Trends in der Regulatorik: Fokus autonomes Fahren

Trends in der Regulatorik

Technische Compliance wird für Unternehmen immer wichtiger. Insbesondere die Regulation von Software nimmt deutlich zu. Aktuelles Beispiel aus der Autobranche: die Absicherung der Sollfunktion (SOTIF) digitaler Sensor- und Steuersysteme in Fahrzeugen (ISO-21448).

Eine wachsende Anzahl von Produktfunktionen wird heute digital realisiert. Das hat weitreichende Implikationen für die Sicherheit und geht daher auch mit neuen regulatorischen Vorgaben einher. Für klassische „Hardware-Hersteller", wie viele OEMS und Zulieferer, liegt darin eine große Herausforderung. Sie müssen sich digital weiterentwickeln und als Industrieunternehmen zugleich das Kompetenzspektrum eines Software-Herstellers aufbauen.

Durch den Wandel von einem v.a. durch Hardware definierten Produkt hin zu einer digtalen Platttform, deren Funktionalität immer mehr durch Software bestimmt wird, ändert sich die Sichtweise auf das Produkt – das Fahrzeug – und auch das Geschäftsmodell der OEMs. Der Fokus des Geschäfts – und künftig wohl auch der Margenerwartungen der OEMs – bewegen sich vom reinen Fahrzeugverkauf in Richtung Aftermarket und den dort, meist auf Software basierenden, Möglichkeiten. Das erfordert auch ein Umdenken oder gar eine Neudefinition der Compliance bezogenen Betrachtung des Produkts. Die Anforderungen werden höher und es sind mehr Rechtsgebiete einzubeziehen. Vor allem aber ist der gesamte Produktlebenszyklus zu betrachten, da die Verantwortung des OEMs nach dem Verkauf und der Garantiezeit nicht endet, sondern völlig neu definiert wird. Die neuen Herausforderungen reichen von den produktbezogenen Compliance-Einheiten der Organisation über die Typzulassung bis hin zur technischen Weiterentwicklung des Produkts (z.B. über neue Software-Funktionen) im Markt und beziehen Entwicklung, Produktion, Vertrieb, Aftersales und Teile der Supply Chain mit ein, die neue, agile Modelle der Zusammenarbeit entwickeln müssen, um erfolgreich bestehen zu können.

In der utomobilbranche sind es die aktuellen zukunftsweisenden Trends wie das vernetzte Fahrzeug, Elektromobilität, Car Sharing und vor allem autonomes Fahren, die eine erhöhte regulatorische Aufmerksamkeit auf sich ziehen und OEMs unter Handlungsdruck setzen. Demnächst sind beispielsweise durch die neuen Regulationen UNECE R155 und R156 ein Cyber Security Management System (CSMS) sowie ein Software Update Management System (SUMS) vorgeschrieben, die in den ersten beiden Beiträgen dieser „Point of View"-Reihe erläutert werden (vgl. PoV R155, PoV R156). Neu ist die Vorschrift zu ALKS (Automated Lane Keeping System), die die vorgenannten Regelungen als UNECE R157 ergänzen wird. Letztere Regulierung ist Teil der Entwicklung zum automatisierten Fahren und Voraussetzung für die Umsetzung von autonomen Fahren Level 3.

Für die Zukunft setzt das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) mit dem Gesetzesvorhaben zum autonomen Fahren noch einen zusätzlichen regulatorischer Schwerpunkt, der im Folgenden im Mittelpunkt stehen soll: der Themenkomplex „Sicherheit der Sollfunktion" (ISO-21448), d.h. die kontinuierliche Gewährleistung einer sicheren Funktion von Sensoren und Algorithmen. *Der Entwurf wurde im Februar 2021 vom Bundeskabinett gebilligt.*

