VOLKSWAGEN

AKTIENGESELLSCHAFT

Konzern Grundanforderungen Software

Grundanforderungen, die der Volkswagen-Konzern an im Fahrzeug verbaute und fahrzeugbezogene Software/softwarebestimmt Systeme und deren Entwicklungsprozesse stellt.

Technische Entwicklung, Querschnittslastenheft: LAH.893.909

Erstausgabe	06.09.2002
Änderungsstand	05.05.2023
Lastenheftversion	4.1

Inhaltsverzeichnis

1 Vorwort ... 4
1.1 Zielsetzung ... 4
1.2 Besitzer dieses Dokumentes ... 4
1.3 Cybersecurity Incident Management ... 5
2 Geltungsbereich ... 6
3 Rechte des Auftraggebers und Pflichten des Auftragnehmers ... 7
4 Terminologie ... 9
4.1 Feature ... 9
4.2 System ... 9
4.3 Systemelement ... 9
4.4 Software ... 9
4.5 Softwareelement ... 9
4.6 Komponente ... 10
4.7 Unit ... 10
4.8 Unitelement ... 10
4.9 Modellelement ... 11
4.10 Weitere Definitionen ... 11
5 System- und Softwareentwicklung ... 13
5.1 Prozessübergreifende Anforderungen ... 13
5.2 Projektmanagement ... 14
5.3 Dokumentation des Lieferumfangs ... 15
5.4 System- und Softwareanforderungsspezifikation ... 16
5.5 System- und Softwarearchitekturspezifikation ... 17
5.6 Softwarefeinspezifikation (Detailed Design) ... 18
5.7 Softwareerstellung ... 19
5.7.1 Programmiersprachen ... 19
5.7.2 Manuelle Quellcodeerstellung ... 20
5.7.2.1 Quellcodemetriken ... 21
5.7.3 Grafische und modellbasierte Programmierung ... 22
5.7.3.1 Metriken für Grafische Programmierung ... 22
5.7.4 Maschinelles Lernen (ML) ... 23
5.7.4.1 Terminologie ... 23
5.7.4.2 Datenakquise ... 24
5.7.4.3 Training und Testing ... 25
5.7.5 Tool-Qualifizierung ... 26
5.7.6 Nachprüfung der Anforderungen der Softwareerstellung ... 26
5.8 Test ... 27
5.8.1 Testplanung ... 27
5.8.2 Testfallspezifikation ... 27
5.8.3 Testdurchführung allgemein ... 28
5.8.4 Unittest ... 29
5.8.5 Softwareintegrationstest ... 29
5.8.6 Softwaretest ... 30
5.8.7 Systemintegrationstest ... 30
5.8.8 Systemtest ... 30
5.9 Qualitätssicherung und -management ... 30
5.9.1 Qualitätsmanagement ... 30
5.9.2 Review der Arbeitsprodukte ... 31
5.9.3 Prüfung der Entwicklungsprozesse ... 32
5.10 Konfigurationsmanagement ... 32

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

5.11 Problemlösungsmanagement ... 32
5.12 Änderungsmanagement ... 34
5.13 Software von Dritten ... 34
5.14 Free and Open Source Software ... 35
5.15 Cybersecurity-relevante Entwicklung ... 37
5.15.1 Allgemeine Cybersecurity-Anforderungen ... 37
5.15.2 Cybersecurity-Terminologie ... 37
5.15.3 Cybersecurity-Management ... 40
5.15.4 Cybersecurity-Risikoanalysen und Cybersecurity-Konzept ... 40
5.15.5 Cybersecurity-Risikomanagement ... 41
5.15.6 Cybersecurity-Architektur und Cybersecurity-Design ... 41
5.15.7 Cybersecurity-Implementierung ... 42
5.15.8 Cybersecurity-Integration und Cybersecurity-Verifikation ... 43
5.15.9 Cybersecurity-Nachweis ... 43
5.15.10 Cybersecurity-Aktivitäten nach der Entwicklungsphase (Serien-/Feldbetreuung) ... 44
6 Referenzierte Unterlagen ... 46
6.1 Dokumente der Volkswagen AG ... 46
6.2 Dokumente des Verbands der Automobilindustrie (VDA) ... 47
6.3 Dokumente der MISRA ... 47
6.4 Internationale Standards und Normen ... 47
7 Release Notes ... 48
8 Vertraulichkeitshinweis ... 49

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

1 Vorwort

1.1 Zielsetzung

[I: KGAS_4110]

Die KGAS definiert den von der Volkswagen AG vorgegebenen Rahmen, um die Entwicklung einer Software, für den Einsatz im Fahrzeug und im Fahrzeugumfeld, nach Stand der Technik sicher zu stellen.

