Was dahinter steckt: Eine Analyse der Abgas-Abschaltvorrichtungen in modernen Kraftfahrzeugen

Moritz Contag*, Guo Li†, Andre Pawlowski*, Felix Domke‡,
Kirill Levchenko†, Thorsten Holz* und Stefan Savage†

* Ruhr-Universität Bochum, Deutschland, {moritz.contag, andre.pawlowski, thorsten.holzg@rub.de
† University of California, San Diego, {gul027, klevchen, savage}@cs.ucsd.edu
‡ tmbinc@elitedvb.net

Zusammenfassung – **Moderne Fahrzeuge müssen eine Reihe von Umweltschutzbestimmungen einhalten, die das Emissionsniveau für die verschiedenen Treibhausgase, Toxine und Feinstaubpartikel limitieren. Um die Gesetzeskonformität sicherzustellen, testen die Regulierungsbehörden Fahrzeuge unter kontrollierten Bedingungen und messen deren Emissionen am Auspuffendrohr. Allerdings haben die „Black Box"-Charakteristik dieser Prüfverfahren und die Standardisierung ihrer Formen Möglichkeiten zur Umgehung geschaffen. Mithilfe moderner elektronischer Motorsteuergeräte können die Hersteller programmgesteuert erschließen, wann ein Fahrzeug einem Emissionstest unterzogen wird, und das Betriebsverhalten des Fahrzeugs entsprechend ändern, so dass die Abgasnormen eingehalten werden, während sie im normalen Fahrbetrieb zugunsten einer höheren Motorleistung überschritten werden. Obwohl der Einsatz einer solchen Abschaltvorrichtung durch Volkswagen die Thematik des Abgasbetrugs in die Öffentlichkeit getragen hat, waren bisher nur wenige Einzelheiten darüber bekannt, um welche Art von Abschaltvorrichtung es sich genau handelt, wie es dazu gekommen ist und wie sie sich auf das Fahrzeugverhalten auswirkt.**

Im vorliegenden Paper stellen wir unsere Analyse zu zwei Software-Abschaltvorrichtungen bei Dieselmotoren vor: eine von der Volkswagen Group für das Bestehen der Emissionsprüfungen in den USA und in Europa eingesetzte Form der Abschaltvorrichtung, und eine zweite, die wir bei Fiat Chrysler Automobiles festgestellt haben. Um diese Analyse durchzuführen, haben wir neue Forensikverfahren zur statischen Firmware-Analyse entwickelt, die notwendig sind, um die bekannten Abschaltvorrichtungen automatisch zu identifizieren und deren Funktion nachzuweisen. Wir prüften über 900 Firmware-Images und konnten eine potenzielle Abschaltvorrichtung in über 400 Firmware-Images über eine Zeitspanne von acht Jahren ermitteln. Wir beschreiben die genauen Bedingungen, anhand derer die Firmware einen Prüfzyklus erkennen kann und wie sie sich auf das Motorverhalten auswirkt. Die vorliegende Arbeit befasst sich mit den technischen Herausforderungen, denen die Regulierungsbehörden in Zukunft gegenüberstehen und unterstreicht die wichtige Forschungsagenda, angesichts der kontroversen Haltung der Hersteller zielgerichtet für Software-Sicherheit zu sorgen.

I. EINLEITUNG

Am 18. September 2015 richtete die US Environmental Protection Agency (EPA) eine Notice of Violation (Mitteilung über einen Rechtsverstoß) an die Volkswagen Group und beschuldigte einen der weltweit größten Automobilhersteller der Umgehung der EPA-Emissionsprüfungen [18], womit der teuerste Abgasskandal in der Geschichte angestoßen wurde.

Kern des Skandals ist der Einsatz einer *Abschaltvorrichtung* durch Volkswagen, die von der EPA als eine Vorrichtung definiert wird, welche „die Wirksamkeit der Abgasreinigungsanlage unter Bedingungen reduziert, die vernünftigerweise bei normalem Fahrzeugbetrieb und Gebrauch zu erwarten sind", mit Ausnahmen für das Starten des Motors, für Rettungsfahrzeuge und zur Vermeidung von Unfällen [19].

Die Abschaltvorrichtung in Volkswagen-Fahrzeugen nutzte Umgebungsparameter, einschließlich Fahrzeit und zurückgelegte Strecke, um einen Standard-Emissionsprüfzyklus zu erkennen: sobald das Motorsteuergerät feststellte, dass das Fahrzeug nicht unter Prüfbedingungen betrieben wurde, deaktivierte es bestimmte Abgasreinigungsmaßnahmen, was in einigen Fällen dazu führte, dass das Fahrzeug das bis zu 40-fache der zulässigen Stickoxide ausstieß [15].

Abschaltvorrichtungen wie die von Volkswagen sind aufgrund der Art und Weise möglich, wie die Regulierungsbehörden die Fahrzeuge auf Gesetzeskonformität prüfen, bevor sie zum Verkauf angeboten werden können. In den meisten Ländern, einschließlich in den USA und in Europa, werden die Emissionsprüfungen auf einem Rollenprüfstand durchgeführt, eine Apparatur, die das Fahrzeug an Ort und Stelle hält, während die Räder frei laufen können. Während der Prüfung durchläuft das Fahrzeug ein genau definiertes Geschwindigkeitsprofil (d. h. zeitabhängige Fahrzeuggeschwindigkeit), mit dem versucht wird, reale Fahrbedingungen zu imitieren. Die Bedingungen der Prüfung, einschließlich des Geschwindigkeitsprofils, sind sowohl standardisiert als auch allgemein bekannt, um sicherzustellen, dass die Prüfung von einer unabhängigen Partei auf transparente und regelkonforme Art und Weise durchgeführt werden kann. Allerdings ermöglicht die Kenntnis der genauen Prüfungsbedingungen den Herstellern auch, das Verhalten ihrer Fahrzeuge während eines Prüfzyklus absichtlich zu verändern, ein umgangssprachlich auch als „Cycle Beating" bezeichnetes Vorgehen.

Während der Betrug von Volkswagen atemberaubende Ausmaße annahm (ein Dutzend Fahrzeugmodelle über eine Zeitspanne von mindestens sechs Jahren), hat er auch deutlich gemacht, wie schwierig die Überwachung zur Einhaltung der Emissionsgrenzwerte durch die Hersteller ist. Die Erfüllung moderner Abgasnormen ist eine der wichtigsten Herausforderungen, denen die Fahrzeughersteller gegenüberstehen, da die Abgasnormen zunehmend strenger werden. In vielen Fällen lässt sich die Gesetzeskonformität aufgrund technischer Einschränkungen nicht mit den Anforderungen der Verbraucher an Leistung, Effizienz oder Kosten in Einklang bringen – was einen mächtigen Anreiz für die Autobauer schafft, die gesetzliche Bürde zu umgehen. Gleichzeitig haben Automobile an Komplexität zugenommen: das moderne Automobil ist ein komplexes cyber-physisches System, das aus zahlreichen elektronischen Komponenten besteht, die es sowohl zu einem softwarelastigen als auch zu einem mechanischen System machen. Ein Fahrzeug der Premiumklasse kann zum Beispiel mehr als 70 elektronische Steuergeräte und 100 Millionen Code-Zeilen umfassen [4]. Im Rahmen dieser Entwicklung werden nahezu alle Aspekte des Motorbetriebs durch ein Motorsteuergerät (Engine Control Unit - ECU) gesteuert, ein eingebettetes System, das einen geschlossenen Regelkreis zwischen Motorsensoren und Aktoren schafft. Damit können die Hersteller alle Aspekte des Motorbetriebs präzise steuern und

dementsprechend erhebliche Verbesserungen in Bezug auf Leistung, Zuverlässigkeit und Kraftstoffverbrauch erreichen. Das ECU ist auch dafür verantwortlich, sicherzustellen, dass das Fahrzeug die von den staatlichen Regulierungsbehörden auferlegten Abgasvorschriften einhält. Während einige Maßnahmen zur Abgasreinigung, wie zum Beispiel der Katalysator oder Partikelfilter, passiv arbeiten, müssen viele andere Komponenten allerdings aktiv vom ECU gesteuert werden, wobei manchmal Kompromisse bei Leistung oder Effizienz zugunsten der Abgaskonformität gemacht werden müssen. Diese Kompromisse stellen besonders für Dieselmotoren eine große Herausforderung dar, die in ihrer einfachsten Form lauter sind und mehr Feinstaubpartikel und Stickoxide (NO_x) als Benzinmotoren ausstoßen [3].

Die elektronische Motorsteuerung hat es zudem einfacher gemacht, die Emissionsprüfung durch Einbindung einer Abschaltvorrichtung in die Software zu umgehen. Die Black Box"-Charakteristik der Emissionsprüfung macht es nahezu unmöglich, diese softwarebasierte Abschaltvorrichtung während einer Prüfung zu entdecken, so dass die Regulierungsbehörden gezwungen sind, sich auf die abschreckende Wirkung hoher Geldstrafen gegen den Betrug zu verlassen. Wie der Volkswagen-Fall zeigt, kann es unglücklicherweise mehrere Jahre dauern, bis eine solche Abschaltvorrichtung entdeckt wird. Angesichts der endgültigen Grenzen der Prüfmethoden fühlen wir uns veranlasst, darüber nachzudenken, ob man Abschaltvorrichtungen mithilfe von *Software-Nachweisverfahren* aufspüren kann. Leider stellt der Nachweis komplexer Software-Systeme für sich genommen eine schwierige Aufgabe dar, insbesondere bei einem cyber-physischen System wie einem modernen Auto. In unserem Fall ist die Situation zudem *kontrovers* – anstatt zu versuchen, Softwarefehler zu finden, suchen wir nach absichtlichen Versuchen, das Verhalten eines Systems unter Prüfbedingungen zu ändern. Dieses Paper soll ein erster Schritt zum cyber-physischen Systemnachweis in einer kontroversen Umgebung mit zwei Fallbeispielen für automobile Abschaltvorrichtungen und binären Analyseverfahren sein, um nachweiskritische Code-Elemente über mehrere Software-Revisionen zu identifizieren.

Wir beginnen mit zwei Fallbeispielen von Software-Abschaltvorrichtungen, die in leichten Dieselfahrzeugen festgestellt wurden. Der erste Fall bezieht sich auf Fahrzeuge, die von der Volkswagen Group hergestellt wurden und die deren Einsatz öffentlich zugegeben hat. Die Volkswagen-Abschaltvorrichtung ist wohl die komplexeste in der Geschichte des Automobils. Leider sind öffentlich nur wenige technische Einzelheiten über ihre Funktionsweise, ihren Einfluss auf das Motorverhalten und ihre zeitliche Weiterentwicklung verfügbar; unser Paper schließt diese Lücke und macht es unserer Ansicht nach einfacher, die wesentlichen Herausforderungen für die Regulierungsbehörden in der Zukunft zu verdeutlichen. Leider ist Volkswagen nicht der einzige Autobauer, der die Abgasuntersuchungen umgeht. Fiat Chrysler Automobiles (FCA) wird derzeit in Europa überprüft, da neueste, im Straßenbetrieb ermittelte Untersuchungsdaten deutlich höhere Emissionen als in den amtlichen Abgasuntersuchungen zur Einhaltung der Emissionswerte gezeigt haben [17]. Im vorliegenden Paper identifizieren und beschreiben wir eine timer-basierte Abschaltvorrichtung, die in einem Fiat 500X eingesetzt wird. Wir gehen davon aus, dass wir die ersten sind, die diese Abschaltvorrichtung öffentlich bekannt machen.

Sowohl in Volkswagen- als auch in Fiat-Fahrzeugen kommt das von Bosch hergestellte Diesel-Motorsteuergerät EDC 17 zum Einsatz. Mittels Kombination aus manuellem Reverse-Engineering der binären Firmware-Images und Erkenntnissen aus der technischen Dokumentation des Herstellers, die in der Motor-Tuning-Szene (d. h. Auto-Enthusiasten, die ihre Software-Systeme zur Leistungssteigerung modifizieren) gehandelt wird, identifizieren wir die eingesetzten Abschaltvorrichtungen, wie von diesen erkannt wurde, wann sich das Fahrzeug im Prüfzyklus befindet, und wie diese Eingriffe zur Änderung des Motorverhaltens eingesetzt wurden. Insbesondere haben wir überzeugende Beweise dafür gefunden, dass beide Abschaltvorrichtungen von Bosch *entwickelt* und dann von Volkswagen und Fiat für ihre jeweiligen Fahrzeuge *freigegeben* wurden.

Um eine größere Studie durchzuführen, haben wir statische Code-Analyseverfahren angewendet, um die Entwicklung der Abschaltvorrichtung über hunderte Versionen von Fahrzeug-Firmware nachzuverfolgen. Genauer gesagt haben wir ein statisches Analysesystem, das sogenannte CURVEDIFF, entwickelt, um die Abschaltvorrichtung von Volkswagen in einem bestimmten Firmware-Image automatisch zu entdecken und die Parameter zu extrahieren, die deren Funktion bestimmen. Insgesamt analysierten wir 926 Firmware-Images und konnten in diesen Images 406 potenzielle Abschaltvorrichtungen erfolgreich identifizieren. Darüber hinaus haben wir den Einfluss auf ein bestimmtes Teilsystem automatisch nachgewiesen.

Zusammenfassend stellt sich unser Beitrag wie folgt dar:

- Wir liefern eine detaillierte technische Analyse der Abschaltvorrichtungen in Fahrzeugen, die von zwei unabhängigen Automobilherstellern, der Volkswagen Group und Fiat Chrysler Automobiles, vertrieben werden, deren Wirkung darin besteht, die Abgasuntersuchungen in den USA und in Europa zu umgehen.
- Wir entwickeln und implementieren ein statisches, binäres Analyse-Tool, genannt CURVEDIFF, zur Identifizierung dieser Abschaltvorrichtungen in einem bestimmten Firmware-Image, mit dem es uns möglich ist, die Entwicklung und das Verhalten des Umgehungs-Codes über eine große Anzahl von Firmware-Images nachzuverfolgen.
- Wir setzen unser Tool ein, um die Entwicklung der Abschaltvorrichtungen und deren Einfluss auf das Motorverhalten über acht Jahre und über ein Dutzend Fahrzeugmodelle zu studieren.

Allerdings sind wir überzeugt, dass die weitreichende Wirkung unserer Arbeit über diesen detaillierten technischen Beitrag hinaus darin besteht, die Herausforderungen in Verbindung mit der Zertifizierung der Gesetzeskonformität in einer cyber-physischen Umgebung zur Sprache zu bringen. Moderne Black-Box-Prüfverfahren sind kostspielig und zeitaufwändig und können, wie diese Fälle zeigen, leicht durch Abschaltvorrichtungssoftware, die „für den Prüfer prüft", umgangen werden. Die Lücke zwischen Black-Box-Prüfung und modernen Software-Sicherungskonzepten treibt eine wichtige Forschungsagenda voran, die erst dann noch wichtiger wird, wenn die Regulierungsbehörden aufgefordert sind, zunehmend komplexere Fahrzeugsysteme (z. B. autonomes Fahren) zu überwachen und zu bewerten. Wir denken, dass konkrete Beispiele, wie die von uns in diesem Paper beschriebenen, die Grundlage für diese Diskussion schaffen und die tatsächlichen Probleme der Regulierungsbehörden verdeutlichen.

Der verbleibende Teil des vorliegenden Paper ist wie folgt aufgebaut. Teil II liefert den nötigen technischen Hintergrund für den Rest des Paper, auf den in Teil III eine Diskussion der verfügbaren Datensätze und in Teil IV eine ausführliche Beschreibung der Abschaltvorrichtungen folgt, die wir aufgespürt haben. In Teil V erläutern wir, wie wir diese Detektion im großen Maßstab umsetzen, gefolgt von einer Zusammenfassung der Ergebnisse, die wir mithilfe dieses Tools gefunden haben. Abschließend erörtern wir die Auswirkungen unserer Erkenntnisse in Teil VII und geben in Teil VIII unsere Schlussfolgerung ab.

II. TECHNISCHER HINTERGRUND

Nachstehend geben wir eine kurze Übersicht der technischen Grundlagen, die erforderlich sind, um den Rest dieses Paper zu verstehen.

A. Dieselmotoren

Der charakteristische Unterschied zwischen einem Benzin- und einem Dieselmotor liegt darin, wie die Verbrennung eingeleitet wird. Bei einem Benzinmotor wird ein Gemisch aus Luft und Kraftstoff in den Verbrennungszylinder gesaugt und von einem Zündfunken entzündet. Bei einem Dieselmotor wird Luft in den Verbrennungszylinder gesaugt und, im entscheidenden Moment während des Kompressionstakts, Kraftstoff in den Zylinder eingespritzt, der sich in der komprimierten Luft entzündet. Dementsprechend entsteht bei einem Benzinmotor das Luft-Kraftstoff-Gemisch, *bevor* es in den Zylinder gesaugt und entzündet wird, während bei einem Dieselmotor die Luft und der Kraftstoff *zum Zündzeitpunkt* vermischt werden, was zu einer unvollkommenen und inhomogenen Mischung führt. Dies ist für viele der charakteristischen Merkmale eines Dieselmotors verantwortlich, einschließlich der schwarzen Rauchfahne und des als „Dieselnageln" bekannten, heftigen Klopfgeräuschs. Der aus Feinstaub bestehende schwarze Rauch, auch als Ruß bezeichnet, resultiert aus der unvollständigen Verbrennung des Kraftstoffs und unterliegt bei leichten Dieselnutzfahrzeugen strengen Grenzwerten. Der zweite wesentliche Schadstoff im Dieselabgas sind Stickoxide (NO und NO_2, abgekürzt NO_x). Die aktuellen Abgasnormen schreiben enge Grenzwerte für die Menge an ausgestoßenem Feinstaub und NO_x vor und verlangen spezielle Begrenzungsmaßnahmen für deren Ausstoßmenge. Die Fahrzeuge, die in den Anwendungsbereich der vorliegenden Arbeit fallen, setzen dabei auf die folgenden Abgasregelvorrichtungen, um so gesetzliche Konformität zu erreichen.

AGR. Die Abgasrückführung (AGR) ist ein Abgasregelsystem, bei dem das Abgas wieder in den Motoransaugtrakt zurückgeführt wird. Die AGR reduziert die NO_x-Menge im Abgas deutlich [12], [16]. Leider erhöht die AGR auch die Menge an Feinstaubpartikeln im Abgas, was zu einem Kompromiss zwischen NO_x und Feinstaub führt.

NSK. Ein NO_x-Speicherkatalysator (NSK), auch als Mager-NO_x-Falle (LNT) bezeichnet, arbeitet nach dem Prinzip der Oxidation von NO zu NO_2 und speichert das NO_2 dann im Katalysator selbst ab. Die Speicherkapazität des Katalysators ist begrenzt und hat eine Dauer von 30 bis 300 Sekunden, danach muss eine Regeneration erfolgen. Um den Katalysator zu regenerieren, wechselt der Motor für 2 bis 10 Sekunden in ein fettes Luft-Kraftstoff-Gemisch. Während der Regeneration arbeitet der Motor weniger effizient, wodurch der Kraftstoffverbrauch steigt [16]. Ein fettes Luft-Kraftstoff-Gemisch führt zudem zu einer erhöhten Feinstaubproduktion, so dass erneut ein Kompromiss bei den NO_x-Emissionen zugunsten der Feinstaubemissionen erfolgt.

