Km-abhängige Verteilungsfunktion (Weibull-verteilt) Maßeinheit: Tkm				
Parameter	Unkorrigiert ohne w	Unkorrigiert mit w	Korrigiert ohne w	Korrigiert mit w
α	$17{,}179 \cdot 10^{-6}$	$720{,}882 \cdot 10^{-6}$	$4{,}02754 \cdot 10^{-6}$	$821{,}255 \cdot 10^{-6}$
β	0,640426	1,92272	1,09656	1,42898
w	-	$340{,}584 \cdot 10^{-6}$	-	$1{,}49491 \cdot 10^{-6}$
B	0,9642	0,9949	0,9920	0,9957
Zeitabhängige Verteilungsfunktion (Weibull-verteilt) Maßeinheit: Jahr Fahrleistungsverteilung bestimmt				
Parameter	Unkorrigiert ohne w	Unkorrigiert mit w	Korrigiert ohne w	Korrigiert mit w
α	$155{,}481 \cdot 10^{-6}$	$553{,}649 \cdot 10^{-3}$	$192{,}233 \cdot 10^{-6}$	$162{,}232 \cdot 10^{-3}$
β	0,64041	1,27608	1,09634	1,31514
w	-	$330{,}233 \cdot 10^{-6}$	-	$1{,}22058^{-3}$
Zeitabhängige Verteilungsfunktion (Weibull-verteilt) Maßeinheit: Jahr Fahrleistungsverteilung übergeben				
Parameter	Unkorrigiert ohne w	Unkorrigiert mit w	Korrigiert ohne w	Korrigiert mit w
α	$135{,}959 \cdot 10^{-6}$	$420{,}59 \cdot 10^{-3}$	$153{,}198 \cdot 10^{-6}$	$129{,}091 \cdot 10^{-3}$
β	0,640412	1,3382	1,09638	1,33893
w	-	$323{,}667 \cdot 10^{-6}$	-	$1{,}15805 \cdot 10^{-3}$

In A5-2 sind die Ergebnisse für das Cluster der Fahrzeuge mit Motoraufladung unter Berücksichtigung der Ausschlussquote dargestellt.

Tabelle A5-2: Zusammenstellung der Ergebnisse der Verteilungsfunktionen für das Cluster Motoraufladung

Km-abhängige Verteilungsfunktion (Weibull-verteilt) Maßeinheit: Tkm				
Parameter	Unkorrigiert ohne w	Unkorrigiert mit w	Korrigiert ohne w	Korrigiert mit w
α	$3{,}66411 \cdot 10^{-7}$	$2{,}0822 \cdot 10^{-9}$	$4{,}54862 \cdot 10^{-9}$	$1{,}15733 \cdot 10^{-11}$
β	1,85023	1,85006	3,23436	3,2337
w	-	176,059	-	393,85
B	0,9938	0,9938	0,9897	0,9897
Zeitabhängige Verteilungsfunktion (Weibull-verteilt) Maßeinheit: Jahr Fahrleistungsverteilung bestimmt				
Parameter	Unkorrigiert ohne w	Unkorrigiert mit w	Korrigiert ohne w	Korrigiert mit w
α	$82{,}1406 \cdot 10^{-6}$	$9{,}96167 \cdot 10^{-7}$	$106{,}124 \cdot 10^{-6}$	$2{,}42694 \cdot 10^{-6}$
β	1,84925	1,85006	3,13274	3,2337
w	-	82,3946	-	39,4011
Zeitabhängige Verteilungsfunktion (Weibull-verteilt) Maßeinheit: Jahr Fahrleistungsverteilung übergeben				
Parameter	Unkorrigiert ohne w	Unkorrigiert mit w	Korrigiert ohne w	Korrigiert mit w
α	$68{,}1968 \cdot 10^{-6}$	$1{,}0014 \cdot 10^{-6}$	$89{,}1667 \cdot 10^{-6}$	$3{,}56641 \cdot 10^{-6}$
β	1,8491	1,85006	3,10498	3,2337
w	-	68,0432	-	21,9654