Die Regulatorik wird dichter

OEMs befinden sich heute ganz allgemein in einer Situation, in der die Bedeutung der Compliance zunimmt. Immer mehr Regulationen sind zu beachten. Spätestens seit den in der Öffentlichkeit viel diskutierten Skandalen hinsichtlich des Schadstoff-Ausstosses von Diesel-Aggregaten, ist das Bewusstsein dafür in Branche sowie bei den Kunden deutlich gestiegen. Damit hat sich auch das Verständnis von Compliance und den damit zusammenhängenden ablauforganisatorischen Vorkehrungen signifikant gewandelt. Standen früher eher „klassische" Themen wie Korruption und Bestechung im Compliance-Fokus, geht es heute verstärkt auch um die Einhaltung technischer Vorschriften. Technische Compliance oder Produkt-Compliance werden daher immer wichtiger, um zulassungsrelevante Vorschriften zu überwachen und zum frühestmöglichen Zeitpunkt Erkenntisse zu Funktionen und Fahrzeugverhalten zu gewinnen und daraus neue und geänderte Produktanforderungen abzuleiten. Nur so sind die Voraussetzungen für die Typzulassung von Fahrzeugen sicherzustellen. Dabei ist zu beachten, dass viele Produkte mit softwarebasierten Anwendungen (darunter auch PKW und LKW) auch nach Produktionsstart weiterentwickelt werden, allein um funktionale Erweiterungen und Updates aus Sicherheitsgründen zu realisieren. Letztere sind mit der schon erwähnten SUMS-Regulation (UNECE R156) ab 2022 für neue Fahrzeuge in Europa sogar gesetzlich vorgeschrieben. Demnach ist es nicht ausreichend, dass sich technische Compliance oder Produkt-Compliance auf die Entwicklungsphase eines Produkts konzentriert – der gesamte Produkt-Lebenszyklus muss betrachtet werden. Technische Compliance ist dabei nicht nur dezentral relevant, also etwa in der Entwicklung von Software und Hardware in den entsprechenden Bereichen. Nun muss sich z.B. in großen OEMs auch die „Second Line of Defense" technisches Knowhow erwerben, sowohl im Hinblick auf Forensik als auch auf Prävention.

Ein weiterer konkreter Treiber ergibt sich aus dem deutschen Verbandssanktionengesetz. Unter dem Titel „Gesetz zur Stärkung der Integrität in der Wirtschaft" wurde es 2020 verabschiedet. Damit wird eine Art Unternehmensstrafrecht geschaffen, das Straftaten aus „Verbänden" (dieser Begriff umfasst auch Unternehmen jeglicher Rechtsform) heraus mit hohen Sanktionen ahndet, wenn keine ausreichenden Compliance-Vorkehrungen aufgebaut wurden. Andererseits sind nun aber auch positive Auswirkungen möglich: Wenn die entsprechende Compliance geschaffen wurde und nachgewiesen wird, wirkt sich dies in der Schwere der Sanktionierung mildernd aus.

Vor dem Hintergrund dieser verdichtenden Regulatorik gewinnt das Compliance Monitoring deutlich an Wichtigkeit. Eine vorausschauende Übersicht und Analyse der sich entwickelnden regulatorischen Landschaft (weltweit) ermöglicht eine frühzeitige Vorbereitung auf Änderungen und Verschärfungen. Dabei ist eine internationale Perspektive zwingend, was die Anforderungen des Monitorings noch erhöht. Wichtig ist beim Compliance Monitoring auch die praktische Anschlussfähigkeit für die einzelnen Domänen des Unternehmens. Juristen mit technischem Compliance-Fachwissen analysieren die Regelwerke, erstellen daraus Datenbanken für verschiedene Domänen und Bereiche und machen die Implikationen für Ingenieure nachvollziehbar und umsetzbar. An die Compliance Funktion wird hier die Anforderung gestellt, sich als integraler Bestandteil der Produktentwicklung zu verstehen und sich in die modernen Entwicklungsprozesse mit ihren agil und skaliert agilen Vorgehensweisen einzubringen.

Aufgrund der sich verdichtenden Regulatorik gewinnt das Compliance Monitoring deutlich an Wichtigkeit. Eine vorausschauende Übersicht und Analyse der sich entwickelnden Regulatorik ermöglicht eine frühzeitige Vorbereitung auf Änderungen und Verschärfungen.