SCR. Die selektive katalytische Reduktion (SCR) stellt eine Alternative zum NSK zur Senkung der NO_x-Emissionen dar, indem Harnstoff in den Abgasstrom eingespritzt wird. Die SCR ist effektiver als der (vorstehend beschriebene) NSK und wird normalerweise bei Dieselmotoren ab 3 Litern Hubraum eingesetzt. Der Nachteil der SCR liegt in ihrer größeren Komplexität und der Notwendigkeit, dass die Harnstoff-Flüssigkeit (auch unter ihrem Markennamen AdBlue bekannt) immer mitgeführt und nachgefüllt werden muss. Bei mehreren Volkswagen-Fahrzeugen, die in den Abgasbetrugsskandal verwickelt sind, wird Berichten zufolge die Harnstoffeinspritzmenge außerhalb eines Prüfzyklus limitiert. Mit Ausnahme der in Tabelle II ausgewiesenen Ergebnisse konnten in diesem Paper keine Abschaltvorrichtungen enttarnt werden, mit denen die SCR manipuliert wird.

DPF. Ein Dieselpartikelfilter (DPF) fängt Feinstaubpartikel (Ruß) ab, wodurch die Menge an schwarzem Rauch, der den Auspuff verlässt, zu einem großen Teil reduziert wird. Zwar arbeitet der DPF beim Abfangen der Feinstaubpartikel sehr effektiv, da die Feinstaubmenge jedoch akkumuliert, steigt auch der Luftstromwiderstand, wodurch die Last für den Motor erhöht wird. Um den DPF von angesammelten Ablagerungen zu reinigen, muss er etwa alle 500 km einen Regenerationszyklus durchlaufen, der 10 bis 15 Minuten dauert. Für die DPF-Regeneration sind hohe Abgastemperaturen erforderlich, die normalerweise nur bei Volllast erreicht werden. Wird das Fahrzeug bei Volllast betrieben, regeneriert der DPF von selbst. Leider ergeben sich diese Bedingungen im normalen Stadtverkehr normalerweise nicht, so dass das ECU eine *aktive Regeneration* durchführen muss. In diesem Modus passt das ECU den Motorbetrieb für eine Erhöhung der Abgastemperatur an, damit die Regeneration des DPF erfolgen kann; wird das Fahrzeug jedoch nur auf Kurzstrecken betrieben, wird eine solche Temperatur gegebenenfalls niemals erreicht. Bei ausreichend hoher Rußbeladung zeigt das Fahrzeug über eine spezielle Warnleuchte an, dass der Fahrer das Fahrzeug mit höherer Geschwindigkeit betreiben soll, um die aktive Regeneration einzuleiten. Geschieht das nicht, muss der DPF gewartet werden [21]. Dementsprechend bringt der DPF, auch wenn er bei der Reduzierung der Partikelemissionen hoch effizient arbeitet, Leistungseinbußen mit sich und kann für den Besitzer Ärger bedeuten, wenn das Fahrzeug auf Kurzstrecken betrieben wird. Darüber hinaus könnte ein Volkswagen-DPF laut Beschwerde des New Yorker Generalstaatsanwalts [15] bei Normallast eine Lebensdauer von nur 50.000 Meilen haben, bevor er gewechselt werden muss, weitaus weniger als die 120.000-Meilen-Norm, die Volkswagen erfüllen musste, wodurch Volkswagen gezwungen wäre, den Verschleiß am DPF zu reduzieren.

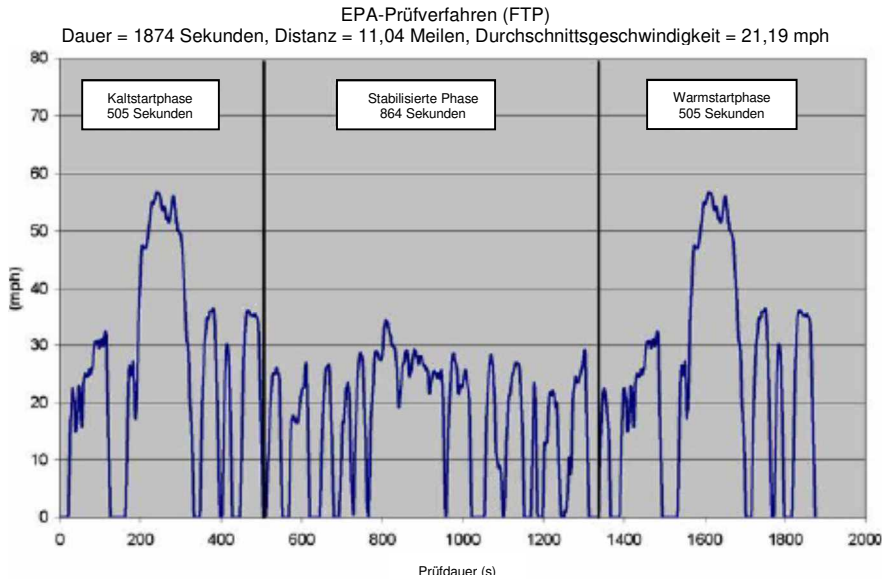


Abb. 1: Fahrzyklus nach FTP-75 (Federal Test Procedure) mit Darstellung des Geschwindigkeit/Zeit-Profils. Abbildungsquelle: EPA [20].

B. Emissionsprüfzyklen und Emissionsnormen

Ein *Emissionsprüfzyklus* definiert ein Protokoll, das reproduzier- und vergleichbare Messungen der Abgasemissionen zur Beurteilung der Emissionskonformität ermöglicht. Das Protokoll legt alle Bedingungen fest, unter denen der Motor getestet wird, einschließlich Labortemperatur und Fahrzeugzustände. Insbesondere definiert die Prüfung ein Geschwindigkeits- und Last-Profil über einen gewissen Zeitraum, mit dem ein typisches Fahrszenario simuliert wird. Abbildung 1 zeigt ein Beispiel für einen Fahrzyklus. Dieses Diagramm stellt den Prüfzyklus nach FTP-75 (Federal Test Procedure) dar, der von der EPA erstellt wurde und für die Emissionszertifizierung und die Kraftstoffverbrauchsprüfung von leichten Nutzfahrzeugen in den USA [7] angewendet wird. Der Zyklus simuliert eine Stadtfahrt mit häufigen Stopps in Verbindung mit einer Kalt- und einer Warmstart-Übergangsphase. Der Zyklus dauert 1877 Sekunden (rund 31 Minuten) und deckt eine Strecke von 11,04 Meilen (17,77 km) bei einer Durchschnittsgeschwindigkeit von 21,2 mph (34,12 km/h) ab.

Tabelle IV im Anhang enthält ein Verzeichnis der Hauptprüfzyklen, die für Abgasemissionsprüfungen von leichten Nutzfahrzeugen in den verschiedenen Regionen der Welt Anwendung finden. Neben den Stadtprüfzyklen wie FTP-75 gibt es noch Zyklen, mit denen das Fahrprofil unter verschiedenen Bedingungen simuliert wird.

Um die Konformität zu beurteilen, werden viele dieser Tests auf einem Rollenprüfstand durchgeführt, einer Apparatur, die das Fahrzeug an Ort und Stelle hält, während die Antriebsräder des Fahrzeugs gegen wechselnden Widerstand drehen können. Die Emissionen werden während des Tests gemessen und mit einer Abgasnorm verglichen, die die maximale Schadstoffmenge definiert, die während eines solchen Tests freigesetzt werden darf. In den USA werden die Abgasnormen von der EPA auf nationaler Ebene überwacht. Darüber hinaus hat Kalifornien seine eigenen Abgasnormen, die vom California Air Resources Board (CARB) definiert und durchgesetzt werden. Die kalifornischen Abgasnormen werden auch von einer Reihe anderer Staaten angewendet, die zusammen mit Kalifornien einen großen Teil des US-Marktes ausmachen, so dass sie de facto den Status einer zweiten nationalen Norm haben. In Europa werden die Abgasnormen mit Euro 1 bis Euro 6 bezeichnet, wobei Euro 6 die aktuellste Norm ist, die seit September 2014 in Kraft ist.

C. Elektronische Motorsteuerung

In einem normalen modernen Auto gibt es 70-100 elektronische Steuereinheiten [4], [8], die zum Beispiel für Bereiche wie das Human-Machine-Interface als Bestandteil des Infotainment-Systems, den Drehzahlregler, das Telematiksteuergerät oder die Bremsregelmodule verantwortlich sind. Dazu gehört auch das Motorsteuergerät (ECU), das den Betrieb des Motors regelt. Gegenstand der vorliegenden Arbeit ist das ECU Bosch EDC17, das in vielen leichten Dieselnutzfahrzeugen und in allen Fahrzeugen, die in den Volkswagen-Dieselabgasskandal verwickelt sind, eingesetzt wird. Im Kern führt das ECU einen geschlossenen Regelkreis durch regelmäßiges Auslesen der Sensorwerte, Analysieren der Steuerfunktion und Überwachung der Aktoren anhand des Steuersignals aus.

Sensoren. Um das Motorverhalten zu überwachen, ist das ECU auf eine Vielzahl von Sensormesswerten angewiesen, einschließlich Kurbelwellenposition, Luftdruck und Temperatur an verschiedenen Stellen im Ansaugtrakt, Ansaugluftmasse, Kraftstoff-, Öl- und Kühlmitteltemperatur, Fahrzeuggeschwindigkeit, Abgassauerstoffgehalt (Lambda-Sonde) sowie die Fahrerbefehle wie Gaspedalstellung, Bremspedalstellung, Tempomateinstellung und eingelegter Gang.

Steuerfunktionen. Anhand der Sensoreingangswerte führt das ECU entsprechend der Interpretation der Eingangswerte verschiedene Funktionen zur Steuerung und Beeinflussung des Verbrennungsvorgangs durch. Bei einem Dieselmotor ist der Kraftstoffeinspritzzeitpunkt einer der wichtigsten Steuerwerte, der festlegt, wann und wie lange der Kraftstoffinjektor im Motorzyklus geöffnet bleibt. Wie weiter oben erwähnt, beeinflusst der Einspritzzeitpunkt die Motorleistung, den Kraftstoffverbrauch und die Abgas-Zusammensetzung. Das ECU bestimmt außerdem, wieviel Abgas zurückgeführt und wieviel Harnstoff in den Abgasstrom eingespritzt werden sollte, um die Stickoxide zu katalysieren.

Aktoren. Das ECU nutzt die Computersteuersignale zur direkten Steuerung der verschiedenen Aktoren, vor allem der Kraftstoffeinspritzventile und der Luftsystemventile, einschließlich des AGR-Ventils.

Kommunikation. Das ECU kommuniziert auch mit anderen Systemen im Auto, um zum Beispiel das aktuelle Motordrehzahlsignal anzuzeigen oder Diagnoseleuchten zu aktivieren. Darüber hinaus werden Status-Informationen in Bezug auf das ECU über eine Schnittstelle wie das Onboard-Diagnose System (OBD II) übermittelt, zudem kann das ECU über den CAN-Bus auch mit anderen Steuereinheiten kommunizieren.

D. Geschäftsbeziehungen

Das ECU EDC17 wird von Bosch produziert und von den Autobauern, einschließlich Volkswagen und Fiat, zur Steuerung ihrer Dieselmotoren eingekauft. Die genauen Einzelheiten der Geschäftsbeziehung zwischen Bosch und seinen Kunden sind öffentlich nicht verfügbar; allerdings weisen Medienberichte, Gerichtsunterlagen [15] und die uns vorliegende Dokumentation auf folgende Grundstruktur hin: Bosch baut die ECU-Hardware und entwickelt die auf dem ECU laufende Software. Die Hersteller passen das ECU dann für jedes Fahrzeugmodell entsprechend an, indem sie charakteristische Firmware-Konstanten kalibrieren, deren Semantik in der ECU-Dokumentation erläutert ist. Wir haben keinen Nachweis dafür finden können, dass die Automobilhersteller einen der auf dem ECU laufenden Codes schreiben. Der gesamte Code, den wir im Rahmen der vorliegenden Arbeit analysiert haben, war in durch Bosch urheberrechtlich geschützten Dokumenten dokumentiert, in denen die Autobauer als vorgesehene Kunden identifiziert sind.

E. Zugehörige Arbeiten

Leider gibt es nur wenige technische Dokumentationen über Abschaltvorrichtungen, die öffentlich verfügbar sind. Domke und Lange waren die Ersten, die verschiedene technische Einblicke in die Abschaltvorrichtung gewährten, die in einem Volkswagen Sharan [9], [10] eingesetzt wurde. Wir haben auf diesen Analyseergebnissen aufbauend eine ähnliche Methodik angewandt, um Abschaltvorrichtungen zu identifizieren. In dem Beschwerdeverfahren des New Yorker Generalstaatsanwalts gegen die Volkswagen AG [15] sind zwar zahlreiche allgemeine Einblicke in Abschaltvorrichtungen enthalten, technische Einzelheiten liefert es jedoch nicht. Derzeit wird in Europa gegen Fiat Chrysler Automobiles (FCA) ermittelt [17], und nach bestem Wissen und Gewissen sind wir die ersten, die dokumentieren, wie diese Abschaltvorrichtung realisiert wird.

III. DATENSATZ

Im vorliegenden Paper konzentrieren wir uns auf das von Bosch hergestellte ECU EDC17. Dieses Dieselmotor-ECU wurde sowohl in den im Volkswagen-Abgasskandal verwickelten Fahrzeugen als auch im Fiat 500X eingesetzt. Wir stützen uns auf drei Datenquellen für unsere Analyse der ECUs und der betroffenen Fahrzeuge, die wir nachstehend beschreiben.

A. Funktionsrahmen

Der Funktionsrahmen dokumentiert das funktionale Verhalten einer bestimmten ECU-Firmwareversion. Der Funktionsrahmen beschreibt jede funktionale Softwareeinheit des ECU mithilfe einer formalen Blockdiagrammsprache, die dessen Ein-/Ausgabeverhalten in Verbindung mit einigen zusätzlichen erläuternden Textinhalten konkret spezifiziert. Das Blockdiagramm und die Textdokumentation enthalten auch die von der funktionalen Einheit verwendeten Variablen und Kalibrierkonstanten. Im Bosch-Funktionsrahmen sind die skalaren Kalibrierkonstanten durch das Suffix „_C“, die eindimensionalen Array-Konstanten durch das Suffix „_CA“ und die mehrdimensionalen Arrays durch das Suffix „_MAP“ gekennzeichnet. Des Weiteren wird bei Kurvendefinitionen das Suffix „_CUR“ verwendet.

Funktionsrahmen stehen normalerweise nicht öffentlich zur Verfügung, viele davon finden jedoch ihren Weg in die automobile Motortuninggemeinde. Alle Funktionsrahmen, die bei dieser Arbeit verwendet wurden, stammen von diesen Tuner-Websites. Alle im vorliegenden Paper enthaltenen Zahlen wurden aus diesen öffentlich bereits verfügbaren Funktionsrahmen abgeleitet.

Authentizität. Da wir die Funktionsrahmen nicht direkt vom ECU-Hersteller (Bosch) bekommen haben, können wir uns ihrer Echtheit nicht absolut sicher sein. Trotzdem tragen alle Funktionsrahmen, die in dieser Arbeit verwendet wurden, den Urheberrechtshinweis der „Robert Bosch GmbH“ und weisen keine Anzeichen für eine Änderung durch Dritte auf. In der Tat haben wir keine Funktionsrahmen vorgefunden, auf denen etwaige Anzeichen für inhaltliche Manipulation zu erkennen sind. Wir haben zudem explizit verifiziert, dass die zentralen Funktionselemente, wie die in Teil IV-A beschriebene „akustische Volkswagen-Bedingung“, dem Code in der Firmware entsprechen.

B. A2L- und OLS-Dateien

Die Automobilindustrie verwendet das Dateiformat ASAM MCD-2 MC [1] , allgemein als A2L bezeichnet, um die Elemente eines Firmware-Image zu übermitteln, die ein Fahrzeughersteller im Kalibrierprozess modifizieren muss. Im Allgemeinen ist eine .a21-Datei mit einer .map oder .pdb-Datei vergleichbar, die Entwickler auf der Linux- bzw. Windows-Plattform verwenden. Während alle diese Dateitypen die Debugging-Symbole bestimmten Adressen zuordnen, kann eine .a21-Datei außerdem Kontextinformationen über die bloßen Symbolnamen hinaus bereitstellen. Das Format wird entwickelt, um „…automobilspezifische Verfahren und Arbeitsmethoden zu unterstützen“ [1]. Dementsprechend können zusätzliche Metadaten, die zur Beschreibung einer Adresse (z. B. eine ECU-Variable) verwendet werden, Achsenbeschreibungen für Lookup-Tabellen, Informationen über die Byte-Reihenfolge oder Einheitenumrechnungsformeln enthalten. Ein Beispiel ist in Verzeichnis 1 im Anhang enthalten.

Da .a21-Dateien viele Einzelheiten und Einblicke zu einem bestimmten ECU enthalten, sind sie normalerweise nur für diejenigen verfügbar, die im Bereich der Motorenentwicklung, Kalibrierung und Wartung tätig sind. Allerdings bekommen auch Autotuning-Enthusiasten diese Dateien regelmäßig in die Hände und handeln damit in Online-Foren. Um die innere Funktionsweise bestimmter ECU-Firmware-Images genauer zu verstehen, haben wir uns Zugriff auf diese Dateien beschafft. Konnten wir zu einem bestimmten Firmware-Image keine .a21-Datei bekommen, haben wir uns nur auf den Binär-Code konzentriert und uns die Einblicke zunutze gemacht, die wir aus ähnlichen ECUs gewonnen haben, um unsere Analyse zu starten.

In einigen Fällen haben wir uns auf OLS-Dateien gestützt, ein von der WinOLS-Software genutztes Anwendungsformat, um Konfigurationswerte in der Firmware zu ändern. Das OLS-Format enthält sowohl ein Firmware-Image als auch Elemente der A2L-Datei, mit der Kalibrierkonstanten hinzugefügt werden.

Authentizität. Wie schon im Fall der Funktionsrahmen haben wir die in dieser Arbeit verwendeten A2L-Dateien weder von Bosch noch vom Autobauer bekommen, daher können wir nicht mit absoluter Sicherheit für deren Echtheit garantieren. Jede A2L-Datei ist mit einem bestimmten Firmware-Image paarweise angeordnet; wir haben deren Übereinstimmung bestätigt, bevor wir mithilfe der A2L die Werte aus dem Image extrahiert haben. Wir haben die A2L zu Rate gezogen, um die Variablen und Konstanten in dem aus der Firmware extrahierten Code zu identifizieren, und den Kontext untersucht, in dem ein Wert demzufolge als eine Art Plausibilitätsprüfung diente.

C. Firmware-Images

Wir haben Firmware-Images zudem von verschiedenen Quellen erhalten. Ähnlich den .a21-Dateien kursieren in der Autotuninggemeinde auch Firmware-Images. Wir haben von der Tuner-Gemeinde mehrere Images erhalten. Außerdem haben wir Images über das *erWin*-Portal („electronic repair and workshop information“) beschafft, einer von Volkswagen betriebenen Plattform, die KFZ-Werkstätten Zugang zu offiziellen Firmware-Images bietet. Das Portal hält Archive mit Firmware-Updates bis zu einem bestimmten Datum bereit. Jedes Image ist nach seiner Software-Teilenummer und Revision benannt, anhand derer wir es eindeutig identifizieren können. Der Zeitstempel entspricht in etwa dem Erscheinungsdatum der Firmware.

Leider enthalten die Images keine zusätzlichen Metadaten, wie das tatsächliche Modell, in dem die Firmware eingesetzt wird. Wir haben mithilfe der Online-Portale von Anbietern für KFZ-Zubehörteile bestimmt, in welchen Fahrzeugen ein Firmware-Image eingesetzt wurde.