[I: KGAS_4111]

Als Grundlage für die Softwareentwicklung nach Stand der Technik dient das Prozessmodell Automotive SPICE® (siehe KGAS_3887).

[I: KGAS_4112]

Die KGAS präzisiert anhand von Prozessanforderungen das Prozessmodell Automotive SPICE® (siehe KGAS_3887).

[I: KGAS_4113]

Die KGAS richtet sich an alle Projektbeteiligten eines Softwareentwicklungsprojektes.

[I: KGAS_4114]

Die KGAS schafft damit die Grundlage, Softwarequalität im Produkt durch stabile Prozesse zu erreichen (siehe KGAS_3043).

[I: KGAS_3090]

Die Methoden, Bewertungsgrundlagen und Konsequenzen der Qualitätssicherungsaktivitäten des Volkswagen Konzerns bei Lieferanten sind in der "Formel Q Fähigkeit Software" (KGAS_2834) beschrieben.

[I: KGAS_3633]

Die in diesem Dokument verwendeten Begriffe "Auftraggeber" und "Auftragnehmer" sind gleichbedeutend mit den in der Formel Q Fähigkeit Software (KGAS_2834) verwendeten Begriffen "Kunde" und "Lieferant".

1.2 Besitzer dieses Dokumentes

[I: KGAS_2085]

Volkswagen AG
Konzern Qualität
Qualität Software
Brieffach 81250
38436 Wolfsburg
Deutschland

Kontakt: software.qualitaet.vwag.r.wob@volkswagen.de

Audi AG
Qualitätssicherung Fahrzeug-Software
85045 Ingolstadt
Deutschland

Kontakt: software-quality.qq@audi.de

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft

Porsche AG
Elektrik/Elektronik Software
Porschestr. 911
71287 Weissach
Deutschland

Kontakt: software-qualitaet@porsche.de

1.3 Cybersecurity Incident Management

[R: KGAS_3890]

Bei Sicherheitsvorkommnissen ist das Incident Team der Marke oder Region zu benachrichtigen, die die Entwicklungsverantwortung für das betroffene Produkt im Volkswagen Konzern hat. Im Fall einer unklaren Verantwortung ist das Incident Team von Volkswagen PKW (KGAS_3876) zu benachrichtigen.

[I: KGAS_3876]

Volkswagen PKW und Volkswagen Nutzfahrzeuge (leichte Nutzfahrzeuge)

Kontakt: CSI-wob@volkswagen.de

[I: KGAS_3891]

Porsche AG

Kontakt: csi@porsche.de

[I: KGAS_3892]

MAN SE

Kontakt: carsecurity@man.eu

[I: KGAS_3926]

Audi AG

Kontakt: vulnerability@audi.de

[I: KGAS_3958]

Kontakt für die in der Entwicklung befindlichen Produkte: Ansprechpartner ist der jeweilige Projektverantwortliche aus der jeweiligen technischen Entwicklung.

[I: KGAS_3993]

Škoda Auto a.s.

Kontakt: teamcsi@skoda-auto.cz

[I: KGAS_4017]

SEAT S.A.

Kontakt: csi@seat.es

[I: KGAS_3959]

Region China

Kontakt: csi-cn@volkswagen.com.cn

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft

2 Geltungsbereich

[I: KGAS_4057]

Dieses Dokument enthält Anforderungen [A], Informationen [I] und Rahmenbedingungen [R].

[R: KGAS_4058]

Anforderungen sind nachweislich einzuhalten.

[R: KGAS_4059]

Rahmenbedingungen sind einzuhalten.

[I: KGAS_4060]

Informationen dienen dem Verständnis der Anforderungen.

[R: KGAS_25]

Die Anforderungen in diesem Dokument gelten für im Fahrzeug eingesetzte Software/softwarebestimmte Systeme und sonstige fahrzeugbezogene Software/softwarebestimmte Systeme sowie deren Entwicklungsprozesse.

[I: KGAS_3666]

Fahrzeugbezogene Software/softwarebestimmte Systeme beinhaltet alle Softwareanteile, die einen Einfluss auf das Fahrzeug und seine Funktionalitäten haben.

[R: KGAS_3028]

Die Anforderungen in diesem Dokument gelten für den gesamten Volkswagen Konzern.