Die Sicherheit digitaler Funktionen

Das neue Gesetzesvorhaben des BVMI stellt ein prominentes Beispiel der dichter werdenden Regulatorik in der Automotive-Branche dar. Im Entwurf wird in Appendix 1 zum Anhang darauf verwiesen, dass eine autonome Fahrfunktion ausreichend abgesichert sein muss. Dadurch sollen unakzeptable Risiken vermieden werden, die durch Unzulänglichkeiten der gewollten Funktionalität (Sollfunktion, intended function) oder durch vorhersehbaren Gebrauch (Fehlgebrauch, der vernünftigerweise vorhersehbar ist) entstehen können. Die Sicherheit der Sollfunktion (Safety of the intended function, SOTIF) kann der Hersteller laut Gesetzentwurf z.B. nach dem neuen Standard ISO 21448 nachweisen (s.u.). Die Regulation hat erhebliche Implikationen: Wenn das bestimmungsgemäße Funktionieren einer Software kritisch für die Sicherheit im Sinne der Safety ist, dann muss eine kontinuierliche Überwachung der Funktion stattfinden. Sicherheitsmaßnahmen müssen auch unter nicht antizipierten Umständen greifen: Ein Fahrzeug bewegt sich vielleicht in Rahmenbedingungen, die so nicht vorsehbar waren. Ein selbstlernendes System beobachtet dabei die Sollfunktion ständig und bewertet, ob sie noch gewährleistet ist – oder ob bestimmte Umstände wie z.B. Nebel die Sicherheit der Sollfunktion gefährden. In solchen Situationen muss ein Zurückschalten auf einen sicheren Fahrfunktions-Level möglich sein, z.B. durch Übergabe an den menschlichen Fahrer.

Ein aufsehenerregender Unfall der letzten Zeit verdeutlichte die Problematik und schärfte das Bewusstsein dafür auch über die Branche hinaus nachhaltig: Ein Elektro-PKW kollidierte bei guter Sicht auf einer Landstraße mit einem weißen LKW, der die Strecke querte. Der PKW-Fahrer war anderweitig beschäftigt. Der Wagen wurde durch einen automatisierten Modus gesteuert, der eine Freigabe lediglich für die Autobahn hatte. Auf querende Fahrzeuge war die Funktion nicht eingestellt, da dies auf Autobahnen kein relevantes Szenario ist; den weißen LKW erkannten die Systeme nicht als solchen. Das Problem lag darin, dass eine Funktion unter Umständen aktiviert werden konnte, für die sie nicht vorgesehen war (Landstraße statt Autobahn). Genau solche Ereignisse muss die Kontrolle der Sollfunktion verhindern, z.B. indem die situativen Umstände ebenfalls erfasst und bewertet werden. Dafür ist eine genaue Definition eines Rahmens der Sollfunktion notwendig, um sie im Zweifelsfall abschalten zu können.

Das betrifft nicht nur Softwarefunktionen. Ein weiteres Beispiel für die zunehmende Komplexität der regulatorischen Anforderungen und deren Erfüllung ist in diesem Zusammenhang die aus der ISO-21448 ableitbare Überwachung der Sensor-Degradierung. Heutige Sensoren stellen Funktionsstörungen durch innere oder äußere Einflüsse fest und melden diese an die angeschlossene Steuereinheit. Diese nimmt dann i.d.R. die davon betroffenen Fahrfunktionen (z.B. Spurhalte-Assistent, Abstandshalte-Assistent) – vorübergehend – außer Betrieb und meldet dies an den Fahrer. Wenn Fahrzeuge im Rahmen der Entwicklung autonomer Fahrfunktionen immer mehr Aufgaben – auch dauerhaft – übernehmen, dann werden die Anforderungen an die Verfügbarkeit und Zuverlässigkeit der Systeme (Software, Hardware und Sensorik) ebenfalls höher. Um die kommenden ISO-21448 Anforderungen erfüllen zu können, reicht die bisherige Ausfallabsicherung nicht mehr aus. Es muss z.B. auch eine schleichende, möglicherweise gebrauchsbedingte Sensordegradierung erkannt und durch das System soweit wie möglich ausgeglichen werden. Eine laufende Überprüfung ist, beispielsweise im Falle eines Kamera-Sensors, durch das individuelle Aufbauen von Referenzbildern je Fahrzeug möglich. Dazu wird an bestimmten, über das Navigationssystem festgehaltenen Punkten ein Referenzbild eines neuen Sensors im System gespeichert und über einen Vergleich (wenn das Fahrzeug wieder an der gespeicherten Stelle vorbeikommt) mit einem aktuellen Bild ein möglicher Qualitätsverlust festgestellt. Da diese permanente Selbstüberprüfung nicht immer gleichermaßen möglich ist, sollte zusätzlich eine externe Überprüfung – beispielsweise im Rahmen der Hauptuntersuchung – eingeplant werden.