Authentizität. Die Firmware-Daten für VW, Audi, Seat und Skoda stammen vom *erWin*-Portal, das von Volkswagen betrieben wird. Das neueste Image datiert auf den 11. Oktober 2016. Außerdem haben wir Images der Volkswagen Group aus 2009-2010 von verschiedenen Online-Quellen bezogen. Dabei haben wir nur die Images berücksichtigt, bei denen es uns aufgrund der *Freigabescheine* gestattet war, die Angaben über Erscheinungsdatum und Fahrzeugmodell zu entnehmen. Die OLS-Datei für den Fiat 500X erhielten wir von einer Tuning-Website. Diese wurde uns als (unmodifiziertes) Original-Image verkauft. Unsere wesentlichen Erkenntnisse anhand dieser OLS-Datei stimmen mit den Prüfergebnissen des deutschen KBA überein [22].

IV. ABSCHALTVORRICHTUNGEN

Eine *Abschaltvorrichtung* ist ein Mechanismus, der dafür sorgt, dass sich ein Fahrzeug während einer Abgasprüfung anders als auf der Straße[1] verhält. Konzeptionell hat eine Abschaltvorrichtung zwei Komponenten:

- **Überwachung**. Entscheidung, ob die festgestellten Bedingungen eine Abgasprüfung *ausschließen*, und
- **Modifizierung**. Veränderung des Fahrzeugverhaltens, sofern es keiner Prüfung unterzogen wird.

Abschaltvorrichtungen nutzen eine Reihe externer und interner Variablen, um zu erkennen, dass eine Prüfung stattfindet. Zwischen 1991 und 1995 zum Beispiel machte sich General Motors die Tatsache zunutze, dass die Klimaanlage bei seinen Cadillac-Fahrzeugen eingeschaltet wurde, um einen Prüfzyklus auszuschließen – zu dieser Zeit wurde die Abgasprüfung bei abgeschalteter Klimaanlage durchgeführt – und das Luft-Kraftstoffgemisch anzureichern, um das Problem des absterbenden Motors zu beheben, womit aber auch die CO-Emissionsgrenzwerte überschritten wurden [14]. General Motors wurde zu 11 Mio. US-Dollar Geldstrafe verurteilt und musste alle betroffenen Fahrzeuge zurückrufen.

Min.	Max.	Einheit	Signal	Beschreibung
-50	140	°C	InjCrv_tClntEngNs_mp	Kühlmitteltemperatur
-50	140	°C	FuelT_t	Kraftstofftemperatur
-50	140	°C	Oil_tSwmp	Öltemperatur
795	-	hPa	EnvP_p	Atmosphärendruck
true			StSys_stStrt	Motorstart

TABELLE I: Ausgangszustand zur Aktivierung der Akustikbedingung in der EDC17C54-Firmware. Die Parameter wurden der Firmware-Teilenummer 03L906012F entnommen. Wenn alle Bedingungen erfüllt sind, wird das für das äußere (oberste) Flipflop in Abbildung 2 *gesetzte* Signal bestätigt.

Wie das Cadillac-Beispiel vermuten lässt, muss das Überwachungselement einer Abschaltvorrichtung nicht perfekt sein, solange dessen Fehler einseitig ist. Ähnlich der Cadillac-Vorrichtung setzen die von uns vorgefundenen Abschaltvorrichtungen voraus, dass das Fahrzeug einer Prüfung unterzogen wird, es sei denn, sie können eine laufende Prüfung aufgrund bestimmter interner oder externer Variablen *ausschließen*. In diesem Fall kann das Fahrzeug, wenn das Überwachungselement signalisiert, dass die festgestellten Variablen mit keinem bekannten Prüfzyklus übereinstimmen, in einen vom Hersteller für reale Fahrbedingungen favorisierten Betriebsmodus wechseln, anstatt in einen sauberen Modus, der zum Bestehen der Abgasprüfung erforderlich ist.

Im restlichen Teil dieses Absatzes beschreiben wir die Abschaltvorrichtungen, die von Volkswagen und Fiat zur Umgehung der Abgasprüfung eingesetzt wurden, sowie deren Einfluss auf das Fahrzeugverhalten. Unsere Beschreibung basiert auf dem Funktionsrahmen für das ECU, auf Reverse Engineering der Firmware und auf öffentlich zugänglichen Informationen, vor allem die vom State of New York gegen Volkswagen und ihre US-Tochtergesellschaften eingereichte Beschwerde [15].

A. Die Volkswagen-Vorrichtung: Prüfungserkennung

Die Volkswagen-Abschaltvorrichtung ist eine kontinuierlich weiterentwickelte Vorrichtungsfamilie. Alle Vorgänge sind um einen einzelnen Zustandsüberwachungsblock, der feststellt, ob das Fahrzeug einer Prüfung unterzogen wird, und die Bereiche in den emissionsrelevanten ECU-Modulen herum aufgebaut, bei denen das Ergebnis dieser Feststellung das Verhalten des Moduls beeinflussen kann. Das Überwachungselement der Volkswagen-Vorrichtung ist in einem Funktionsblock verborgen, der den Status der *kundenspezifischen Akustikbedingung* berechnet (*Kunde* bezieht sich hierbei auf den Autobauer, also Volkswagen). Das Ergebnis der Berechnung wird durch das Signal / die Variable InjCrv_stNsCharCor (kurz stNsCharCor) dargestellt. Dieses Signal wird dann an zahlreichen Stellen im ECU eingesetzt, um das Verhalten des Motors zu ändern. Abbildung 2 zeigt den Logik-Block, der für die Berechnung der Akustikbedingung zuständig ist (die Abbildung stammt aus dem von Bosch aufgestellten Funktionsreferenzrahmen). Der Wert stNsCharCor = 0 bedeutet, dass das ECU für sich selbst den normalen Fahrbetriebsmodus annimmt, während stNsCharCor = 1 den (emissionskonformen) Prüfmodus indiziert.

Aktivierungsbedingungen. Der Status der Akustikbedingung ist im obersten Flipflop in der Abbildung unter Ziffer ① gespeichert. Das für das Flipflop *gesetzte* Signal hat den Wert true, wenn aus fünf Bedingungen alle zutreffen. Diese Bedingungen sind in Tabelle I enthalten. Zu beachten ist hier, dass die letzte Bedingung, Motorstart, nur dann zutrifft, wenn der Motor startet, und während des normalen Betriebs nicht zutrifft. Wenn der Motor im normalen Modus läuft (d. h. er wurde nicht erst vor kurzem gestartet), er an einem bestimmten Punkt eine Geschwindigkeit von beispielsweise 9,5 km/h überschritten hat, und Druck und Temperatur den vorgenannten Grenzen entsprechen, fährt die Funktion mit der eigentlichen Zyklusprüfung fort. Ansonsten bleibt der Motor im gleichen Modus. Der Effekt davon ist, dass die Akustikbedingung nur dann gesetzt werden kann, wenn die Kühlmitteltemperatur, Kraftstofftemperatur, Öltemperatur und der Atmosphärendruck sich innerhalb der vorgeschriebenen Grenzwerte bewegen, wenn das Fahrzeug gestartet wird ②. Befindet sich einer der vier Parameter außerhalb des erforderlichen Bereichs, wird eine laufende Emissionsprüfung ausgeschlossen und die Akustikbedingung wird nie aktiviert. Allerdings müssen wir feststellen, dass diese Bedingungen sowohl in Prüf- als auch in Realszenarien leicht erfüllt sind.

Wenn die Akustikbedingung beim Starten gesetzt wird, kann sie durch die Erfüllung der verschiedenen Bedingungen, die eine Prüfung ausschließen, gelöscht werden. Wir bezeichnen dies als *Deaktivierungs*bedingungen. Wird eine dieser Bedingungen erfüllt, wird das innere Flipflop gesetzt ③. Die Ausgangsgröße des inneren Flipflop bestätigt das *Reset*-Signal des äußeren Flipflop, so dass die Variable der Akustikbedingung tNsCharCor auf Null gesetzt wird. Es gibt vier Deaktivierungsbedingungen, von denen jede, sofern sie zutrifft, das innere Flipflop setzt, das wiederum tNsCharCor auf Null setzt und damit indiziert, dass sich das Fahrzeug im normalen Fahrbetriebsmodus befindet.

[1] Genauer gesamt definiert der US Code of Federal Regulations eine *Abschaltvorrichtung* als „eine zusätzliche Emissionsminderungsvorrichtung (AECD), die die Wirksamkeit der Abgasreinigungsanlage unter Bedingungen reduziert, die vernünftigerweise bei normalem Fahrzeugbetrieb und Gebrauch zu erwarten sind, es sei denn: (1) diese Bedingungen sind im Wesentlichen im Bundesprüfverfahren enthalten; (2) die Notwendigkeit einer AECD ist im Hinblick auf den Schutz des Fahrzeugs vor einem Schaden oder Unfall gerechtfertigt; (3) die AECD geht nicht über die Anforderungen des Motorstarts hinaus; oder (4) die AECD gilt nur für Rettungsfahrzeuge…“ (40 CFR § 86.1803-01). Die europäischen Bestimmungen folgen einer sehr ähnlichen Definition.

Deaktivierungsbedingungen. Es gibt vier Deaktivierungsbedingungen ④. Die erste deaktiviert die Akustikbedingung, wenn der Motor gestartet wurde und eine konfigurierbare Zeitspanne InjCrv_tiNsAppVal_C verstrichen ist, seitdem die Gaspedalstellung erstmals einen konfigurierbaren Grenzwert InjCrv_rNsAppVal_C überschritten hat. Die zweite deaktiviert die Akustikbedingung, wenn der Motorumdrehungszähler einen konfigurierbaren Grenzwert InjCrv_ctNsStrtExtd_C überschritten hat. Die dritte Deaktivierungsbedingung wird, wenn die Akustikbedingung unterdrückt ist, nie ausgelöst.

Bis etwa Mai 2007 gab es nur drei der oben beschriebenen Deaktivierungsbedingungen. Bei den uns vorliegenden Firmware-Images erscheint die vierte Bedingung erstmals in einem Firmware-Image aus Mai 2007 für EDC17CP04 P 617. Sie beginnt mit der Bestimmung einer Zeit- und Distanzmessung. Die Zeitmessung, nennen wir sie *t*, wird bestimmt, indem die Zeit gemessen wird, seitdem das Fahrzeug erstmals eine konfigurierbare Geschwindigkeit InjCrv_vThres_C überschritten hat. Die Distanzmessung entspricht der Strecke im aktuellen Fahrzyklus, nennen wir sie *d*.

Prüfzykluskurven. Die Logik der Akustikbedingung berechnet anhand von zwei linear interpolierten Kurven ein Punktepaar d_{lower} und d_{upper}. Diese Kurven, die mithilfe einer geringen Anzahl von Punkten eine Funktion *t* definieren, können vom Hersteller konfiguriert werden. In diesem Fall gibt es sieben Kurvenpaare, aus denen sich sieben Wertepaare d_{lower} und d_{upper} ergeben, die für den aktuellen Wert *t* berechnet werden. Ist *d* irgendwann kleiner als d_{lower} oder größer als d_{upper}, wird das dem Kurvenpaar entsprechende Flipflop gesetzt und bleibt für unbegrenzte Zeit gesetzt ⑤.

Die Ausgangsgröße dieses Flipflop gibt an, dass das Fahrzeug von dem vorgeschriebenen, vom Kurvenpaar definierten Zeit/Distanz-Profil abgewichen ist. Dementsprechend beschreiben die Kurven eine obere und untere Grenze über die erfasste Distanz. Das Flipflop lässt zu, dass sich die Logik diesen Grenzbereich merkt, und der Status der Flipflops gibt zu jedem beliebigen Zeitpunkt an, ob das Fahrzeug bisher in dem vorgeschriebenen Zeit/Distanz-Profil, wie vom Kurvenpaar definiert, geblieben ist. Werden alle sieben Flipflops gesetzt, hat das Fahrzeug das Profil zu jeder dieser Kurven mindestens einmal seit dem Start verlassen. Wenn das passiert, wird die Akustikbedingung gelöscht.

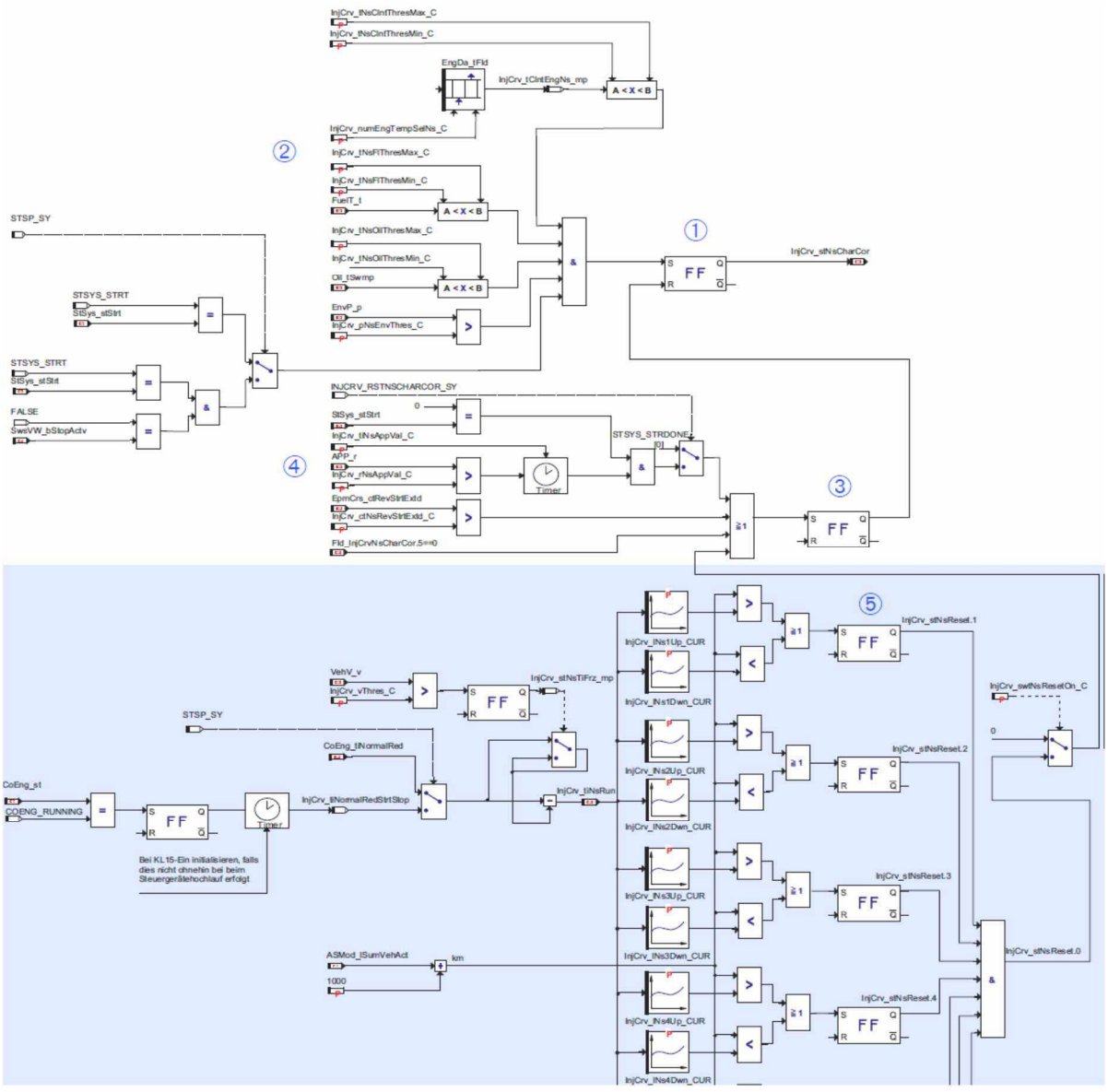


Abb. 2: Aktivierungslogik für die Akustikbedingung aus dem Funktionsrahmen EDC17C54 P 874 für z. B. VW Passat vom Dezember 2009. Der hellblau schattierte Bereich deaktiviert die sogenannte „kundenspezifische Akustikbedingung", wenn die zeitabhängig gefahrene Distanz keinem der 7 möglichen Prüfzyklusgeschwindigkeitsprofilen entspricht. Der hellblau schattierte Bereich erscheint in keinem Funktionsrahmen vor EDC17C04 P 617 vom Mai 2007. Copyright der Robert Bosch GmbH. Das Diagramm ist bei der vierten Prüfkurve abgeschnitten, erstreckt sich nach unten bis sieben. Die blaue Schattierung und die Ziffern ① bis ⑤ wurden von den Autoren ergänzt.

In der von uns untersuchten Firmware werden diese Kurven verwendet, um das genaue Zeit/Distanz-Profil bekannter Abgasprüfungen festzulegen. Im Allgemeinen stellen wir fest, dass die Anzahl der Profile mit der Zeit zugenommen hat. Wie in Tabelle II dargestellt, ist die Anzahl der untersuchten Kurven von 0 in EDC17CP04 P 531 auf 7 in EDC17CP44 P 859 gestiegen.

Abbildung 3 zeigt mehrere Kurvenpaare, die in der Firmware eines EDC17C54 ECU (Software-Teilenummer 03L906012, Revision 7444; restliche festgestellte Kurven in Abbildung 14 im Anhang) gefunden wurden. Der Bereich außerhalb der von den Kurven definierten oberen und unteren Grenzen d_{lower} und d_{upper} ist abschattiert. Wenn der berechnete Zeit- und Distanzwert (t, d) in diesen Graubereich fällt, gilt die Prüfung als ausgeschlossen, und das entsprechende Flipflop wird gesetzt. Zusätzlich zu den Grenzwerten haben wir die in Tabelle IV enthaltenen Prüfzyklen bekannter Abgasprüfungen eingetragen. Die Prüfzyklen, die dem Profil entsprechen, sind mit dicken Linien dargestellt; alle anderen mit dünnen Linien. Wie unsere Ergebnisse zeigen, kommen viele der konfigurierten Grenzen einem bekannten Prüfzyklus recht nahe. Vor allem Profil 1 entspricht bis km 4,2 dem Prüfzyklus nach FTP-75, und Profil 5 bis km 16,1 dem Prüfzyklus nach HWFET (in der Abbildung nicht ganz dargestellt).