A6 Variantenuntersuchung

Nachfolgend werden die Ergebnisse der Untersuchungen der vier Varianten der Analysemenge präsentiert. Diese Varianten ergeben sich aus der Tatsache, dass es bei den Datensätzen der Schnittmenge aus den Daten des GuK-Bereichs und der Diagnosebewährung möglich ist, dass sowohl unterschiedliche Datumsangaben als auch verschiedene Fahrleistungen vorliegen können. Das Datum der Diagnose und das GuK-Reparaturdatum müssen nicht übereinstimmen, so dass in der Zwischenzeit eine gewisse Fahrleistung zusätzlich hinzugekommen sein kann. Mögliche Erklärungen hierfür sind z.B. Überprüfungsfahrten in der entsprechenden Werkstatt oder die Durchführung der GuK-Reparatur und der Diagnose in unterschiedlichen und örtlich getrennten Werkstätten.
Vier Varianten für die mögliche Zusammensetzung der Analysemenge wurden identifiziert, die sich wie folgt zusammensetzen:

- Variante 1: Reparaturdatum mit zugehöriger Fahrleistung,
- Variante 2: Startdatum Diagnose mit zugehöriger Fahrleistung,
- Variante 3: früheres Datum mit zugehöriger Fahrleistung (bei gleicher Datumsangabe wurde die kleinere Fahrleistung gewählt) und
- Variante 4: späteres Datum mit zugehöriger Fahrleistung (bei gleicher Datumsangabe wurde die größere Fahrleistung gewählt).

In Tabelle A6-1 sind die Ergebnisse des Wuppertaler Zuverlässigkeitsprognosemodells für die jeweils unterschiedlich zusammengesetzte Analysemenge gegenübergestellt. Es handelt sich dabei jeweils um Datensätze zu den gleichen 46 Ereignissen der gleichen Fahrzeuge. Nur der Wert des Reparaturdatums und der Fahrleistung können unterschiedlich sein. Der betrachtete Zulassungs- und Ausfallzeitraum sowie die Fertigungsmenge ist bei allen Varianten derselbe.

Tabelle A6-1: Zusammenstellung der Ergebnisse der Variantenuntersuchung

	Variante 1	**Variante 2**	**Variante 3**	**Variante 4**
Parameter der jährlichen Fahrleistungsverteilung (lognormal-verteilt)				
μ	3,0595	3,0609	3,0607	3,0598
σ	0,6505	0,6511	0,6511	0,6505
$E(S)$	26,34	26,39	26,38	26,35
Parameter der an die PiU-Ereignisse angepassten Weibull-Verteilung				
$\alpha\left[\frac{1}{a^{\beta}}\right]$	$24{,}823 \cdot 10^{-6}$	$24{,}866 \cdot 10^{-6}$	$24{,}861 \cdot 10^{-6}$	$24{,}829 \cdot 10^{-6}$
β	1,561	1,559	1,560	1,561
Ereignisrate nach einem Jahr				
$h_E(t)\left[\frac{1}{a}\right]$	$38{,}743 \cdot 10^{-6}$	$38{,}776 \cdot 10^{-6}$	$38{,}772 \cdot 10^{-6}$	$38{,}745 \cdot 10^{-6}$
Ereignisrate nach fünf Jahren				
$h_E(t)\left[\frac{1}{a}\right]$	$95{,}528 \cdot 10^{-6}$	$95{,}403 \cdot 10^{-6}$	$95{,}419 \cdot 10^{-6}$	$95{,}560 \cdot 10^{-6}$

In obiger Tabelle A6-1 ist zunächst zu erkennen, dass die Ergebnisse der Fahrleistungsverteilung nahezu identisch sind. Die Parameter μ weichen um weniger als 0,05% voneinander ab, die Parameter σ um weniger als 0,09% und die Erwartungswerte der jährlichen Fahrleistung um weniger als 0,2%. Die Unterschiede in den Ergebnissen der Variantenanalysen sind folglich zu vernachlässigen.

Weiterhin sind auch die Unterschiede bei den zeitabhängigen Parametern der an die PiU-Ereignisse angepassten Verteilungsfunktion nicht signifikant genug, um einen Einfluss hervorzurufen. Die Parameter α weichen um weniger als 0,15% voneinander ab, die Parameter β um weniger als 0,13%. Die Ergebnisse der Ereignisrate nach einem Jahr weichen um weniger als 0,09% voneinander ab, nach fünf Jahren um weniger als 0,16%.

Folglich hat es keinen signifikanten Einfluss auf die Ergebnisse, welche Variante der möglichen Zusammensetzung der Analysemenge zum Einsatz kommt.