Bei der Betrachtung der Sicherheit der Sollfunktion sind außerdem auch Cyber Security-Aspekte relevant und damit das schon erwähnte Cyber Security Management System (PoV CSMS). Ebenso ist für die Aufrechterhaltung von Funktionen, wie ebenfalls schon angesprochen, ein leistungsfähiges Software Update Management System (PoV SUMS) nötig. Letztlich greifen beim Thema Software die verschiedenen regulatorischen Aspekte ineinander. Auch der oben beschriebene Einsatz von selbstlernenden Systemen in Fahrzeugen wird durch die zunehmende Regulatorik weiter voranschreiten, da konventionell entwickelte Software nicht flexibel genug ist und in den Algorithmen nur bereits vorgedachte Situationen abbildbar sind. Genau hier geht die ISO-21448 jetzt einen Schritt weiter. Systeme, die auf künstlicher Intelligenz basieren (hier: neuronale Netzwerke, maschinelles Lernen), erzeugen jedoch neue Herausforderungen für Entwicklung, Test und Wartung bzw. Weiterentwicklung betreffender Fahrzeuge. Für KI-Systeme ist derzeit eine separate Regulierung im Entstehen begriffen.

Ein Standard und seine Folgen

Der Standard ISO 21448, auf den der Gesetzentwurf Bezug nimmt, ist als globaler Standard konzipiert und befindet sich noch in der Entwicklung. Die ISO 21448 existiert länger in einer Vorläufer-Version als PAS und wird seit 2016 in Fahrerassistenzsystemen implementiert (Level 1). Es handelt sich um den zentralen Standard, intendiert als eine Ergänzung zum bestehenden Standard ISO 26262 zur funktionalen Sicherheit. ISO 21448 stellt Konzepte und Best Practices für Systeme dar, die selbsttätig Daten sammeln bzw. verarbeiten, und bei denen eine komplexe Wechselwirkung der verschiedenen Komponenten vorliegt. Ziel dieses Ansatzes ist eine Vermeidung bzw. Verringerung von Schäden durch Minimierung von unbekannten und potenziell gefährlichen und bekannten gefährlichen Verhaltensweisen des Systems. Triggerbedingungen für das Abschalten der Funktion, potenzielle Schwachstellen der Sollfunktion und mögliches Missbrauchsverhalten müssen definiert werden. Die Überwachung des Fahrer-Status gehört ebenfalls zu den erforderlichen Sicherheitsmaßnahmen. Da in der Praxis nicht alle möglichen Kausalketten bei der Sicherheitsanalyse erfasst werden können, sollte das sich daraus ergebende Risiko aus ISO-21448-Sicht auch durch Testen, Simulieren und statistische Analyse reduziert werden. Im Gesetzentwurf werden in Appendix 5 außerdem Anforderungen an die Kommunikation gestellt, wie etwa die Bereitstellung von drei separaten Funkdatenverbindungen. Auch für die Datenspeicherung werden Regelungen aufgestellt (Appendix 3): Im Fahrzeug müssen Ereignisdaten in nicht-flüchtigem Speichern abgelegt werden, hierzu werden ergänzend Standards und Notfallprozesse definiert.

Auch wenn die neue Gesetzeslage gestaffelt eingeführt werden wird und nicht in allen Punkten zum gleichen Zeitpunkt schon verbindlich sein wird, müssen sich die OEMs bereits jetzt darauf einstellen. Dass grundlegende Implikationen für den Entwicklungsbereich abzuleiten sind, liegt auf der Hand. Die Verantwortung für die Entwicklung erstreckt sich nun auch auf den Aftermarket – d.h. auf den gesamten Lebenszyklus eines Fahrzeugs. Kontinuierliche Verbesserungen (z.B. Bugfixes), ein permanentes Monitoring der Fahrzeuge sowie eine Weiterentwicklung im laufenden Betrieb sind nun zusätzlich im Fokus der OEMs.