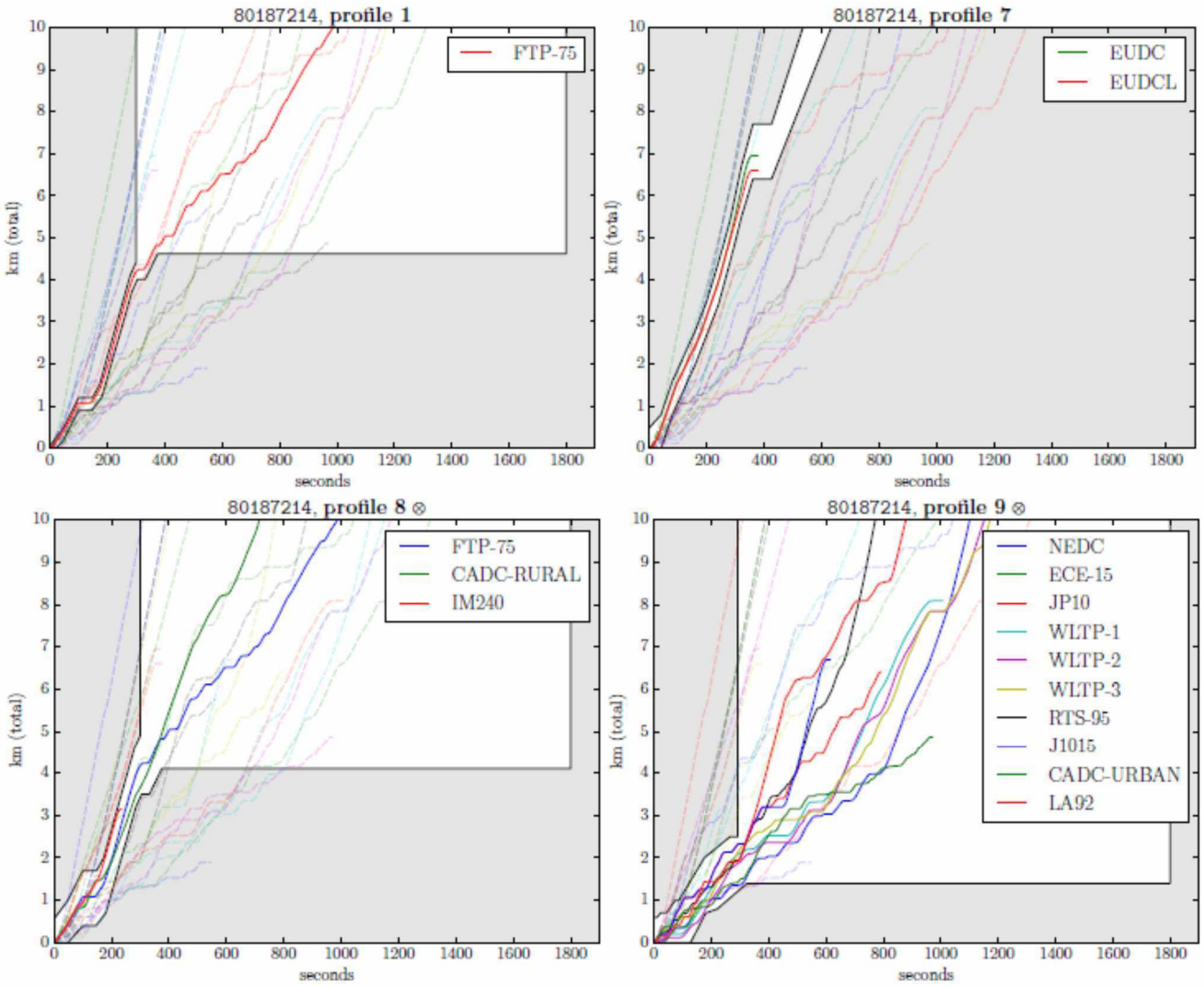


Abb. 3: Auswahl von Kurvenkontrolluntersuchungen anhand verschiedener Abgasprüfzyklen in der Firmware für einen VW Passat, Freigabe 12/2014 (EDC17C54, Software-Teilenummer 03L906012, Revision 7444). Der Bereich, in dem die Software meldet, dass das Fahrprofil entsprechend übereinstimmt, ist weiß markiert. Wie aus den Graphen hervorgeht, folgt dieser Bereich dem Prüfzyklus tendenziell genau. In der Legende sind die bekannten übereinstimmenden Prüfzyklen aufgeführt. ⊗ markiert eine zusätzliche Lenkradkontrolle. Abbildung 14 im Anhang enthält die restlichen Kurven.

Lenkradkontrollen. Ab 2009 wurde die Anzahl der Profilkontrollen in der in Volkswagen-Fahrzeugen eingesetzten EDC-Firmware von 7 auf 10 erhöht. Wie bereits angemerkt, wurden die in Abbildung 3 dargestellten Profile aus einem EDC17C54-Firmwareimage, VW-Teilenummer 03L906012 extrahiert, das 10 Profile umfasst, von denen vier in der Abbildung dargestellt sind (die in Abbildung 2 dargestellte Akustikbedingung, die aus einem älteren EDC17C54-Funktionsrahmen stammt, zeigt nur 7 Profile).

Beachten Sie bitte, dass die Profile 8 und 9 deutlich ungenauer sind, als die Profile 1 und 7. Tatsächlich stimmt Profil 9 mit insgesamt 10 bekannten Abgasprüfzyklen überein. Neben der Überprüfung der in Abbildung 3 dargestellten Zeit/Distanz-Relation wurde in den Profilen 8, 9 und 10 zusätzlich eine Lenkradwinkelkontrolle berücksichtigt: neben der Abweichung von einem vorgeschriebenen Zeit/Distanz-Profil würde das den Profilen 8, 9 und 10 entsprechende Flipflop zurückgesetzt werden, wenn der Lenkradwinkel um mehr als 20° von der Neutralstellung abweicht. Leider konnten wir keinen Funktionsrahmen beschaffen, der diese erweiterte Akustikbedingung enthält. Der folgende Code stellt unsere Rekonstruktion der Logik dar, anhand derer bestimmt wird, ob die Akustikbedingung bei einer Lenkradwinkelabweichung gelöscht werden soll.

```
if (-20 /* deg */ < steeringWheelAngle &&
    steeringWheelAngle < 20 /* deg */) {
    lastCheckTime = 0;
    cancelCondition = false;
} else {
    if (lastCheckTime < 1000000 /* microsec */) {
        lastCheckTime = lastCheckTime + dT;
        cancelCondition = false;
    } else
        cancelCondition = true;
}
```

In der aktualisierten Firmware dient das Signal cancelCondition, wie oben berechnet, als dritter Eingabewert für die ≥1 Gates, die zu den dem jeweiligen Profil entsprechenden Flipflops führen.

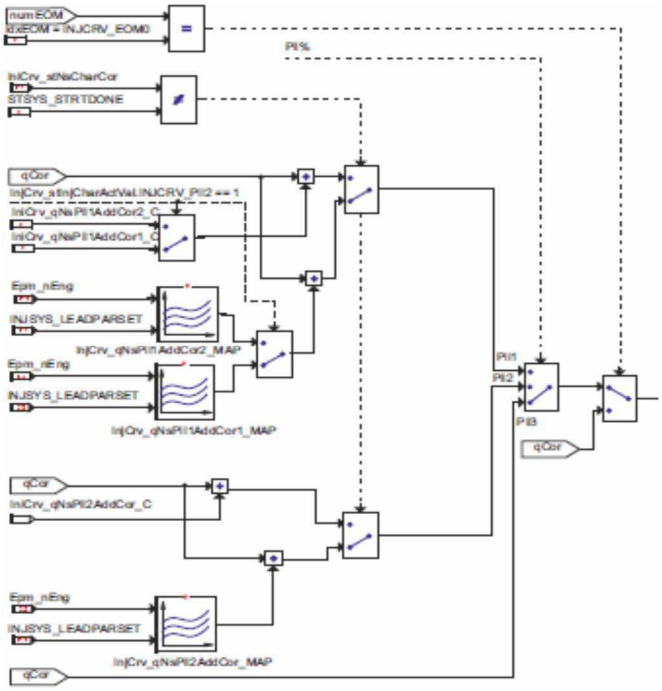


Abb. 4: Akustikbedingung (Signal InjCrv_stNsCharCor), die zur Änderung der gewünschten Einspritzmengenkorrektur qCor herangezogen wird. Aus dem Funktionsrahmen EDC17C54 P874. Copyright der Robert Bosch GmbH.

Wenn die vorstehend kodierte, komplexe Prüfzyklus-Detektionslogik die Akustikbedingung auf 1 setzt, finden mehrere Veränderungen im Fahrzeugverhalten statt. Diese Veränderungen werden durch den Wert der Akustikbedingungsvariablen stNsCharCor bewirkt, um zwischen den konfigurierbaren Variablen bzw. Parametern umzuschalten, so dass das Fahrzeug mit einem Kalibrierwerte-Set im normalen Fahrmodus und mit einem anderen Set im Prüfmodus arbeiten kann, als würden sich zwei verschiedene Persönlichkeiten beim Steuern des Fahrzeugs abwechseln. Als nächstes beschreiben wir die beiden gegensätzlichen Persönlichkeiten, die sich je nach Status der Akustikbedingung ergeben.

B. Die Volkswagen-Vorrichtung: Einfluss auf die Einspritzung

Wie in Absatz II-A beschrieben, wird der Betrieb eines Dieselmotors über den Kraftstoffeinspritzzeitpunkt gesteuert. Der Beginn und die Dauer der Einspritzungen wirken sich nicht nur auf die Motorleistung sondern auch auf die Abgasemissionen aus. Auf ihrer Bezeichnung und ersten Verwendung basierend wurde die Akustikbedingung eingeleitet, um das Motoreinspritzverhalten zu ändern [15]. Wir identifizierten mehrere Bereiche in der Firmware, die wir manuell analysiert haben, in denen die Akustikbedingung das Kraftstoffeinspritzverhalten modifizieren kann. Hier beschreiben wir, wie die Akustikbedingung eingesetzt werden kann, um die Einspritzmenge anzupassen.

Abbildung 4 zeigt, wie die (zusätzliche) Kraftstoffeinspritzmengenkorrektur (qCor) durch die Akustikbedingung modifiziert wird. Trifft die Akustikbedingung zu (unter Prüfbedingung), wird qCor durch Ergänzung einer Konstante (InjCrv_qNsPil1AddCor{1,2}_C oder InjCrv_qNsPil2AddCor_C) modifiziert. Ansonsten wird qCor durch Ergänzung eines Wertes modifiziert, der anhand der Motordrehzahl berechnet wird (Epm_nEng). Der Funktionsrahmen beschreibt diesen Logikblock als „*Berechnung zusätzlicher (kundenspezifischer) Korrekturen für die Voreinspritzungen*“.

C. Die Volkswagen-Vorrichtung: Einfluss auf die AGR

Wie bereits angemerkt, ist die Abgasrückführung (AGR) ein sehr effektives Mittel zur Reduzierung der NO_X-Menge im Abgas. Leider bewirkt der günstige Effekt auf das NO_X das Gegenteil bei den Feinstaubpartikeln: die Reduzierung der NO_X-Emissionen durch die Erhöhung der Menge an zurückgeführten Abgasen führt zu einer Erhöhung der Rußmenge im Abgas. Dadurch steigt wiederum die Belastung für den Dieselpartikelfilter (DPF), der zur Senkung der Rußemissionen eingesetzt wird. Die Akustikbedingung kann auch zur Veränderung der Menge an zurückgeführten Abgasen herangezogen werden (siehe Abbildung 11 im Anhang). Der in der

Abbildung dargestellte Logikblock wird zur Berechnung von mDesVal1Cor verwendet, ein Korrekturwert in Bezug auf die insgesamt gewünschte Luftmenge. Die Korrektur kann, auf einem konfigurierbaren Parameter basierend, additiv oder multiplikativ auf den Basiswert angewendet werden, um den gewünschten Luftmassenwert zu erreichen (diese Berechnung ist in der Abbildung nicht dargestellt).

D. Die Fiat 500X-Vorrichtung

Der Volkswagen-Abgasskandal hat die Aufmerksamkeit nicht nur auf Volkswagen selbst gelenkt, sondern auch auf andere Autobauer von Dieselfahrzeugen. Darunter war auch Fiat Chrysler Automobiles (FCA), die am 02. Februar 2016 in einer Pressemitteilung erklärten: „In FCA-Dieselfahrzeugen gibt es keinen Mechanismus, der entweder erkennt, dass das Fahrzeug einem Rollenprüfstandstest im Labor unterzogen wird, oder der eine Funktion aktiviert, wodurch die Abgasreinigung ausschließlich unter Laborprüfungsbedingungen arbeitet. […] Die im Einklang mit dem nach europäischem Recht (NEDC) einzig vorgeschriebenen Prüfzyklus getesteten [FCA-Dieselfahrzeuge] erfüllen die gesetzlichen Grenzwerte und damit die maßgeblichen gesetzlichen Vorschriften“ [11]. Am 09. Februar 2016, eine Woche nach Veröffentlichung der FCA-Pressemitteilung, wurde der Konzern von der deutschen Umweltschutzorganisation Deutsche Umwelthilfe (DUH) wegen Überschreitung der Emissionsgrenzwerte bei seinem Crossover-SUV Fiat 500X mit Fiat 2-Liter-MultiJet-II-Dieselmotor angeklagt. Die DUH verwendete für die Abgasprüfung einen Rollenprüfstand. Zum Zeitpunkt der vorliegenden Arbeit hat FCA nicht bestätigt, dass ihr Fahrzeug über eine Abschaltvorrichtung verfügt.

Wie bei anderen Fahrzeugen in dieser Studie wird auch beim Dieselmotor des Fiat 500X das Bosch EDC17 ECU eingesetzt. Dessen Abgasnachbehandlungssystem umfasst einen NO_X-Speicherkatalysator (NSK) und einen Dieselpartikelfilter (DPF). Um die Klagebehauptung zu untersuchen, haben wir uns einen Fiat-500X-Funktionsrahmen (EDC17C69 P1264) und das Firmware-Image (55265162) besorgt. Wir haben beides auf ein Vorhandensein der Volkswagen-Abschaltvorrichtung überprüft, fanden jedoch weder eine namentliche Erwähnung der Akustikbedingung im Funktionsrahmen noch einen Nachweis für die Kurvenkontrolllogik im Firmware-Image.

Allerdings fanden wir heraus, dass im Fiat 500X ein Vorgang eingesetzt wird, der auf eine Abschaltvorrichtung in der Steuerungslogik der NSK-Regeneration hinausläuft. Im Gegensatz zur Volkswagen-Abschaltvorrichtung setzt der FCA-Mechanismus nur auf die zeitliche Komponente *und reduziert die Frequenz der NSK-Regenerationen 26 Minuten 40 Sekunden nach dem Motorstart*. Wie bereits erwähnt, besteht die Hauptaufgabe des NSK (Absatz II-A) in der Reduzierung der NO_X-Emissionen, indem NO_2 während der Lastphase (die zwischen 30 bis 300 Sekunden dauert) im Katalysator abgefangen und während der Regenerationsphase (die zwischen 2 und 10 Sekunden dauert) ausgespült wird. Die Regeneration reduziert die Kraftstoffeffizienz und erhöht die Belastung für den DPF. Durch die Reduzierung der NSK-Regenerationsfrequenz kann ein Hersteller die Kraftstoffeffizienz verbessern und die Lebensdauer des DPF erhöhen, allerdings zu Lasten erhöhter NO_X-Emissionen.

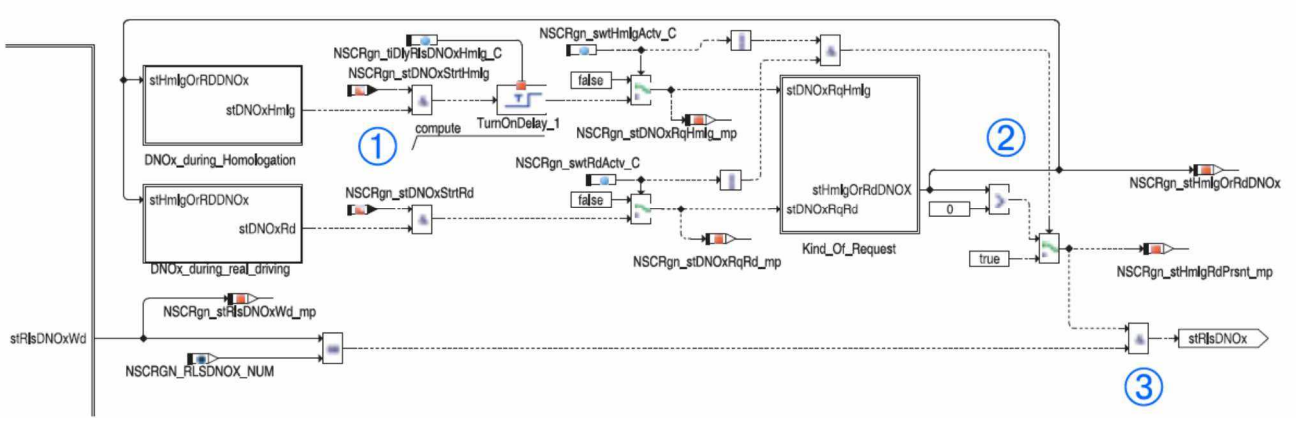


Abb. 5: Freigabelogik für die NO_X-Regeneration, bei der die Start- und Freigabesignale aus der Homologations- und der Realfahrbetriebslogik zur Berechnung des einzelnen Regenerations-Freigabesignals (stRlsDNOx) miteinander verknüpft werden. Die Bedarfs- und Freigabebedingungen werden für die Homologations- und die Realfahrbetriebslogik separat berechnet ①. Die Ausgangsgröße des (Kind of Request)-Blocks ist ungleich Null, wenn entweder die Homologations- oder die Realfahrbetriebssignale den Wert true haben②. Das endgültige Freigabesignal (stRlsDNOx) wird erst bestätigt ③, wenn entweder die Homologations- oder die Realfahrbetriebs-Freigabesignale den Wert true haben. Die blauen Ziffern ① bis ③ wurden von den Autoren ergänzt. Aus dem Funktionsrahmen EDC17C69 P 1264 für Fiat 500X. Copyright der Robert Bosch GmbH.

Im ECU des Fiat 500X ist die Logik zur Steuerung der NSK-Regeneration in eine *Bedarfslogik* und eine *Freigabelogik* unterteilt. Die Erstgenannte bestimmt, wann die NSK-Regeneration stattfinden soll, während Letztere Einschränkungen festlegt, wann die Regeneration eingeleitet werden darf. Damit die Regeneration eingeleitet werden kann, muss die Bedarfslogik die Regeneration durch Bestätigung des NSCRgn_stDNOxStrt-Signals anfordern, während das NSCRgn_stRlsDNOx-Freigabesignal durch die Freigabelogik bestätigt werden muss (DNOx bezieht sich auf die NSK-Regeneration, die das gespeicherte NOx aus dem Katalysator spült). In dem von uns untersuchten EDC17C69-Funktionsrahmen war sowohl die Bedarfs- als auch die Freigabelogik in zwei Parallelblöcken *dupliziert*. Das erste Paar der Bedarfs- und Freigabeblöcke gilt für einen „Homologationszyklus“, während das zweite Paar für einen „Realfahrbetriebszyklus“ gilt (*Homologation* bezieht sich auf den Vorgang bzw. Akt zur Erteilung der Zulassung durch eine amtliche Behörde, zum Beispiel die Verkaufszulassung für ein Fahrzeug in einem bestimmten Land. Die Begriffe „Homologation“ und „Realfahrbetrieb“ sind dem EDC17C69-Funktionsrahmen entnommen). Die Bezeichnungen der in der Homologationslogik verwendeten Signale und Logikblöcke beinhalten das Kürzel Hmlg in ihrer Bezeichnung, während in den in der Realfahrbetriebslogik verwendeten Bezeichnungen das Kürzel Rd verwendet wird. Die Bedarfslogik für die Homologations- und die Realfahrbetriebsblöcke ist sehr ähnlich und bestimmt anhand der geschätzten Gesamt-NOx-Last, der Katalysatortemperatur und anderer Variablen, wann die Regeneration aktiviert wird. Die Homologations- und die Realfahrbetriebslogik greifen allerdings auf andere Kalibrierungsparameter zurück und ermöglichen dem Hersteller damit, völlig unterschiedliche Modelle für den Prüfzyklus und den Realfahrbetrieb zu liefern.

Sowohl die Homologations- als auch die Realfahrbetriebslogikblöcke können eine Regeneration anfordern. In ähnlicher Weise wird auch das Freigabesignal von zwei parallelen Logikblöcken gesteuert. Abbildung 5 zeigt, wie die Signale zusammengeführt

werden. Das Homologationsfreigabesignal wird durch AND-Verknüpfung mit dem Homologationsbedarfssignal verbunden, ebenso die Realfahrbetriebsbedarfs- und Freigabesignale (in Abbildung 5 mit ① gekennzeichnet). Das Homologationsfreigabesignal wird durch den Befehl NSCRgn_tiDlyRlsDNOxHmlg_C verzögert, der im 55265162-Firmware-Image auf 300 Sekunden festgelegt ist. Das daraus resultierende Freigabesignal aus dem Block wird bestätigt, wenn entweder das Homologations- oder das Realfahrbetriebssignal den Wert true hat.