[R: KGAS_3551]

Die Anforderungen in diesem Dokument sind als vertragliche Verpflichtungen des Auftragnehmers zu verstehen und müssen vom Auftragnehmer als solche erbracht und erfüllt werden.

[R: KGAS_3546]

Steht eine Anforderung der KGAS in Widerspruch zu einer Anforderung aus einer mitgeltenden Unterlage, so muss der Auftragnehmer eine spezifische Vereinbarung zwischen dem Auftragnehmer und dem Auftraggeber initiieren.

[I: KGAS_3899]

Eine Identifizierung der Widersprüche in KGAS_3546 ist u.a. Teil der Analyse der Anforderungen. Siehe dazu auch KGAS_3266.

[R: KGAS_3610]

Vom Auftraggeber als sicherheitsrelevant eingestufte Software und deren Entwicklung unterliegen zusätzlich den Zielen und Anforderungen der ISO 26262:2018 Road vehicles -- Functional safety (KGAS_3895).

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft

3 Rechte des Auftraggebers und Pflichten des Auftragnehmers

[A: KGAS_3885]

Alle Entwicklungsartefakte und Dokumente müssen in englischer oder deutscher Sprache verfasst werden.

[A: KGAS_1806]

Der Auftragnehmer muss auf Anfrage des Auftraggebers Nachweise über die Einhaltung der KGAS erbringen.

[A: KGAS_27]

Der Auftragnehmer muss alle von ihm eingesetzten Unterauftragnehmer auf die Erfüllung der KGAS verpflichten und deren Umsetzung sicherstellen.

[A: KGAS_2933]

Können der Auftragnehmer oder von ihm eingesetzte Unterauftragnehmer die KGAS nicht vollständig erfüllen, muss der Auftragnehmer die Abweichungen schriftlich vor Projektstart durch die Qualitätssicherung des Auftraggebers genehmigen lassen. Die vereinbarten und genehmigten Änderungen sind an die Konzern Qualität (Kontakt siehe KGAS_2085) zu senden.

[I: KGAS_2932]

Nicht genehmigte Abweichungen von den KGAS können dazu führen, dass die Qualitätsfähigkeitsbewertung des Auftragnehmers herabgestuft wird (siehe auch KGAS_2834, "Formel Q Fähigkeit Software").

[A: KGAS_3107]

Sind Abweichungen zu den KGAS bekannt, muss der Auftragnehmer unverzüglich ein Verbesserungsprogramm aufsetzen.

[A: KGAS_42]

Verbesserungsmaßnahmen des Verbesserungsprogramms (KGAS_3107) müssen mit festgelegten Umfängen und Zeitpunkten durchgeführt werden, die mit dem Auftraggeber abgestimmt werden müssen.

[A: KGAS_2184]

Der Auftragnehmer muss sicherstellen, dass dem Auftraggeber die Möglichkeiten zur Einsicht in die System- und Softwareentwicklungsprozesse und alle zusammenhängenden Arbeitsprodukte inklusive des Software-Produkts gegeben sind.

[I: KGAS_3614]

Die Einsicht (KGAS_2184) erfolgt unter Wahrung von Geheimhaltungsverpflichtungen des Auftragnehmers gegenüber Dritten bezogen auf Anforderungen und Inhalte dieser Dritten.

[R: KGAS_1877]

Der Auftraggeber kann seine Einsichtsrechte (KGAS_2184), die sich aus den KGAS ergeben, vollständig oder teilweise durch Dritte wahrnehmen lassen.
Der Auftragnehmer kann verlangen, dass zum Schutz seiner geheimhaltungsbedürftigen Informationen ein aggregierter Bericht durch einen Dritten angefertigt werden kann. Dieser Bericht muss die Bewertung der Qualität der Prozesse des Auftragnehmers gewährleisten. Daher darf nur auf Informationen verzichtet werden, die den konkreten Prozessablauf betreffen.

[I: KGAS_2948]

Der Auftraggeber wird dem Auftragnehmer im Vorfeld einer Beauftragung eines Dritten (KGAS_1877) den Dritten benennen. Dritte in diesem Sinne werden auf inhaltliche Verschwiegenheit verpflichtet und dürfen weder selbst noch dessen verbundene Unternehmen (§15 AktG) Wettbewerber des Auftragnehmers sein. In dem Fall, dass der Auftragnehmer objektiv nachvollziehbare, sachliche Gründe vorbringen und belegen kann, dass die Beauftragung des benannten Dritten für

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

den Auftragnehmer unzumutbar ist, werden sich der Auftraggeber und der Auftragnehmer gemeinsam – unter Berücksichtigung der jeweiligen wirtschaftlichen Interessen – zur weiteren Vorgehensweise abstimmen und ggf. einen anderen Dritten beauftragen. Verbundene Unternehmen des Auftraggebers sind keine Dritten im Sinne dieser Vorschrift.