Eine mögliche Rückwirkung der genannten Regulierungen auf schon bestehende oder bereits in Entwicklung befindliche Fahrzeugplattformen kann hohen Aufwand für Aktualisierungen oder notwendige Zusatzmaßnahmen (z.B. Abschirmen von scherheitskritischen Funktionen in älteren Architekturen) mit sich bringen. Wie bereits erwähnt, macht die Einhaltung der Vorschriften eine Überwachung der Fahrzeugflotte im Feld erforderlich. Diesem Erfordernis begegnet man durch die Schaffung eines Vehicle Security Operations Center (VSOC), das diese Aufgabe übernimmt. Prozesse zur Sicherstellung von Maßnahmen bei auftretenden Zwischenfällen (z.B. Hacker-Angriffe oder schwerwiegende Fehlfunktionen) und Prozess für wichtige, zeitkritische Updates müssen definiert werden, einschließlich eines sicheren Datentransfers. Wesentliche rechtliche Risiken müssen identifiziert und Gegenmaßnahmen getroffen werden – daraus ergeben sich zum Beispiel Fragen nach der Haftung bei einem abgelehnten Update (entsteht hieraus hieraus ggf. sogar die Pflicht, ein Fahrzeug stillzulegen?).

Die Compliance-Vorgaben haben signifikante Folgen für die Typzulassung: Durch Verstöße kann diese nachträglich erlöschen. Daher müssen die Homologations- und Typzulassungsprozesse angepasst werden, um Risiken für im Markt befindliche Fahrzeuge abzudecken. Daraus ergibt sich die unmittelbare Notwendigkeit weiterführende Lösungen für die technischen und prozessualen Abhängigkeiten bis in die komplexen Lieferketten zu verankern. Da sich Lieferanten nach den OEM-Prozessen ausgerichtet haben, ist ein neuerliches Alignment erforderlich. Dies betrifft vor allem die gemeinsame Software-Entwicklung und damit die bisher wenig beachtete Entwicklungsphase nach dem SoP. Die regulatorischen Anforderungen sind bisher wenig durchgängig bis auf die verschiedenen Ebenen der Lieferkette implementiert. Hauptgrund dafür ist die immer noch unterschätzte gemeinsame regulatorische Verantwortung z.B. im Sinne der Produkthaftung. Diese erfordert eine klare Verteilung der Rollen und Verantwortlichkeit um z.B. eine lückenlose Nachweisbarkeit und Dokumentation der Umsetzung von regulatorischen Anforderungen abzusichern. Mit den Zulieferern sind Absprachen über Verantwortungen und Zeiträume (End of Life [EOL], End of Service [EoS]) zu treffen; Prozessuale Schnittstellen und Zugang zum Produkt sind zu regeln, damit ein Zulieferer seiner Verpflichtung zum Updae nachkommen kann.

Durch die erweiterte Verantwortung über die gesamte Lebenszeit des Produkts ergeben sich neue Kostenrisiken mit vielen Unbekannten: die Infrastruktur zur Überwachung der Fahrzeugflotten muss aufgebaut werden, Datenanalyse-Verfahren, um Hacker-Angriffe von Qualitätsproblemen unterscheiden zu können und Prozesse zur Reaktion auf erkannte Verdachtsfälle sind zu etablieren und zu optimieren. Letztendlich könnte der größte Kostenfaktor aber die zuverlässige und zeitnahe Versorgung aller Fahrzeuge mit Updates werden, da voraussichtlich verschiedene Updateverfahren parallel in Betrieb sein werden (OTA, etc.), Lieferanten zuliefern müssen und ein erheblicher Testaufwand entsteht – u.a. auch zur Absicherung des Erhalts der Typzulassung, wie oben bereits beschrieben. Da die Anzahl und die Komplexität der verpflichtenden Updates (Bugfixes) im Voraus nicht bekannt sind und auch keine Erfahrungswerte existieren, baut sich hier ein erhebliches Kostenrisiko auf, das die Verkaufsmargen je Fahrzeug der OEMs erheblich unter Druck setzen wird. Umso wichtiger ist es, diesem Kosten- bzw. Margenrisiko mit neuen Geschäftschancen ein zusätzliches Margenpotential gegenüberzustellen. Dies erfordert die konsequente Nutzung der für verpflichtende Updates ohnehin aufzubauenden Infrastruktur, aber auch einen Plan für die (software-seitige) Weiterentwicklung von Fahrzeugen im Markt und den Verbau der dafür notwendigen Hardware in diesen Fahrzeugen (Hardware-Vorhalt). Durch diese Entwicklungen verändert sich nicht nur der Zeitpunkt, sondern auch die Art der Margengenerierung. Wenn sich Margen aus dem Fahrzeugverkauf in den Aftermarket verlagern – das heißt, dass das Fahrzeug immer mehr zur Plattform für zusätzliches Geschäft wird, dann entstehen auch neue Anforderungen an den Vertrieb- und Aftersales-Organisationen, die beide vor allem auf das technsiche Produkt an sich, aber nicht auf Geschäftschancen auf Basis dieses Produkts fokussiert sind. Neue digitale Geschäftsmodelle erfordern hier ein neues Denken.