Abb. 6: Die stTiCoEngHmlg-Signallogik, die zum Setzen des Befehls stDNOxHmlg erforderlich ist, damit die Regeneration im Rahmen des „Homologations"-Programms eingeleitet werden kann. In dem von uns untersuchten Firmware-Image 55265162 des Fiat 500X ist NSCRgn_tiCoEngMaxHmlg_C auf 1600 Sekunden festgelegt. Copyright der Robert Bosch GmbH.

Die Logik zur Steuerung des Homologations-Regenerationsfreigabesignals ist in Abbildung 12, und der entsprechende Logikblock für den Realfahrbetrieb in Abbildung 13 im Anhang dargestellt. Die wichtige Eigenschaft des Homologationsfreigabeblocks besteht darin, dass alle Bedingungen, die durch die in der Abbildung gezeigten Blöcke bestimmt werden, erfüllt sein müssen, da deren Ausgangsgrößen durch AND-Verknüpfung miteinander verbunden sind, um das Ausgangssignal stDNOxHmlg zu erzeugen. Das bedeutet vor allem, dass die stTiCoEngHmlg-Ausgangsgröße des ersten Subblocks den Wert true haben muss. Der untere Teil von Abbildung 12 zeigt, wie dieses Signal berechnet wird: stTiCoEngHmlg wird gesetzt, wenn die Laufzeit seit dem Motorstart, tiSnceFrstRunngRed, weniger oder gleich der Konstante NSCRgn_tiCoEngMaxHmlg_C ist. In dem von uns untersuchten Firmware-Image des Fiat 500X war diese Konstante auf 1600 Sekunden kalibriert. Dementsprechend *wird das Homologations-Regenerationsfreigabesignal stDNOxHmlg unterdrückt, wenn der Motor länger als 1600 Sekunden läuft*. Zudem verlangt stDNOxHmlg auch, dass der gesamte Fahrzyklus-Kraftstoffverbrauch höchstens NSCRgn_volFlConsMaxHmlg_C beträgt, der in unserem Firmware-Image mit 1,3 Liter konfiguriert ist.

Das bedeutet, dass die vom Homologationsbedarfsblock angeforderte Regeneration *nur während der ersten 1600 Sekunden (26 Minuten 40 Sekunden) des Motorbetriebs eingeleitet werden darf*. Danach darf nur noch eine von der „Realfahrbetriebslogik" angeforderte NSK-Regeneration eingeleitet werden. Wir stellen fest, dass dies mit der Dauer der standardisierten Abgasprüfzyklen übereinstimmt.

Die vorstehend beschriebenen Logikblöcke umfassen mehrere Schaltungen, die dieses Dual-Pfad-Verhalten deaktivieren können. In dem von uns untersuchten Firmware-Image des Fiat 500X stellten wir fest, dass beide Pfade aktiviert waren (NSCRgn_swt{Hmlg,Rd}HmlgActv_C = true). Die Homologationsfreigabeverzögerung NSCRgn_tiDlyRlsDNOxHmlg_C war auf 300 Sekunden festgelegt, womit die Frequenz der in der Homologation angeforderten Regeneration auf einmal alle fünf Minuten limitiert war. Wir untersuchten auch die Bedarfslogik für die Homologation und den Realfahrbetrieb.

V. NACHWEIS VON ABSCHALTEINRICHTUNGEN

Anhand der Erkenntnisse, die wir in unseren Fallstudien gewonnen haben, gestalteten wir ein Tool für die statische Analyse, das uns hilft, Abschalteinrichtungen in einem jeweiligen Firmware-Image zu erkennen. Wir implementierten einen Prototyp dieses Ansatzes in einem Tool namens CURVEDIFF für Steuergeräte vom Typ EDC17, wodurch wir die Entwicklung und das Verhalten dieser Steuergeräte über eine große Anzahl von Firmware-Images verfolgen konnten. Im Folgenden möchten wir Überlegungen zum Aufbau und dem allgemeinen Arbeitsablauf zusammen mit Details zur Implementierung ansprechen.

A. Überlegungen zum Aufbau

Unsere Methode soll *automatisch* mögliche Abschalteinrichtungen erkennen, die aktiv versuchen, laufende Emissionsprüfungen anhand des Fahrprofils während des Prüfzyklus zu identifizieren. Genauer gesagt, wir versuchen Code-Regionen in einem bestimmten Firmware-Image zu finden, welche den Versuch unternehmen, festzustellen, ob das Fahrzeug derzeit einen der standardisierten Prüfzyklen durchläuft und deren Verhalten dann die Funktion des Motors beeinflusst. Wir konzentrieren uns somit auf Abschalteinrichtungen, die von Volkswagen implementiert wurden, da diese Geräte den zeitgesteuerten Geräten, die von FCA benutzt werden, überlegen ist.

Unser Entscheidung, der Prüfzyklus-Erkennung Priorität einzuräumen, fiel aufgrund zwei wichtiger Faktoren. Erstens erfordert dieser Ansatz relativ wenig Vorwissen über Firmware-Spezifika und ist nicht so sehr anfällig hinsichtlich syntaktischer Veränderungen in der Prüflogik. Dies wiederum bedeutet für uns auch, dass wir nicht auf zusätzliche Daten wie **.a21**-Dateien angewiesen sind, die für ein bestimmtes Firmware-Image möglicherweise schwer zu beschaffen sind (obwohl dies die Analyse erheblich vereinfachen würde). Zweitens bietet dieser Ansatz einen höheren Grad der Nichtabstreitbarkeit: Da wir nicht darauf angewiesen sind, ECU-Variablen genau zu ermitteln, sondern versuchen, auf allgemeine Weise Übereinstimmungen mit bekannten Emissionsprüfzyklen zu erkennen, ist die Tatsache, dass die Software dies *aktiv* prüft, im Allgemeinen schwer zu widerlegen.

B. Allgemeiner Workflow

Wir benutzen für die Umsetzung unseres Ansatzes eine statische Code-Analyse, da wir nicht einfach ein bestimmtes ECU-Firmware-Image in einem Emulator ausführen können und so eine dynamische Analyse durchzuführen. Darüber hinaus erlaubt uns die statische Analyse, große Mengen Code zu analysieren, da jede Funktion einzeln geprüft wird. Unser Analyse-Framework mit der Bezeichnung **CURVEDIFF** beruht auf dem IDA Pro 6.9 [13] Disassembler, mit Support für den Infineon TriCore-Prozessor, der im Steuergerät Bosch EDC17 verwendet wird. Das voll automatisierte Framework akzeptiert eine binäre Firmware-Image als Eingabe. Bei der Analyse eines Firmware-Image führen wir die folgenden Schritte aus:

1) Erzeugen und Vorverarbeiten der IDA-Datenbank,
2) Aufbau der Kernstrukturen und Konversion auf Static Single Assignment (SSA)-Form,

3) Analyse der Kurvenfunktionsinvokationen,
4) Abgleich der Kurve mit Prüfzyklen.

In den folgenden Abschnitten beschreiben wir jeden Schritt im Detail und teilen Näheres über die Implementierung mit.

C. Vorarbeiten

Die Kurvenfunktion **SrvX_IpoCurveS16** ist ein wichtiger Teil der von Volkswagen verwendeten Abschalteinrichtungen. Es handelt sich zudem um eine der *Kernfunktionen*, die das Betriebssystem selbst bereitstellt und somit in allen Firmware-Images vorhanden ist, die das gleiche Betriebssystem benutzen. Ferner stellten wir fest, dass die Funktion im gesamten Code eines Firmware-Image verwendet wird. Im Prinzip gibt die Funktion die **y-Koordinate** für eine bestimmte **x-Koordinate** auf der **Kurve c** aus, im Wesentlichen **y <- SrvX_IpoCurveS16 (c, x)**. Da **c** auch nur durch einige Datenpunkte dargestellt werden könnte, interpoliert die Funktion linear.

Der Abgleich des aktuellen Fahrprofils gegenüber vordefinierten Emissionsprüfzyklen erfolgt durch Darstellung von zwei Kurvenabfragen mithilfe von **SrvX_IpoCurveS16**: Eine Abfrage ergibt die obere Grenze von **y** entsprechend zum angegebenen **x**-Wert, während die andere Abfrage die untere Grenze liefert. Insbesondere passen die Grenzen zu einem bekannten Prüfzyklus, der das reale Fahrprofil (Sekunden seit dem Motorstart **x** und zurückgelegte Strecke **y**) damit vergleicht.

D. Vorverarbeitung

Um für unsere Analyse Speicherzugriffe zu ermöglichen, müssen wir die *kleinen Datenregionen* (für globale Variablen über das globale Register **a0** des TriCore-Systems) sowie *wörtlichen Datenregionen* (nur Daten lesen, über Register **a1**) und die Funktionsvektortabelle (über Register **a9**) erhalten, welche Daten speichert, die mit einer bestimmten Funktion verknüpft sind. Die globalen Register des Systems hängen von der Systemarchitektur und vom Betriebssystem ab und werden beim Hochfahren initialisiert, da alle Funktionen damit betrieben werden, um auf spezifische Speicherregionen zuzugreifen. Weiterhin benötigen wir noch die Adresse der Kurvenfunktion, die leicht durch den Abgleich zu Teilen der Funktionssemantik (nämlich die lineare Interpolation der zwei Kurvenpunkte) erhalten werden kann und das Ergebnis wird durch seinen Call Graph verifiziert. Da diese Funktion nicht kundenspezifisch ist, sondern vom Betriebssystem geliefert wird, ändert sich dies nicht wesentlich.

Beachten Sie bitte, dass wir einige Punkte zu berücksichtigen haben. Da die Kurvenfunktion eingeschlossen sein könnte, müssen wir solche Fälle erkennen, um keine späteren Zwischenanalysen durchführen zu müssen. In der Praxis können solche Hüllenfunktionen leicht mit dem Call Graph der Funktion erkannt werden. Wir müssen darüber hinaus die Besonderheiten der Architektur berücksichtigen: TriCore unterstützt *Scratch Pad RAM* (SPRAM), die Teile des Codes der Firmware in einen schnelleren Speicher spiegelt. Da dies beim Hochladen erfolgt (also bei Runtime), müssen wir das Mapping der gespiegelten Regionen extrahieren, da wir andernfalls die Aufrufe dieses Speicherbereiches verpassen könnten.

E. Konversion zu Static Single Assignment-Form und Optimierung

Um ein robuste statische Analyse zu ermöglichen, die sich für unsere Aufgabe eignet, benutzen wir eine Intermediate Language (IL) in Static Single Assignment (SSA) Form. SSA wurde von Cytron et al 1991 [6] vorgestellt und beschreibt die Eigenschaft einer IL, nur eine einzige Definition für jede Variable zu haben und jede Definition bestimmt die jeweilige Nutzung. Dies wiederum ermöglicht den Aufbau von effizienten Datenanalyse-Algorithmen.

Die TriCore-Assembler-Sprache ist ausdrucksstark genug, damit die Notwendigkeit für eine vollwertige IL entfallen kann. Dadurch sind Nebenwirkungen selten und fast der gesamte Datenfluss ist explizit. Statt der Entwicklung einer neuen IL von Grund auf neu, haben wir die Assembly-Darstellung geringfügig verändert, um sie den Anforderungen anzupassen, die bei der Umwandlung auf die SSA-Form vorliegen. Genauer gesagt, für Anweisungen, die einen Operanden enthalten, der sowohl gelesen als auch geschrieben wird, kopieren wir den Operanden dergestalt, dass *Nutzung* und *Definition* sich korrekt unterscheiden. Gleichermaßen haben wir für Anweisungen mit mehreren Variablen eine einzige Definition hinzugefügt (ein temporäres Register) und Hilfsanweisungen eingefügt, welche die korrekte Definition aus dem temporären Register extrahieren und diese dann in der Zielvariablen abspeichern. Zum Beispiel kann **calls** unter anderem die Ergebnisse sowohl im Register **a2** als auch dem Register **d2** speichern. Da die SSA-Form keine mehrfachen Definitionen für eine Anweisung erlaubt, führen wir das temporäre Register **re** ein, welches die Rückgabewerte des Aufrufs speichert. Direkt nach der Anweisung **Call** fügen wir künstliche Anweisungen **cconv.w** hinzu, die **re** auslesen und den entsprechenden Teil des Rückgabewertes in **a2** bzw. **d2** speichern. Ferner verschlüsseln wir andere Besonderheiten der TriCore-Aufrufkonvention explizit. So haben wir zum Beispiel die Nutzung der Parameter-Register **a4** und **d4** bei **Calls** hinzugefügt und gleichermaßen **a2** und **d2** für Rückgabeanweisungen benutzt. Wir wandeln den daraus resultierenden Assembler-Code in SSA-Form [5] mithilfe Liveness-Analyse um. Um schließlich den Speicherzugriff über die globalen Register **a0**, **a1** und **a9** zusammenzuführen, optimieren wir jede Funktion mithilfe konstanter Ausbreitung.

F. Abfragen nach zusammenhängenden Kurven

Nach der Umwandlung aller Funktionen in eine Zwischendarstellung wird jede Funktion separat analysiert, um eine Liste der Kandidaten zu erstellen, die möglicherweise eine Kontrolle auf Emissionsprüfzyklen durchführen. Zu diesem Zweck extrahieren wir alle Aufrufe der Kurvenfunktion und versuchen, sie paarweise zu gruppieren, wobei jeder Aufruf entweder die obere Grenze oder die untere Grenze für einen gegebenen Datenpunkt abfragt. Dies ermöglicht uns das programmgesteuerte Extrahieren der Kurven, welche beide Grenzen definieren und sie dann mit bekannten Zyklen in einem späteren Schritt zu vergleichen. Wir legen dabei fest, dass jeweils zwei Aufrufe einer Kurvenfunktion miteinander *zusammenhängen müssen*.

Im Abschnitt V-C wird erläutert, wie zwei Aufrufe der Kurvenfunktion **SrvX IpoCurveS16** vorgenommen werden, um das aktuelle Fahrprofil mit vordefinierten Emissionsprüfzyklen zu vergleichen.

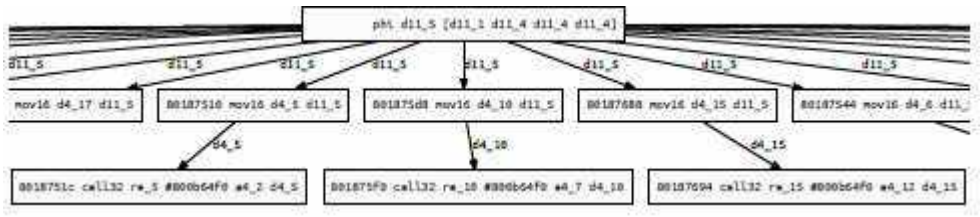


Abbildung 7: Auszug aus einem Datenflussdiagramm, welche dem Nachweis der Eigenschaft **P-1** dient. Kurvenaufrufe können nach ihrem Ursprung der eingegebenen Koordinate **x** gruppiert werden (weitergegeben über das Register **d4**, mit dem Ursprung im Register **d11**).

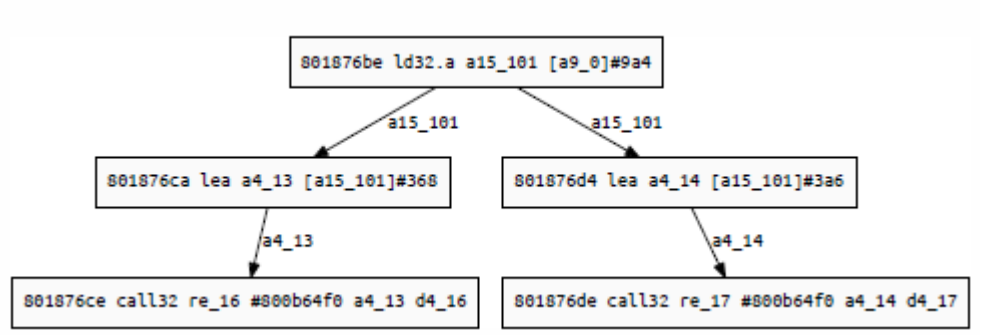


Abbildung 8: Beispiel für ein Datenflussdiagramm für den Nachweis der Eigenschaft **P-2**. Bei den Aufrufen der Kurvenfunktion wird eine andere Zielkurve über Register **a4** übergeben.

Diese Beobachtung erlaubt uns, mehrere wichtige Eigenschaften zu identifizieren, die für zwei miteinander verbundene Kurvenabfragen gelten:

P-1 Beide Kurvenabfragen in einer miteinander zusammenhängenden Prüfung müssen die gleiche Variable als Abfragepunkt **x** (Parameter **d4**) verwenden. Diese Anforderung ergibt sich aus der Tatsache, dass beide Kurven die gleiche Achse verwenden. Im konkreten Fall entspricht **x** dem Zeitraum seit dem Anlassen des Motors.

P-2 Beide Kurvenabfragen müssen auf bestimmten Kurven beruhen (Parameter **a4**). Dies liegt daran, weil beide Kurven mehrere mögliche Fahrprofile codieren und gewisse Abweichungen von den exakten Prüfzyklen aufgrund möglicher Ungenauigkeiten während der Emissionsprüfung gestatten.

P-3 Die Ergebnisse $\boldsymbol{y_{low}}$ und $\boldsymbol{y_{high}}$ (Register **d2**) der beiden Kurven müssen in dem Sinne miteinander zusammenhängen, weil sie eine Bereichsprüfung des tatsächlichen **y**-Wertes durchführen (**y** ist ja die zurückgelegte Strecke seit dem Anlassen des Motors).

Eigenschaften P-1 und P-2. Im Endeffekt gestattet uns die Eigenschaft **P-1**, mehrere Aufrufe der Kurvenfunktion zusammen zu gruppieren, anhand des Wertes, der für den Parameter **x** zur Verfügung gestellt wird. Um dies zu erreichen, werden wir für jeden Aufruf das Register **d4** zurückverfolgen und ein Datenflussdiagramm aufbauen, bei dem die Knoten Anweisungen darstellen und die Kanten die (notwendigerweise eindeutige) Definition einer Variablen und deren Verwendungen verbinden. In der Abbildung 7 wird ein Beispiel für die sich ergebende Grafik gezeigt. Es ist offensichtlich, dass alle Kurvenaufrufe $\mathbf{d11_5}$ als Parameter **x** nutzen. Gleichermaßen können wir das Register a4 zurückverfolgen, um die tatsächlichen Kurven zu finden, auf denen die Funktionen operieren. Abbildung 8 veranschaulicht diesen Ansatz. Beachten Sie bitte, dass beide Aufrufe Knoten hinterlassen, die über $\mathbf{a15_{101}}$ miteinander verbunden sind, welches die Funktionsvektoreingabe ist, in der alle mit der aktuellen Funktion zusammenhängende Daten aufbewahrt werden. Aber beide Aufrufe operieren immer noch auf verschiedenen Kurven mit Versatz **0x368** bzw. **0x3a6**.

Eigenschaft P-3. Eigenschaft **P-3** gibt im Prinzip an, dass die resultierende ***ys*** von zwei unterschiedlichen Kurvenaufrufen *miteinander zusammenhängen*, falls für sie der gleiche „aussagekräftige" Ausdruck gilt. Ein Ausdruck ist dann aussagekräftig, wenn beispielsweise eine Intervallprüfung durch Vergleich eines bestimmten Wertes mit oberen und unteren Bereichsgrenzen erfolgt, wie dies ja durch die Kurven vorgegeben wird.