[A: KGAS_3612]

Der Auftragnehmer muss von Projektbeginn an Metriken erheben. Der Auftragnehmer muss zu jedem Release und auf Nachfrage die Metriken erheben, mindestens aber alle 4 Wochen.

[A: KGAS_3915]

Der Auftragnehmer muss auf Anfrage die erhobenen Metriken dem Auftraggeber zur Verfügung stellen. Das Austauschformat wird durch den Auftraggeber festgelegt.

[A: KGAS_3623]

Die Dauer der Erhebung und die Berichtszyklen können zu Projektbeginn abweichend zu KGAS_3612 durch den Auftraggeber festgelegt werden.

[A: KGAS_4107]

Der Mindestsatz der Projektmetriken ist definiert in KGAS_4093 sofern vom Auftraggeber nicht anders vorgegeben.

[I: KGAS_3916]

Die erhobenen Metriken (KGAS_3915) werden für Freigaben beim Auftraggeber (z.B. Baumustergenehmigung, PPF-Verfahren) herangezogen.

[A: KGAS_4002]

Im Rahmen des PPF-Verfahrens (Produktionsprozess- und Produktfreigabe ehemals Bemusterung) sind die unter (KGAS_4093) enthaltenen Projektmetriken mit der Kennzeichnung „KPIs“ als Nachweis zur Verfügung zu stellen.

[A: KGAS_3624]

Für Prozessabweichungen, die durch den Einsatz der Metriken (KGAS_3612) erkennbar werden, sind Verbesserungsmaßnahmen mit Zielterminen festzulegen.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

4 Terminologie

[I: KGAS_1984]

In diesem Kapitel wird definiert, wie relevante Fachbegriffe im Rahmen der KGAS zu interpretieren sind.

4.1 Feature

[I: KGAS_3665]

Ein Feature ist ein durch einen Stakeholder definierter Funktionsumfang, der durch eine Teilmenge der Anforderungen abgebildet wird.

4.2 System

[I: KGAS_2877]

Das System ist der gesamte vom Auftragnehmer zu erbringende Lieferumfang.

[I: KGAS_2879]

Das System besteht aus Systemelementen.

4.3 Systemelement

[I: KGAS_3604]

Ein Systemelement ist ein logischer Bestandteil eines Systems.

[I: KGAS_3639]

Systemelemente sind in der Systemarchitekturspezifikation beschrieben.

[I: KGAS_3606]

Typische Systemelemente sind Software, Hardware (z. B. Sensoren, Aktoren, Leiterplatten, Bauteile und Verbindungen) und Mechanik (z. B. Gehäuse).

4.4 Software

[I: KGAS_2876]

Software ist die gesamte im Lieferumfang enthaltene Software.

[I: KGAS_3523]

Software besteht aus einem oder mehreren Softwareelementen.

[I: KGAS_2878]

Typische Bestandteile von Software sind Applikation, Treiber, Hardware-Abstraktionen, Betriebssystem, implementierte Algorithmen.

[I: KGAS_2880]

Zur Software zählen auch Plattformelemente, Software von Dritten und programmierte Schaltungen.

4.5 Softwareelement

[I: KGAS_3095]

Ein Softwareelement ist ein Bestandteil der Software mit einer eigenen Spezifikation.

[I: KGAS_3580]

Ein Softwareelement kann aus mehreren Softwareelementen bestehen.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

[I: KGAS_3602]

Ein Softwareelement kapselt logisch zusammenhängende Funktionalität und besitzt definierte Schnittstellen.

[I: KGAS_3640]

Softwareelemente sind in der Softwarearchitekturspezifikation beschrieben.

[I: KGAS_3103]

Ein Softwareelement ist z. B. eine Bibliothek (C, C++, Java) oder eine Funktion auf Applikationsebene (z. B. ABS-Regler, Diagnose).

4.6 Komponente

[I: KGAS_3651]

Eine Komponente ist ein Softwareelement auf der untersten Hierarchieebene.