Dieses neue Denken hat hohe Dringlichkeit, da das daraus resultierende Geschäftsmodell unmittelbar von der Fahrzeugarchitektur und den damit verbundenen marktbezogenen Strategien unterstützt werden muss. Die Produktkalkulation muss den Fokus auf den gesamten Produkt-Lebenszyklus genauso unterstützen wie die Variantenplanung in der Fahrzeugausstattung, die – zumindest was die Hardware angeht – ihre Komplexität deutlich reduzieren und die notwendige Funktionalität und Leistung für das Geschäft im Aftermarket bereitstellen muss. Nur so kann die Transformation des Fahrzeugs zu einer Geschäftsplattform mit Kunden erfolgreich sein.

Unterm Strich sind eine Vielzahl von Geschäftsprozessen auf die neuen Gegebenheiten vorzubereiten sowie neue Formen der Zusammenarbeit zu etablieren. Wir haben in diesem Beitrag einige neue Regularien für die (software)technische Gestaltung von Fahrzeugen herausgegriffen und potentielle Auswirkungen auf das Geschäftsmodell der OEMs aufgezeigt. Weitere relevante Regelungen und Standards wurden nicht oder nur oberflächlich behandelt – dies sind zum Beispiel:

- Für die Software-Entwicklung ist allgemein der Standard IEC 61508 einschlägig.
- In Form der Regulierung UNECE Automated Lane-Keeping Assistant Systems (ALKS) liegt schon eine spezifische Ausdifferenzierung von ISO-21448-Aspekten vor, die u.a. autonomes Fahren bis Level 3 betrifft.
- Mit ISO/PRF TR 4804 ist außerdem ein Standard veröffentlicht worden, der aus den Sicherheitsprinzipien einer Vielzahl regulatorischer Vorschriften ein Regelwerk für die Sicherheit beim autonomen Fahren bündelt.

Um nur einige Beispiele zu nennen. Insofern ist Compliance – hier insbesondere Product-Compliance oder Technical Compliance – ein wesentlicher Bestandteil von erfolgreichen Product-Launches oder Marktstrategien.

Die Internalisierung von Verantwortung, Risiken und Haftung

In der aktuellen regulatorischen Situation sehen sich OEMs genötigt, ihre Compliance-Strukturen zu erneuern. Der gesetzgeberische Trend geht zu einer Ausweitung der Vorschriften, und damit steigen die Risiken der Hersteller. Das führt aus Herstellersicht generell zu einer Internalisierung der Haftung – der Fahrer wird tendenziell enthaftet. Diese Zuspitzung müssen sich OEMs jetzt dringend bewusst machen und ihre Markt- und Produktstrategie darauf abstellen. Security und Safety überschneiden sich in Zukunft in immer größerem Maße. Die Perspektive der Entwicklung verändert sich, Software-Qualität muss ins Zentrum der Aufmerksamkeit rücken. Den Rahmen dafür liefert eine neu strukturierte *Software Governance* im Unternehmen. Ergänzend dazu ist ein vorausschauendes regulatorisches Monitoring eine der wichtigsten Voraussetzungen für einen erfolgreichen Compliance-Ansatz; die Experten von Deloitte unterhalten zu diesem Zweck ein ausgedehntes Netzwerk in Gremien und Verbänden. Technische Hilfsmittel – bei Deloitte: die Dienste des *aiStudios* oder des *RegTechLabs* – liefern dabei eine wertvolle Unterstützung für den Wandlungsprozess (LINKS AI Studios, RegTechLab).

Kontakte

Andreas Herzig
Partner
Automotive Lead Risk Advisory
Tel: +49 (0)711 16554 7160
aherzig@deloitte.de

Dorit Schroeren
Partner | Risk Advisory
Lead Regulatory and Compliance
Tel: +49 (0)211 8772 4108
dschroeren@deloitte.de

Anke Guderian
Director | Risk Advisory
Automotive Software Governance
Tel: +49 (0)89 29036 6212
aguderian@deloitte.de

Ingo Dassow
Director | Risk Advisory
Automotive Cybersecurity
Tel: +49 (0)151 58801451
idassow@deloitte.de

Deloitte.

Stand 04/2021