Um **P-3** zu prüfen, beginnen wir mit dem Aufbau eines Bestandes („Wald") von Datenflussgraphen, indem wir die Rückgabewerte aller Kurvenaufrufe zurückverfolgen, die sich in der gleichen Gruppe befinden, nach Eigenschaft **P-2**. Beachten Sie bitte, dass in den Datenflussgraphen nicht alle Verwendungen einer Anweisung berücksichtigt werden. Jede miteinander verbundene Komponente entspricht dann entweder dem Datenflussdiagramm aus einem einzelnen Kurvenaufruf oder verbindet Datenflussgraphen mehrerer Kurvenaufrufe miteinander. Während der erste Fall keine nützlichen Informationen liefert, kann der letztere Fall Aufschluss darüber geben, ob beide Kurvenaufrufe tatsächlich miteinander zusammenhängen. Obwohl diese Tatsache an sich bereits nützlich ist, können wir noch einen Schritt weitergehen und prüfen, *wie* zwei Aufrufe miteinander zusammenhängen.

Intuitiv wird die Art der Beziehung zwischen zwei Kurvenaufrufen durch den Knoten beschrieben, wo die Datenflüsse für jeden Rückgabewert *zusammentreffen*. Wir bezeichnen diese Knoten auch als „*Vorwärts gerichtete Synchronisationsknoten*". Diese können berechnet werden, indem der *Lowest Common Ancestor* (LCA, etwa „letzter gemeinsamer Vorgänger") [2] des durch den Scheitelpunkt induzierten Teilgraphen aller möglichen Paare von Kurvenaufrufe berechnet wird. Abbildung 10 im Anhang zeigt einen Teil der (einzigen) verbundenen Komponente, wodurch die Beziehungen aller Kurvenaufrufe in die akustische Funktion aufgezeigt werden. Diese Aussage implementiert eine Intervallprüfung, die weiterhin nachgewiesen werden konnte, etwa durch symbolische Nachverfolgung des Weges bis zum Synchronisationsknoten. Gleichermaßen können wir sogenannte „*Rückwärts gerichtete Synchronisationsknoten*" als die LCA in einem umgekehrten Datenflussdiagramm definieren (genauer gesagt, im Teilgraphen, der

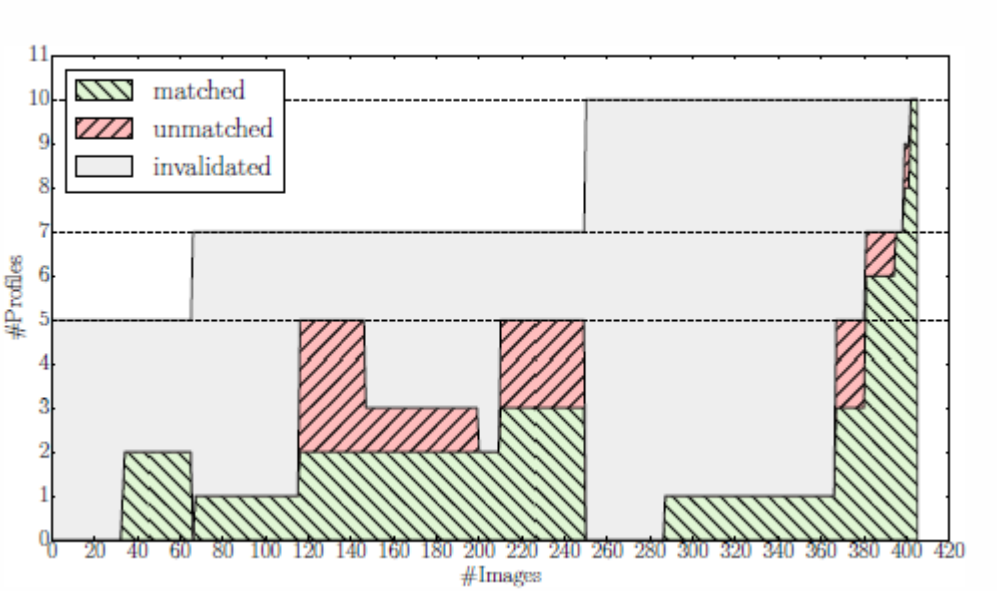
durch alle Paare von „Blättern“ induziert wird). Abbildung 10 zeigt ein Beispiel für einen rückwärts gerichteten Synchronisationsknoten, der Knoten *phi* (ϕ) legt dabei **d9₃** fest. Es überrascht nicht, dass diese Definition der bisher zurückgelegten Strecke entspricht.

Um Fälle abzubilden, bei denen beispielsweise die Ausführung einer Prüfung der unteren Grenze von der Prüfung der oberen Grenze abhängt (es findet als Beispiel keine Ausführung statt, je nach den Ergebnissen der anderen Prüfung), aber keine direkte Datenabhängigkeit besteht, bereichern wir den Datenflussgraphen durch prüfungsabhängige Kanten, d. h., wir erstellen einen Abhängigkeitsgraph eines reduzierten Programms. Die hier vorgestellten Konzepte gelten allerdings auch für diese Erweiterung.

G. Abgleich von Prüfzyklen auf Übereinstimmung

Sofern zwei miteinander zusammenhängende Kurvenaufrufe vorliegen, können wir die zugrunde liegenden Kurven durch Zurückverfolgung des Parameterregisters **a4** extrahieren. Auf diese Weise erhalten wir eine Kurve, welche die obere Grenze der abgeglichenen Fahrprofile $\mathbf{c}_T$ und die untere Grenze $\mathbf{c}_\perp$ darstellt. Grob gesagt, ein bestimmtes Fahrprofil *stimmt dann überein*, wenn seine Datenpunkte innerhalb dieser Grenzen liegen.

Beachten Sie bitte, dass wir eine Plausibilitätsprüfung der extrahierten Kurven durchführen können, bevor wir die Verarbeitung fortsetzen. Das heißt, wir möchten sehen, dass die Kurve monoton ansteigt, da sich die zurückgelegte Strecke natürlich nicht verringert. Diese Anforderung wird dann in den letzten Datenpunkten einer Grenze nicht mehr strikt durchgesetzt, da es Fälle gibt, bei denen $\mathbf{c}_T$ unter $\mathbf{c}_\perp$ fällt und alle Fahrprofile nach diesem Punkt abgelehnt werden. Gleichermaßen können wir ermitteln, ob sogenannte „*ungültige Prüfungen*“ vorliegen. Diese sind dadurch gekennzeichnet, dass alle ***y***-Werte auf einen konstanten Wert gesetzt werden (**0x7fff** für $\mathbf{c}_\perp$ und 0 für $\mathbf{c}_T$ in den von uns analysierten Firmware-Images), damit die Prüfung jedes Fahrprofil ablehnt. Mit dieser Methode kann der Hersteller ein Profil so parametrisieren, dass es tatsächlich nicht zum Einsatz kommt. Die Referenzprüfzyklen, wie sie für die Emissionsprüfung verwendet werden, sind entweder kostenlos erhältlich [20] oder können gegen eine geringe Subskriptionsgebühr bezogen werden [7].



Anzahl Images
Übereinstimmung
Keine Übereinstimmung
Ungültig

Abbildung 9: Abdeckung der Profile in allen Firmware-Images, in denen eine Abschalteinrichtung gefunden wurde. Übereinstimmende Profile werden mit rückwärts gerichteten diagonalen Linien dargestellt, nicht übereinstimmende Profile werden durch vorwärts gerichtete diagonale Linien dargestellt und ungültige Kurven werden grau hinterlegt dargestellt.

In den meisten Fällen werden die Zyklen in Form von zweidimensionalen Datenpunkten dargestellt, welche Informationen über die verstrichene Zeit in Sekunden und die Geschwindigkeit zum jeweiligen Punkt anzeigen (Angabe entweder in Meilen/h oder km/h). Um die Prüfzyklen tatsächlich mit den Grenzen abzugleichen, die aus den Firmware-Images extrahiert wurden, müssen beide Darstellungen zunächst normalisiert werden. Hierfür haben wir die y-Achse um den Faktor 0,1 skaliert, um die Strecke in Kilometern zu erhalten. Die x-Achse haben wir um den Faktor 6,25 skaliert, um die Laufzeit des Motors seit dem Anlassen in Sekunden zu erhalten (entspricht der Einheit **TimeRed** in der A2L-Datei). Da die Prüfkurven die Geschwindigkeit statt der zurückgelegten Strecke angeben, integrieren wir sie und wandeln die Angaben gegebenenfalls von Meilen/h in km/h um. Schließlich muss für die Übereinstimmung einer Kurve jeder Datenpunkt im Intervall liegen, welches durch $\mathbf{c}_T$ beziehungsweise $\mathbf{c}_\perp$ festgelegt wird.

Trotzdem beenden einige Prüfungen das Fahrprofil zum Ende des jeweiligen Prüfzyklus, wenn die Emissionseffekte am ehesten nicht mehr bei einer laufenden Emissionsprüfung erkannt werden. Der entsprechende Prüfzyklus liefert dann keine Übereinstimmung durch den Abgleich aller seiner Datenpunkte wegen des vorzeitigen Moduswechsels. Um dies zu berücksichtigen, prüfen wir das Intervall für die letzten 10% eines jeweiligen Prüfzyklus nicht mehr.

VI. BEWERTUNG

Auf der Basis der Prototyp-Implementierung von **CURVEDIFF** führten wir eine größere Studie von Volkswagen-Firmware-Images durch, um zu untersuchen, bei welchen eine Abschalteinrichtung enthalten ist. Im Folgenden stellen wir die Bewertung der Ergebnisse neben einigen Highlights vor, die wir gefunden haben.

Wir analysierten 963 Firmware-Images und haben das System für die Analyse mit einem Zeitlimit von 7 Minuten konfiguriert, um zu lange laufende Analysen zu vermeiden. Es wurden 924 Images erfolgreich nach den im vorangegangenen Abschnitt beschriebenen Schritten analysiert, während 20 Aufgaben das Zeitlimit überschritten haben und 19 Aufgaben durch IDA nicht verarbeitet wurden. Insgesamt haben wir festgestellt, dass 406 (44 %) der untersuchten Images eine Abschalteinrichtung enthielten, von denen 333 mindestens ein aktives Profil (also ein Profil, das nicht ungültig ist) enthalten.

Durchführung. Die statische Analyse ist voll automatisiert und die schnellste Analyse-Aufgabe wurde nach 55 Sekunden beendet, wobei das Zeitlimit bei mehreren Aufgaben überschritten wurde (siehe oben). Das geometrische Mittel für die Analyse aller erfolgreichen Aufgaben beträgt 105 Sekunden. Wir können somit ein jeweiliges Images im Durchschnitt in weniger als zwei Minuten analysieren.

TABELLE II: Akustische Bedingungslogik und betroffene Systeme anhand von Funktionsdatenblättern. Die Spalte *Modell* zeigt das ECU-Modell (Präfix EDC wurde weggelassen). Die Spalte *Version* zeigt die ECU-Version, für welche das Funktionsdatenblatt erzeugt wurde. Die Spalte *Datum* gibt das Datum des Funktionsdatenblatts an. Die Spalte *N* gibt die Anzahl der Profile an, welche auf die akustische Bedingung geprüft wurde. Wird „---“ angegeben, wurde der Baustein für die akustische Bedingungslogik nicht in der Funktion berücksichtigt. Die Spalte *Betroffene Teilsysteme* zeigt die Teilsysteme, bei denen die akustische Bedingung referenziert wurde, extrahiert von der Variablen-Referenztabelle im Funktionsdatenblatt.

Modell	Version	Datum	N	Betroffene Teilsysteme
16CP	P_397 A.V.0	2005-06-24	0	InjCrv, Rail
17CP04	P_531 2.F.0	2005-10-28	0	InjCrv
16CP	P_397 A.V.9	2006-03-02	0	InjCrv, Rail
17CP04	P_617 3.K.0	2006-11-06	0	InjCrv
17CP04	P_617 3.N.0	2006-12-22	0	InjCrv
17CP24	P_628 3.K.1	2007-03-29	—	InjCrv
17CP24	P_628 3.U.0	2007-05-02	—	
17CP24	P_703 3.V.5	2007-07-12	—	
17CP04	P_617 3.U.0	2007-05-14	5	
17CP14	P_531 3.U.0	2007-05-24	5	
17CP14	P_617 3.U.5	2007-08-30	5	
17CP24	P_628 3.W.5	2007-09-18	—	AirCtl, InjCrv
17CP14	P_714 3.U.A	2007-10-12	5	InjCrv
17CP24	P_703 3.W.A	2007-11-05	—	AirCtl, InjCrv
17CP24	P_628 3.W.G	2008-02-12	5	AirCtl, PFlt, InjCrv
17CP24	P_703 3.W.G	2008-02-14	5	AirCtl, PFlt, InjCrv
17CP24	P_628 3.W.H	2008-03-04	5	AirCtl, PFlt, InjCrv
17CP14	P_804 4.F.0	2008-03-26	5	InjCrv, Rail
17CP24	P_703 3.W.K	2008-04-23	5	AirCtl, PFlt, InjCrv
17CP24	P_628 3.W.L	2008-05-17	5	AirCtl, SCRFFC, PFlt, InjCrv
17CP24	P_859 4.F.0	2008-05-30	5	AirCtl, PFlt, InjCrv, Rail
17CP24	P_628 3.W.M	2008-06-27	5	AirCtl, SCRFFC, PFlt, InjCrv
17CP44	P_804 4.P.0	2008-08-05	—	AFS, AirCtl, ASMod, InjCrv, PCR, Rail
17CP24	P_859 4.P.0	2008-09-18	—	AFS, AirCtl, ASMod, InjCrv, PCR, PFlt, Rail
17CP44	P_930 4.P.5	2008-11-13	—	AFS, AirCtl, ASMod, InjCrv, PCR, PFlt, PFltPOp, Rail
17CP44	P_804 5.A.0	2009-01-22	7	AFS, AirCtl, ASMod, InjCrv, InjSys, PCR, PFltPOp, Rail, SmkLim
17CP44	P_804 5.A.5	2009-02-04	7	
17CP44	P_859 5.A.0	2009-03-16	7	AFS, AirCtl, ASMod, InjCrv, InjSys, PCR, PFlt, PFltPOp, Rail, SmkLim
17CP44	P_859 5.F.5	2009-07-13	7	

Im Vergleich zu einer Analyse auf einem Rollenprüfstand ist ein solches Vorgehen um mindestens zwei Größenordnungen schneller.

Ergebnisse. Tabelle III zeigt die Ergebnisse unserer Analyse. Ergebnisse oberhalb der doppelt durchgezogenen Linie enthalten Firmware aus dem Dump, erhalten von der Chiptuning-Szene (2009 und 2010). Daten und Software-Teilenummern wurden dem Release-Zertifikat neben den Firmware-Images entnommen. Ergebnisse unterhalb der doppelt durchgezogenen Linie beruhen auf Firmware-Images, die über das *erWin*-Portal bezogen wurden, das offizielle Firmware-Images für Autowerkstätten anbietet (2012 bis 2016). Datumsangaben wurden dem Zeitstempel der Firmware entnommen. Für beide Datenquellen wurden die Modelle durch Abfragen einer Online-Datenbank für Ersatzteile abgeglichen, welche Metadaten für eine jeweilige Artikelnummer liefert (in diesem Fall geben die Teilenummern das Steuergerät vor). Diese Zuordnung ist möglicherweise nicht 100% genau, was auch von besagten Stellen mitgeteilt wird. Wurden für Teilenummern mehrere Modell-Namen angegeben (wegen der unterschiedlichen Modellbenennung für verschiedene Regionen), entschieden wir uns für den europäischen Namen, da die meisten Firmware-Images für die europäischen Emissionsprüfzyklen arbeiten. Falls mehrere Firmware-Images in einem Monat sich auf das gleiche Modell beziehen, haben wir die Anzahl der für ein bestimmtes Modell analysierten Images in Klammern gesetzt. Schließlich haben wir für alle im gleichen Monat veröffentlichten Images die Gruppe der Prüfzyklen verwendet, für welche sie arbeiten, um einen Eindruck von der Anzahl und Vielfalt von übereinstimmenden Zyklen zu vermitteln. Abbildung 9 zeigt den Umfang der erkannten Prüfzyklen. Für Firmware-Images mit 5 Profilen konnten wir einen Prüfzyklus für jedes Profil abgleichen. Bei späteren Images, bei denen 5 bzw. 7 Profile abgeglichen wurden, konnten wir keinen passenden Prüfzyklus für einige der Profile finden.

Auswirkungen auf die Abgasrückführung. Auf Grundlage der Ergebnisse in der Tabelle III haben wir *automatisch* eine untere Grenze der Firmware-Images gefunden, bei denen die akustische Bedingung das **AirCtl**-Teilsystem beeinflusst, das für die Berechnung des Umfangs der Abgasrückführung (EGR) verantwortlich ist. Wir haben hierfür keine A2L-Dateien verwendet, da uns keine passenden Dateien für alle Firmware-Images vorliegen. Wir haben festgestellt, dass für mindestens 268 Images (66 %) die akustische Bedingung die Abgasrückführung beeinflussen könnte. Auf der Grundlage der extrahierten Parameter können wir bestätigen, dass bei 247 (92 %) dieser Images die akustische Bedingung tatsächlich die Wahl der Parameter beeinflusst. Beachten Sie bitte, dass die **AirCtl**-Erkennung verbessert sowie auch auf andere Teilsysteme erweitert werden kann. Näheres findet sich in Tabelle II, wodurch weitere Abschalteinrichtungen in der Tabelle III bestätigt werden.

Wir haben zudem manuell einige der Abschalteinrichtungen analysiert, die durch **CURVEDIFF** erkannt wurden, um unsere Ergebnisse zu verifizieren. Im Folgenden stellen wir einige der wichtigsten Ergebnisse vor.

Prüfung des Lenkradeinschlags. Wir stellten fest, dass das Firmware-Image EDC17C54P1169 aus dem Jahr 2014 mit der Teilenummer 03L906012DE und Revision 8401 begonnen hat, den Lenkradeinschlag zu messen, zusätzlich zu dem Zeit-Strecken-Profil wie in Abschnitt IV-A beschrieben. Ein automatischer Scan für die Prüfung des Lenkradeinschlags ergab drei weitere Images, nämlich 0L906012, Revision 7444 (in Abbildung 3 dargestellt); 03L906012DD, Revision 8400; sowie 03L906012BP, Revision 7445. Die Images wurden scheinbar am 3. Dezember 2014, um 22:55 freigegeben und werden nach Angabe einer Online-Datenbank in den Modellen VW Passat verwendet. Diese Verfeinerung der Abschalteinrichtung ist bemerkenswert angesichts der Tatsache, dass an diesem Punkt CARB bereits begonnen hatte, Emissionsauffälligkeiten bei Volkswagen-Fahrzeugen zu untersuchen [15] (vgl. Fakten 140, 141). Wie sich aus Tabelle III ergibt, sind diese Images für die größte Gruppe von Prüfzyklen mit fast 400 Image-Übereinstimmungen verantwortlich, wodurch die Notwendigkeit der Prüfung weiter unterstrichen wird. Sonstige Firmware-Images, die im gleichen Monat freigegeben wurden (für Audi A4 und A6) enthalten diese zusätzliche Logik nicht und es findet sich nur bei einem Teil der aufgeführten Prüfzyklen eine Übereinstimmung.

VII. DISKUSSION

Unsere empirischen Ergebnisse zeigen, dass unsere Vorgehensweise zur Erkennung von Abschalteinrichtungen im Stil der bei Volkswagen verwendeten über eine große Anzahl von Firmware-Images plausibel ist. Es gibt jedoch auch bestimmte offene Herausforderungen und mögliche Einschränkungen bei unserem Ansatz, die wir im Folgenden diskutieren.