[I: KGAS_2991]

Eine Komponente besteht aus Units, kapselt logisch zusammenhängende Funktionalität und besitzt definierte Schnittstellen.

[I: KGAS_3641]

Komponenten sind in der Softwarearchitekturspezifikation dargestellt.

[I: KGAS_3642]

Komponenten sind in der Softwarefeinspezifikation beschrieben.

[I: KGAS_3102]

Eine Komponente beinhaltet z. B. eine oder mehrere Quelldateien in C, oder eine oder mehrere Klassen inklusive vererbter Eigenschaften in objektorientierten Programmiersprachen (z. B. C++, Java).

4.7 Unit

[I: KGAS_2998]

Eine Unit ist die kleinste separat ausführbare und testbare Einheit einer Komponente.

[I: KGAS_2989]

Eine Unit kapselt Daten und Anweisungen auf Ebene einer Funktion (C), Methode (C++, Java) oder Prozedur (Pascal).

[I: KGAS_3643]

Units sind in der Softwarefeinspezifikation beschrieben.

4.8 Unitelement

[I: KGAS_3646]

Ein Unitelement ist ein Bestandteil einer Unit (z. B. Berechnung, Schnittstelle, Funktionsaufruf oder Makro).

[I: KGAS_3647]

Unitelemente sind in der Softwarefeinspezifikation beschrieben.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

4.9 Modellelement

[I: KGAS_3527]

Ein Modellelement ist die logische Repräsentation eines oder mehrerer Basisobjekte in einem Tool zur modellbasierten Codegenerierung.

[I: KGAS_3528]

Ein Basisobjekt ist ein atomares Objekt innerhalb eines Tools zur modellbasierten Codegenerierung, das nicht weiter in Unterobjekte teilbar ist.

4.10 Weitere Definitionen

[I: KGAS_3920]

Eigensoftware ist Software, die durch oder für den Auftraggeber entwickelt wurde.

[I: KGAS_3919]

Fremdsoftware ist Software, die keine Eigensoftware ist.

[I: KGAS_3921]

Beistellsoftware ist Software, die der Auftraggeber dem Auftragnehmer im Rahmen der Erbringung der Leistungen zur Verfügung stellt. Dies kann Fremd- oder Eigensoftware sein.

[I: KGAS_3820]

Free and Open Source Software (FOSS) ist jegliche Software, die unter Nutzungs- und Lizenzbestimmungen vertrieben wird, zu deren wesentlicher Verpflichtung typischerweise die Weitergabe oder Offenlegung des Quellcodes der Software bei deren Verbreitung gehört.

[I: KGAS_3826]

Closed Source Software ist Software, die nicht unter Lizenzbestimmungen für Free and Open Source Software vertrieben wird und deren Quellcode nicht frei zugänglich ist.

[I: KGAS_3952]

Auftragnehmer Software ist Fremdsoftware, die für den Auftragnehmer entwickelt wurde oder durch diesen, aber nicht vollentgeltlich im Auftrag des Auftraggebers.

[I: KGAS_3953]

Gelieferte Software, ist die vom Auftragnehmer gelieferte Software (u.a. Auftragnehmer Software, Beistellsoftware, Software von Dritten).

[I: KGAS_4066]

Die Inhalte des Lieferumfangs sind im Rahmen einer Beauftragung festgelegt.

[I: KGAS_3954]

Software von Dritten ist Fremdsoftware, welche nicht Auftragnehmer-Software ist.

[I: KGAS_4067]

Whitebox-Test ist ein Testverfahren, das auf der inneren Struktur einer Komponente oder eines Systems basiert.

[I: KGAS_4068]

Blackbox-Test ist ein Testverfahren, das auf einer Analyse der Spezifikation einer Komponente oder eines Systems basiert, gemäß ISO/IEC/IEEE 29119 (KGAS_3479) .

[I: KGAS_3956]

Toter Code ist in der Auslieferung enthaltener Code, der durch den von der Spezifikation vorgegebenen Programmablauf (inkl. Fehlerhandling) nicht ausgeführt werden kann.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft

[I: KGAS_3962]

Toter Code ist gegeben, wenn der Code nicht ausgeführt wird, weil dieser
- nicht mehr benötigt wird,
- nicht aufgerufen wird,
- nicht aufgerufen werden kann.