TABELLE III: Ergebnisse für 363 von 406 Firmware-Images, bei denen **CURVEDIFF** eine potenzielle Abschalteinrichtung im Stil der bei Volkswagen verwendeten erkannte. Für nicht in dieser Tabelle aufgeführte Firmware ist entweder das Freigabedatum oder das Modell unbekannt. Die Zahl in Klammern zeigt die Anzahl der Firmware-Images, die für dieses Modell analysiert wurden. Der untere Teil der Tabelle unterhalb der doppelt durchgezogenen Linie zeigt das Ergebnis anhand der *erWin*-Daten; der obere Teil wurde aus einem Chip-Tuning-Dump extrahiert.

Übereinstimmende Emissionsprüfzyklen werden als die Gruppe mit identischen Zyklen in allen Firmware-Images in der entsprechenden Zeile aufgeführt. Die letzte Spalte zeigt an, ob die in dieser Zeile gefundenen Firmware-Images außerdem zusätzliche Prüfungen des Lenkradeinschlags enthielten, welche einzelne Kurven schützen. Die betroffenen Modelle in dieser Zeile werden in Fettdruck dargestellt. Beachten Sie bitte, dass die Daten in dieser Tabelle aus externen Quellen abgerufen wurden (und nicht von VW stammen). Weitere Bedingungen können den Betrieb der Abschalteinrichtungen beeinflussen.

Veröffentlichungsdatum	Modelle (Anzahl der Images)	Übereinstimmende Zyklen (obere Grenze)	Lendkradpr.
2009-01	Golf, Passat (2)	ECE-15, EUDC(L), NEDC	✗
2009-07	A3	ECE-15, FTP-75, HWFET, LA92, NEDC, SC03, US06	✗
2009-08	Passat Blue Motion	ECE-15, EUDC(L), NEDC	✗
2009-09	Golf (2), Passat (3)	ECE-15, EUDC(L), NEDC	✗
2009-10	Golf+, Passat	ECE-15, EUDC(L), NEDC	✗
2009-11	A3 (8), Golf Blue Motion, Golf (2), Passat	ECE-15, EUDC(L), NEDC	
2009-12	A3 (5), Golf Variant (2), Golf+ (2), Golf (7), Jetta (3), Passat (4)	ECE-15, EUDC(L), FTP-75, HWFET, LA92, NEDC, SC03, US06	✗
2010-01	Jetta, Passat (2)	ECE-15, EUDC(L), NEDC	✗
2010-03	A3 (2), Golf (3), Jetta, Passat (3), Q5 (4)	ECE-15, EUDC(L), FTP-75, HWFET, LA92, NEDC, SC03, US06	✗
2010-04	Jetta (2), Passat, Passat Coupe (4), Q5	ECE-15, EUDC(L), NEDC	✗

2012-05	A3 (19), A4, A6, Alhambra (4), Altea, Eos (2), Golf, Ibiza (4), Leon, Octavia (6), Q5 (2), Superb (2), TT, Tiguan, Yeti (4)	ECE-15, EUDC(L), FTP-75, HWFET, LA92, NEDC, SC03, US06	✗
2012-06	Amarok (8), CC, Eos (2), Golf (2), Jetta (2), Octavia (3), Q5 (2), Sharan (7), Tiguan, Touran (2)	ECE-15, EUDC(L), NEDC	✗
2012-07	A1 (3), Alhambra (4), Caddy (2), Sharan (8)	ECE-15, EUDC(L), NEDC	✗
2012-09	Golf (2), Passat, Yeti (6)	ECE-15, EUDC(L), FTP-75, HWFET, LA92, NEDC, SC03, US06	✗
2012-10	A3, Alhambra (2), Tiguan, Yeti	ECE-15, EUDC(L), FTP-75, HWFET, LA92, NEDC, SC03, US06	✗
2012-12	Eos (2), Golf Cabriolet, Tiguan (7), Touran, Yeti	ECE-15, NEDC	✗
2013-01	Leon, Passat	ECE-15, EUDC(L), FTP-75, HWFET, LA92, NEDC, SC03, US06	✗
2013-04	Amarok (6)	(deactivated)	✗
2013-05	Amarok (4)	ECE-15, EUDC(L), NEDC	✗
2013-06	Amarok (5), Superb (3), Tiguan	ECE-15, EUDC(L), NEDC	✗
2013-07	Octavia	ECE-15, EUDC(L), NEDC	✗
2013-08	Yeti (3)	ECE-15, NEDC	✗
2013-11	Superb (3)	ECE-15, EUDC(L), NEDC	✗
2013-12	Superb (2), Yeti (4)	ECE-15, EUDC(L), NEDC	✗
2014-01	Caddy (4)	ECE-15, NEDC	✗
2014-03	Amarok (16), Eos, Tiguan, Yeti	ECE-15, EUDC(L), NEDC	✗
2014-04	Q5, Superb (2)	ECE-15, EUDC(L), NEDC	✗
2014-06	Amarok (6), Tiguan (4)	ECE-15, EUDC(L), NEDC	✗
2014-09	Alhambra	ECE-15, EUDC(L), NEDC	✗
2014-10	Sharan	ECE-15, EUDC(L), NEDC	✗
2014-12	A4 (3), A6, **Passat** (4)	CADC-RURAL, CADC-URBAN, ECE-15, EUDC(L), FTP-75, HWFET, IM240, J1015, JP10, LA92, NEDC, RTS-95, SC03, US06, WLTP-1, WLTP-2, WLTP-3	✓
2015-01	Superb	ECE-15, NEDC	✗
2015-02	A3 (3)	ECE-15, FTP-75, HWFET, LA92, NEDC, SC03, US06	✗
2015-03	Alhambra (2)	ECE-15, EUDC(L), NEDC	✗
2015-05	Alhambra (6), Sharan (6)	ECE-15, EUDC(L), NEDC	✗
2015-07	Q3 (2)	ECE-15, NEDC	✗
2015-10	Altea (2), Yeti (3)	ECE-15, EUDC(L), NEDC	✗
2015-11	Superb	ECE-15, EUDC(L), NEDC	✗
2016-02	Altea	ECE-15, NEDC	✗
2016-03	A4, Exeo (4)	ECE-15, NEDC	✗
2016-04	A6, Exeo, Q3	ECE-15, NEDC	✗
2016-06	Altea (3), CC (3), Jetta, Leon (2), Superb, Tiguan (2)	ECE-15, EUDC(L), NEDC	✗
2016-07	Amarok, CC, Golf, Superb	ECE-15, NEDC	✗
2016-08	CC (3), Golf Cabriolet, Golf (2), Passat (2), Scirocco, Touran (3)	ECE-15, EUDC(L), NEDC	✗
2016-09	CC (14), Octavia (2), Passat (2), Tiguan (7)	ECE-15, EUDC(L), NEDC	✗
2016-10	Eos	ECE-15, NEDC	✗

Generell gesagt, gibt es zwei Ansätze, um die Bedingungen einer normalen Autofahrt auf der Straße von den (eher besonderen) Bedingungen während der Emissionsprüfungen zu unterscheiden: *Aktive* und *passive* Erkennung. Aktive Erkennungstechniken berücksichtigen Eigenschaften des Kraftfahrzeuges während der Emissionsprüfungen und können somit an spezifische Prüfungen angepasst werden. Vor allem die Abschalteinrichtungen von Volkswagen, die Gegenstand dieser Abhandlung sind, können eine laufende Prüfung der Emissionen anhand des Fahrprofils feststellen und mit bekannten Prüfkurven vergleichen. Unser Ansatz beruht auf dieser Erkenntnis und wir schlagen ein kurvenunabhängiges Verfahren vor, um festzustellen, ob die Firmware versucht, eine Übereinstimmung mit einem bestimmten Fahrprofil zu finden. **CURVEDIFF** kann solche Abschalteinrichtungen erkennen und wir fanden viele Beispiel für solche Vorrichtungen. Ein Autohersteller könnte aber auch weitere aktive Verfahren für Abschalteinrichtungen entwickeln, bei denen zum Beispiel eine Übereinstimmung mit dem Profil zusammenhängender Parameter gesucht wird, etwa Drehzahl oder Drehmoment. Ein weiteres konkretes Beispiel dafür ist die Abschalteinrichtung, die im Opel Zafira [9] gefunden wurde.

Andererseits benutzen passive Abschalteinrichtungen prüfungsunabhängige Verfahren, die nicht aktiv Fahrzeugmerkmale überwachen, um eine laufende Emissionsprüfung zu erkennen. Stattdessen zielen sie eher auf allgemeine Besonderheiten der jeweiligen Prüfungen ab. So sind Emissionsprüfungen beispielsweise vergleichsweise kurz. Das eröffnet die Möglichkeit, einfach in einem kompatiblen Modus so lange zu bleiben, wie die durchschnittliche Emissionsprüfung dauert, und anschließend wieder mehr schädliche Emissionen auszustoßen. Die bei Fiat eingesetzte Abschalteinrichtung, die wir zuvor besprochen haben, gehört zu dieser Kategorie. Im Prinzip kann ein Steuergerät alle verfügbaren Sensoren in einem Versuch einsetzen, die Prüfumgebung zu erkennen, etwa durch Messung der Temperatur oder des Umgebungsdrucks, da beide Parameter auch standardisiert sind. Neben auf Software beruhenden Methoden fallen auf Hardware beruhende Verfahren wie Aufpumpen von Reifen über den Nenndruck für einen Rollenprüfstandstest auch in diese Kategorie. Wir habe solche passiven Abschalteinrichtungen nur im begrenzten Maße untersucht, da wir uns auf Abschalteinrichtungen konzentrieren, die Kurven benutzen. Dies ist vor allem deswegen der Fall, weil dieser Ansatz diskreter ist. Solche passiven Abschalteinrichtungen können trotzdem erkannt werden, wenn der Datenfluss im Code verfolgt und untersucht wird, ob bestimmte Sensorbedingungen die Abgasrückführung (EGR) oder andere Teilsysteme zur Abgasentgiftung beeinflussen. Im Rahmen künftiger Arbeiten planen wir, die Plausibilität solcher Ansätze zu studieren und zu bewerten, ob wir die Abschalteinrichtung von Fiat auf einem automatisierten Wege erkennen können.

Wir haben unseren Ansatz in einem Tool mit der Bezeichnung **CURVEDIFF** umgesetzt. Angesichts der Tatsache, dass wir eine intraprozedurale Analyse durchführten, haben wir eventuell bestimmte Vorgehensweisen übersehen, wie eine Abschalteinrichtung implementiert werden kann und eine interprozedurale Analyse könnte die Zuverlässigkeit unserer Implementation untermauern.

Darüber hinaus kann unsere Analyse erweitert werden, um primitivere Bausteine wie Zeitgeber und Multiplexer zu berücksichtigen, um so das Wissen über das Verhältnis der verschiedenen Komponenten in der Erkennungslogik zu vertiefen.

VIII. FAZIT

Software wird als Merkmal komplexer Systeme immer vorherrschender und die Aufsichtsbehörden der Automobilindustrie (sowie vielen anderen) müssen Softwaresysteme zertifizieren, deren Hersteller einen immensen finanziellen Anreiz zum Betrug haben. In dieser Abhandlung haben wir zwei Familien von Abschalteinrichtungen beschrieben, die im Steuergerät Bosch EDC17 zur Umgehung von US-Emissionsprüfungen zum Einsatz kommen. Die erste Familie von Abschalteinrichtungen wurde von Volkswagen verwendet und steht im Mittelpunkt des Volkswagen-Diesel-Emissionsskandals. Die zweite Einrichtung wird im Diesel Fiat 500X eingesetzt. Dieses Fahrzeug wird in Europa verkauft und wurde bislang noch nicht dokumentiert. Wir haben zudem einen automatisierten Ansatz für das Erkennen von Abschalteinrichtungen in einem jeweiligen Firmware-Image anhand von Erkenntnissen vorgestellt und beurteilt, die wir aus der manuellen Analyse der Volkswagen-Abschalteinrichtungen erhalten haben.

DANKSAGUNGEN

Ein Teil dieser Arbeit wurde vom Europäischen Forschungsrat (ERC) unter der Leitung des Programms „Horizon 2020“ für Forschung und Innovation der Europäischen Union (Finanzhilfevereinbarung Nr. 640110 - BASTION) finanziert. Diese Arbeit wurde zum Teil von der National Science Foundation durch Grant NSF-1646493 finanziert.

VERWEISE

[1] Association for Standardisation of Automation and Measuring Systems (ASAM e.V.). ASAM MCD-2 MC. https://wiki.asam.net/ display/STANDARDS/ASAM+MCD-2+MC.
[2] Michael A. Bender, Martin Farach-Colton, Giridhar Pemmasani, Steven Skiena, and Pavel Sumazin. Lowest Common Ancestors in Trees and Directed Acyclic Graphs. In Journal of Algorithms, 2005.
[3] Robert J. Blaszczak. EPA Technical Bulletin: Nitrogen Oxides (NOx) – Why and How They are Controlled. https://www3.epa.gov/ttncatc1/cica/other7_e.html, 1999.
[4] Robert N. Charette. This Car Runs on Code. IEEE Spectrum, 46(3), 2009.
[5] Jong-Deok Choi, Ron Cytron, and Jeanne Ferrante. Automatic Construction of Sparse Data Flow Evaluation Graphs. In ACM Symposium on Principles of Programming Languages (POPL), 1991.
[6] Ron Cytron, Jeanne Ferrante, Barry K. Rosen, Mark N. Wegman, and F. Kenneth Zadeck. Efficiently Computing Static Single Assignment Form and the Control Dependence Graph. In ACM Transactions on Programming Languages and Systems (TOPLAS), 1991.
[7] DieselNet. Emission Test Cycles. https://www.dieselnet.com/standards/cycles.
[8] Christof Ebert and Capers Jones. Embedded Software: Facts, Figures, and Future. Computer, 42(4), 2009.
[9] Felix Domke. Software Defined Emissions, 33C3. https://media. ccc.de/v/33c3-7904-software_defined_emissions.
[10] Felix Domke and Daniel Lange. The exhaust emissions scandal (“Dieselgate”), 32C3. https://media.ccc.de/v/32c3-7331-the_ exhaust_emissions_scandal_dieselgate.
[11] Fiat Chrysler Automobiles. FCA on Real Driving Emissions. https://www.fcagroup.com/en-US/media_center/fca_press_release/2016/february/Pages/fca_on_real_driving_emissions.aspx, 2016.
[12] Ulrich Flaig, Wilhelm Polach, and Gerhard Ziegler. Common Rail System (CR-System) for Passenger Car DI Diesel Engines; Experiences with Applications for Series Production Projects. In SAE Technical Paper. SAE International, 1999.
[13] Hex-Rays SA. Product Page for the Interactive Disassembler. https://www.hex-rays.com/products/ida.
[14] Laura Myers. GM Forced to Recall Cadilacs with Emission ‘Defeat Device’. http://www.apnewsarchive.com/1995/GM-Forced-to-Recall-Cadillacs-With-Emission-Defeat-Device-/id-4b030c7601a14dcc8208fcc1d1bd30cc, 1995.
[15] New York State Office of the Attorney General. NY A.G. Schneiderman, Massachusetts A.G. Healey, Maryland A.G. Frosh Announce Suits Against Volkswagen, Audi And Porsche Alleging They Knowingly Sold Over 53,000 Illegally Polluting Cars And Suvs, Violating State Environmental Laws. http://www.ag.ny.gov/press-release/ny-ag-schneiderman-massachusetts-ag-healey-maryland-ag- frosh-announce-suits-against, 2016.
[16] Robert Bosch GmbH. Diesel Engine Management. John Wiley & Sons Ltd., fourth edition, 2005.

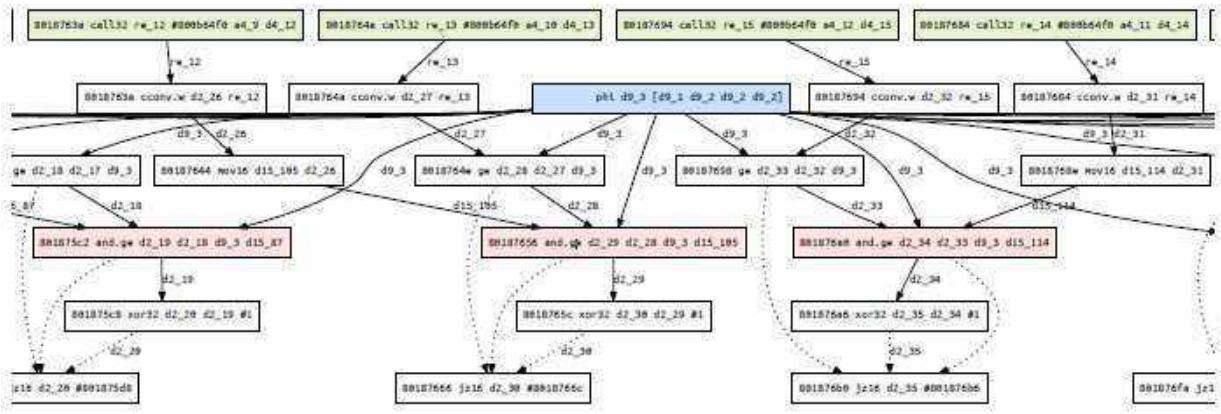


Abbildung 10: Ein Teil der angeschlossenen Komponente im Datenfluss-"Wald" der Abschalteinrichtung. Man kann erkennen, wie die Grenzen, die über zwei Aufrufe an **SrvXIpoCurveS16** (bei **0x800b64f0**) gewonnen werden, mit der zurückgelegten Strecke (in $d9_3$) verglichen werden. Insbesondere nach den beiden Kurvenaufrufen links außen (bei **0x8018763a** und **0x8018764a**) gelangen wir zum *vorwärts gerichteten Synchronisationsknoten* bei **0x80187656** (**and.ge d2, d2, d9, d15**), wodurch die Intervallprüfung erfolgt. Gleichermaßen ist der Knoten ϕ, der $\mathbf{d9_3}$ definiert, ein *rückwärts gerichteter Synchronisationsknoten*, dessen Definition der bislang zurückgelegten Strecke entspricht. Durchgehende Linien stellen den Datenfluss der markierten Variable dar, während gestrichelte Linien die Steuerungsabhängigkeiten zeigen.

TABELLE IV: Überblick über verschiedene Prüfzyklen für die Emissionsprüfung. Das erste Segment führt Prüfungen nach den Vorschriften der US EPA und CARB auf, während das zweite Segment für das EU-Recht maßgeblich ist. Das letzte Segment zeigt internationale Standards. Näheres unter [7], [20].

Abkürzung	**Voller Name**
EPA IM-240	Inspection and Maintenance (Inspektion und Wartung)
FTP-75, EPA-75	Federal Test Procedure (US-Prüfverfahren)
EPA HWFET	Highway Fuel Economy Driving Schedule (Fahrzyklus für den Verbrauch außerorts)
SFTP SC03	Speed Correction Driving Schedule (Geschwindigkeitskorrektur-Fahrzyklus), SC03 SFTP CARB LA92 "Unified" Dynamometer Driving Schedule, Unified Cycle („einheitlicher" Fahrzyklus auf dem Rollenprüfstand)
CADC-RURAL	Common Artemis Driving Cycles, Rural Road Cycle (Fahrzyklus Landstraße) CADC-URBAN Common Artemis Driving Cycles, Urban Cycle (Fahrzyklus innerorts) UN/ECE 15 ECE Elementary Urban Cycle
UN/EUDC	ECE Extra-Urban Driving Cycle (Fahrzyklus außerorts)
UN/EUDCL	ECE Extra-Urban Driving Cycle for Low-Powered Vehicles (Fahrzyklus innerorts für Fahrzeuge geringer Leistung)
NEDC	New European Driving Cycle (Neuer EU-Fahrzyklus)
WLTP	Worldwide Harmonized Light Vehicles Test Procedure (Weltweit harmonisierte Prüfverfahren für PKW)

[17] The Telegraph. Diesel emissions scandal: Fiat under investigation. http://www.telegraph.co.uk/cars/news/diesel-emissions-scandal-fiat-under-investigation, 2016.
[18] United States Environmental Protection Agency. Notice of Violation. https://www.epa.gov/sites/production/files/2015-10/documents/vw-nov-caa-09-18-15.pdf, 2015. [19] US Code of Federal Regulations. 40 CFR §86.
[20] US Environmental Protection Agency (EPA). Dynamometer Drive Schedules. https://www.epa.gov/vehicle-and-fuel-emissions-testing/dynamometer-drive-schedules.
[21] Volkswagen of America, Inc. Self Study Program 826803: 2.0 Liter TDI Common Rail BIN5 ULEV Engine. http://www.natef.org/natef/ media/natefmedia/vw\%20files/2-0-tdi-ssp.pdf, 2008.
[22] WirtschaftsWoche Online. Kommt der zweite Abgasskandal aus Italien? http://www.wiwo.de/unternehmen/auto/fiat-500x-doblo-und-jeep-renegade-kommt-der-zweite-abgasskandal-aus-italien/14483066.html, 2016.

ANHANG

/B e g i n M E A S U R E M E N T
InjCrv stNsCharCor

" S t a t u s d e r A k u s t i k b e d i n g u n g "
U B Y T E
O n e T o O n e
1
1 0 0
0 . 0 0
2 5 5 . 0

F O R M A T "%5.1"

```
E C U _ A D R E S 0 x C 0 0 0 0 C D
/ e n d M E A S U R E M E N T

/ b e g i n C H A R A C T E R I S T I C
AirCtl numInjChar CA
" A b g a s t r a t e g i e f Ã r A i r C t l u n d V s w C t l " M A P
0 x 8 0 1 C 5 A 3 4
M a p _ X u 8 Y u 8 W u 8
2 5 5 . 0
O n e T o O n e
0 . 0 0
2 5 5 . 0

F O R M A T " % 5 . 1 "
E X T E N D E D _ L I M I T S 0 . 0 0 2 5 5 . 0

/ b e g i n A X I S _ D E S C R S T D _ A X I S
I n j C r v _ s t N s C h a r C o r
O n e T o O n e
...
```

Liste 1: Auszug einer A2L-Datei mit Darstellung von Metadaten, die für die akustische Bedingung **InjCrvstNsCharCor** sowie das Array **AirCtlnumInjCharCA** gelten. Im letzteren Fall ist offensichtlich, wie die x-Achse durch den akustischen Zustand indiziert wird. Ähnlich wie bei regulären Symboldateien verweist die Eingabe **ECU_ADDRRESS** auf die Adresse der Variable im Firmware-Image.

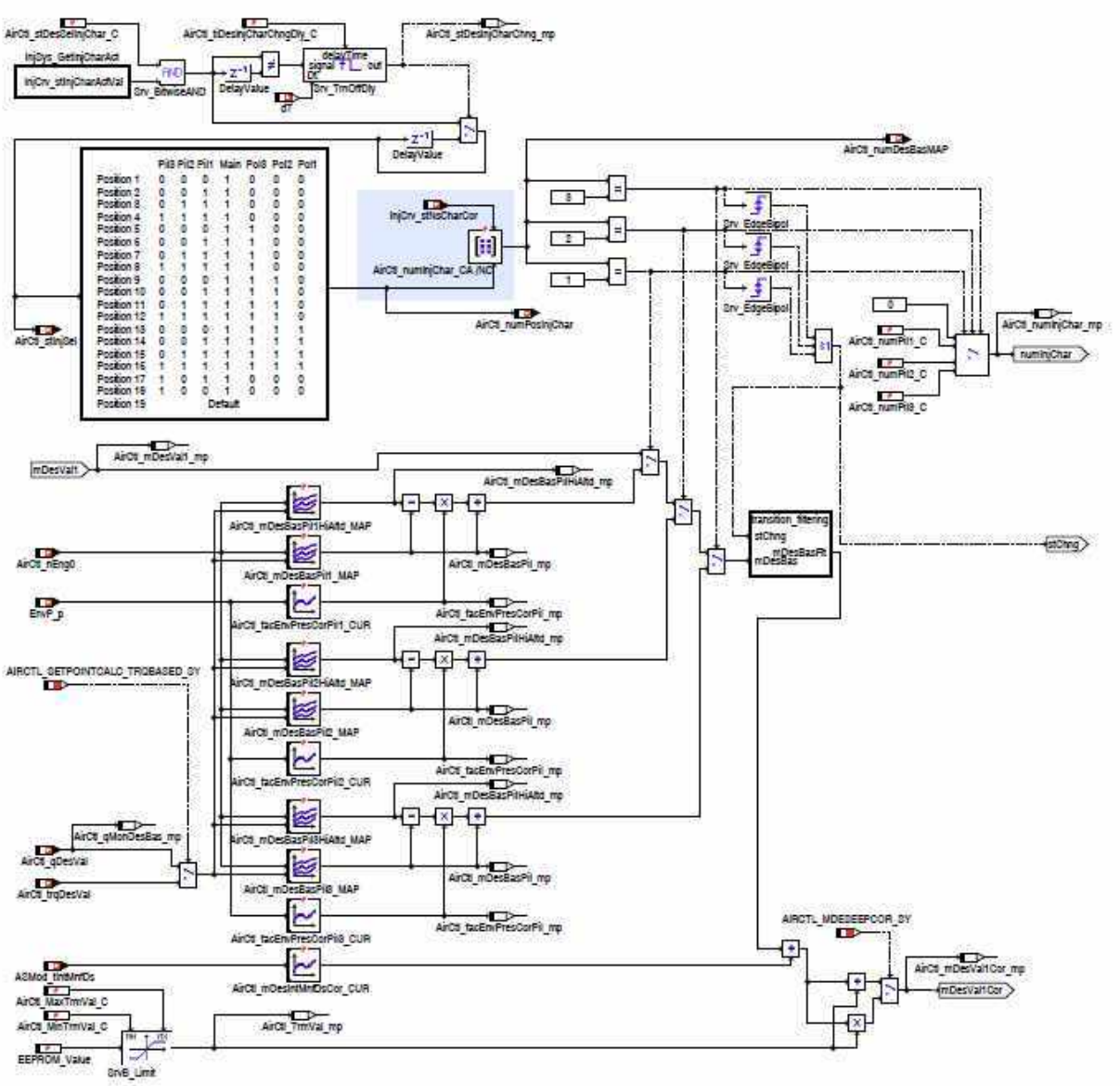


Abbildung 11: Akustische Bedingung (Signal **InjCrvst_NsCharCor**), dient der Steuerung der gewünschten Luftmassenkorrektur **mDesVal1Cor**, welche die gewünschte Luftmasse abändert, aus denen die Menge der rezirkulierten Luft berechnet wird. **AirCtl_numInjCharCA** ist ein zwei-dimensionales Array. Die akustische Bedingung wird verwendet, um eine jeweilige Zeile auszuwählen. Aus dem Funktionsblatt **EDC17C54 P 874**. Hinterlegung durch die Autoren hinzugefügt. Copyright Robert Bosch GmbH.

(Der folgende Text ist nicht in der PDF-Datei sichtbar, wurde jedoch konvertiert, Anmerkung des Übersetzers)
*Dies ist sichergestellt über eine Abfrage mit der Maske **NSCRgn_stDNOxMsk_C** aus dem Statuswort der Betriebssystem-Modi-Koordinator **CoEOM_stOpModeAct**. Der Messpunkt **NSCRgn_stDNOxActv_mp** zeigt den Status einer DNOx-Regeneration an. Falls **NSCRgn_stIntrMADDNOx_mp=TRUE** gilt, wird die DeNOx-Regeneration abgebrochen.*

Bedingungen für die Aktivierung zur Auslösung des DeNO$_x$-Ereignisses während des Homologationszyklus

Abbildung 5444
NSCRgn_RlsLogic/NSCRgnRlsLogic/RegenerationReleaseLogic/ReleaseLogicDNOx/DNOx_during_Homologation [NSCRgn_RlsLogic.NSCRgn- RlsLogic.RegenerationReleaseLogic.ReleaseLogicDNOx.DNOx_during_Homologatio]

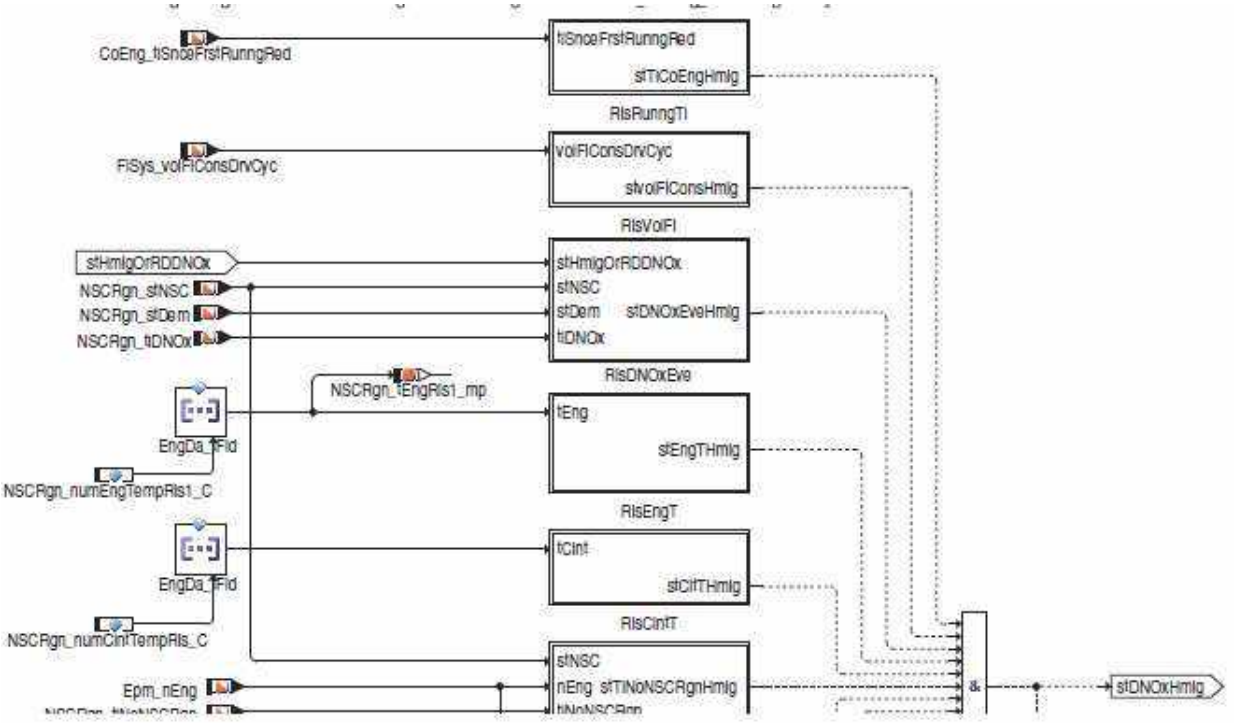


Abbildung 12: Teil der NO$_x$-Regenerationslogik während des „Homologationszyklus“ aus dem Funktionsblatt EDC17C69 für Fiat 500X. Das Homologationsfreigabesignal benötigt mehrere Signale für den Nachweis, einschließlich **stTiCoEngHmlg** (Abschnitt IV-D). Dies erfolgt nur, wenn die Motorlaufzeit den Wert für **NSCRgn_tiCoEngMaxHmlg_C** (eingestellt auf 1600 Sekunden) im Firmware-Image 55265162 Fiat 500X nicht überschreitet. Copyright Robert Bosch GmbH.

Abbildung 5456
NSCRgn_RlsLogic/NSCRgnRlsLogic/RegenerationReleaseLoRgilscN/REnegleaseLogicDNOx/DNOx_during_real_driving [NSCRgn_RlsLogic.NSCRgnRls-NSCRgn_numEngTempRls2_Cogic.RegenerationReleaseLogic.ReleaseLogicDNOx.DNOx_during_real_driving]
(Der folgende Text ist nicht in der PDF-Datei sichtbar, wurde jedoch konvertiert, Anmerkung des Übersetzers)

Die DNOx-Regeneration während des Homologationszyklus wird ausgelöst, wenn eine von vier Bedingungen erfüllt ist:
Motorlaufzeit im aktuellen Fahrzyklus ist weniger oder gleich dem Schwellenwert

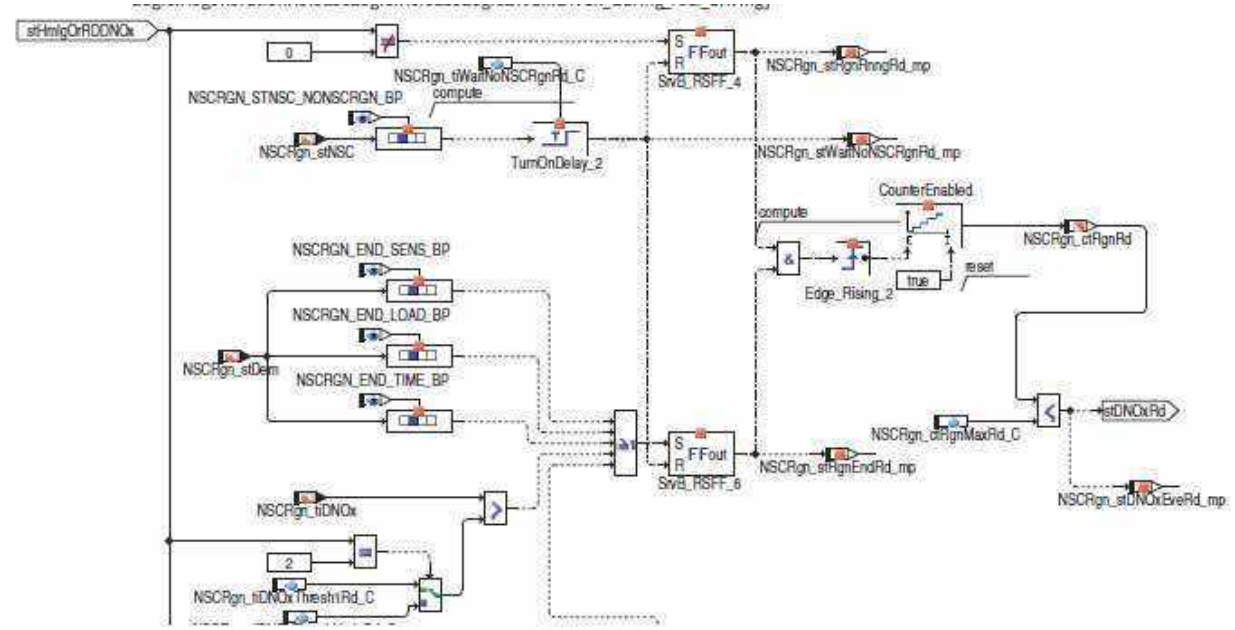


Abbildung 13: Erstes Element steuert je nach Motorlaufzeit. Ein paralleler Logik-Baustein steuert die Freigabe „während der echten Fahrt“. Copyright Robert Bosch GmbH.

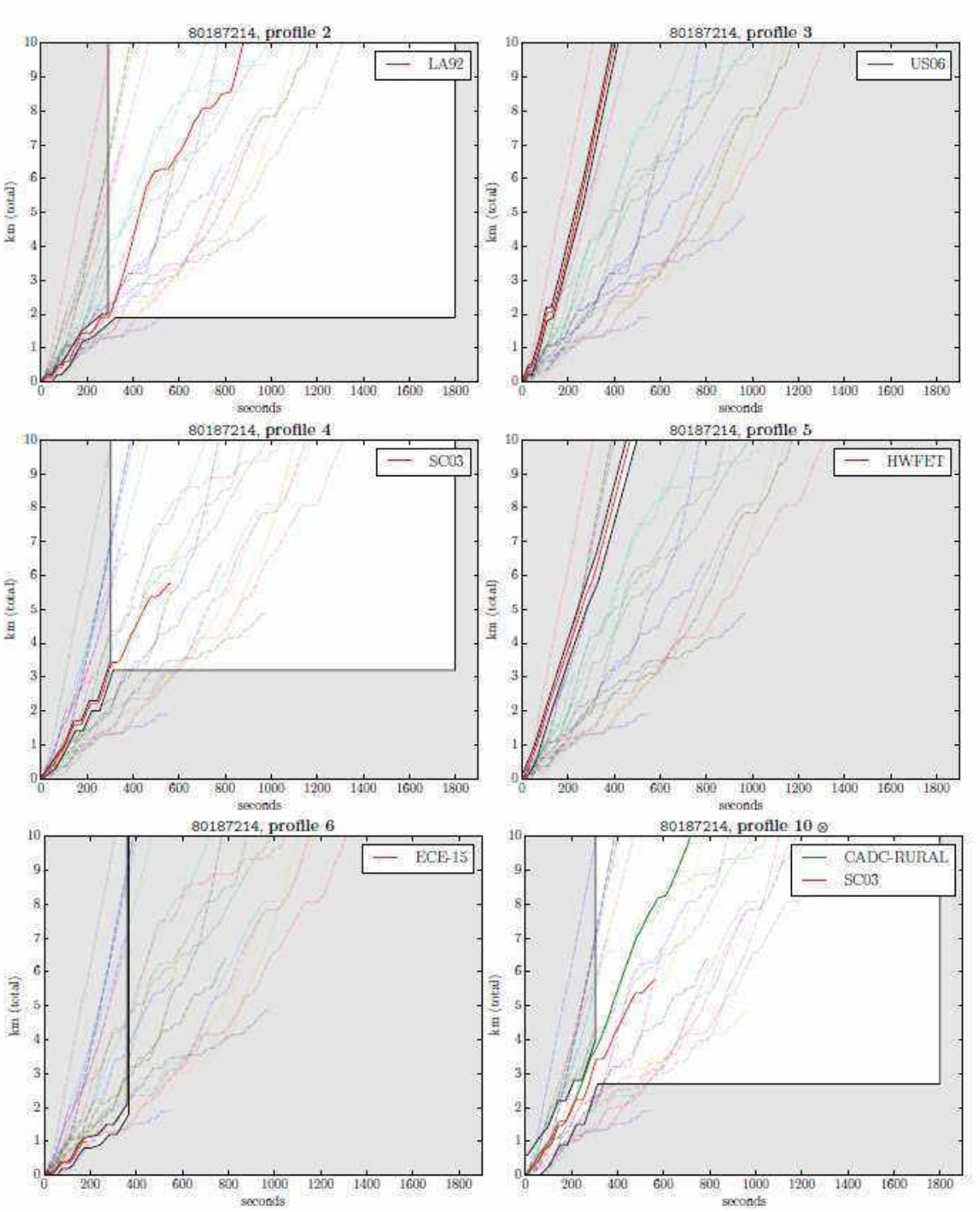


Abbildung 14: Verbleibende Kurvenkontrollprüfungen gegen verschiedene Emissionsprüfzyklen in der Firmware für einen VW Passat, 12/2014 (EDC17C54, Software-Teilenummer 03L906012, Revision 7444), ergänzt Abbildung 3. Der Bereich, in dem die Software meldet, dass das Fahrprofil übereinstimmt, ist weiß gefärbt. In der Legende werden die bekannten übereinstimmenden Prüfzyklen aufgeführt, (X) zeigt an, dass eine zusätzliche Lenkradeinschlagprüfung erfolgt.