[I: KGAS_3964]

Toter Code ist nicht gegeben, wenn
- eine Anforderung geplant, umgesetzt, aber durch den Auftraggeber nicht eingesetzt wird,
- der Code durch Parametrierung (z.B. Zieldatencontainer) nicht aufgerufen wird.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft

5 System- und Softwareentwicklung

[I: KGAS_3124]

Dieses Kapitel beinhaltet Anforderungen an die Organisation, die Entwicklungsprozesse, die Arbeitsprodukte und die Infrastruktur des Auftragnehmers.

5.1 Prozessübergreifende Anforderungen

[A: KGAS_2074]

Das gesamte im Lieferumfang enthaltene Produkt muss mit Prozessen entwickelt sein, die mindestens einen Reifegrad **„Level 2“** in einem Automotive SPICE® Assessment mit VDA Scope gemäß VDA Automotive SPICE® Guidelines (siehe KGAS_3813) erreichen.

[A: KGAS_4095]

Falls Cybersecurity relevante Anteile im Lieferumfang enthalten sind (siehe KGAS_3687), müssen diese mit Prozessen entwickelt sein, die mindestens einen Reifegrad „Level 2“ in einem Automotive SPICE for Cybersecurity® Assessment mit dem Assessmentscope gemäß VDA Automotive SPICE for Cybersecurity® Guidelines (KGAS_4096) erreichen.

[A: KGAS_3669]

Die Anforderung KGAS_2074 muss auch für bereits entwickelte Softwareanteile erfüllt werden. Dies beinhaltet z. B. Softwareanteile, die bereits vor Nominierung entwickelt oder eingekauft wurden.

[A: KGAS_2986]

Die von Automotive SPICE® geforderte bidirektionale Traceability muss von den Stakeholder-Anforderungen über die Unitebene bis zum Test erstellt werden.

[A: KGAS_3679]

Der Auftragnehmer muss bis zu 15 Jahre nach End of Production (EoP) in der Lage sein, alle vom Auftraggeber für erforderlich erachteten Fehlerkorrekturen in der Software umzusetzen. Der Auftragnehmer muss sicherstellen, dass die gelieferte Software vorgehalten wird und alle notwendigen Voraussetzungen zur Bearbeitung und Lieferung der Software unter Beachtung der Anforderungen der KGAS gegeben sind.

[A: KGAS_3407]

Jedes Element einer Spezifikation muss bis zu seiner Quelle rückverfolgbar sein.

[A: KGAS_3483]

Es muss eine Analyse durchgeführt und dokumentiert werden, welche zusätzlichen Arbeitsprodukte, neben den in Automotive SPICE® geforderten Work Products, Teil des Prozesses sind. Dies können z.B. die Folgenden sein:

- Strategiedokumente
- Alle Arbeitsprodukte des Development Interface Agreements (DIA) gemäß ISO 26262:2018 Road vehicles -- Functional safety (KGAS_3895).

[A: KGAS_2035]

Alle vom Prozess vorgeschriebenen Arbeitsprodukte müssen zum Zeitpunkt eines Releases an den Auftraggeber inhaltlich konsistent zueinander sein.

[A: KGAS_3552]

Die Verfeinerung von Spezifikationselementen (z.B. Anforderungen, Architekturelemente) von einer Abstraktionsebene bzw. Hierarchieebene auf die darunter liegende Abstraktionsebene darf ein Verhältnis von 1 zu 10 nicht überschreiten.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft

Wenn dieses Verhältnis in Einzelfällen überschritten werden muss, muss die Überschreitung nachweislich begründet werden.

[R: KGAS_3498]

Jede Veränderung der Entwicklungsprozesse und Entwicklungsstandorte des Auftragnehmers, die Einfluss auf die Einhaltung der KGAS hat, muss den in KGAS_2085 genannten Stellen unverzüglich mitgeteilt werden.

[A: KGAS_3794]

Systemanforderungen, die Funktionalitäten spezifizieren, die keinen nachweislichen Bezug zu den Anforderungen des Auftraggebers haben, müssen durch den Auftraggeber genehmigt werden.

[A: KGAS_3795]

Jede im Produkt enthaltene Softwareunit muss einen nachweislichen Beitrag zur Erfüllung mindestens einer Systemanforderung leisten.

[I: KGAS_3797]

Ziel der Anforderungen KGAS_3794 und KGAS_3795 ist die Vermeidung von unbestellten, potentiell schadhaften Softwareanteilen im Produkt (schadhaft bedeutet z. B.: gesetzeswidrig, sicherheitsverletzend, unethisch, umweltschädigend, Image-schädigend, Datenschutz-verletzend).

[R: KGAS_3968]

Um einen datenschutzkonformen Einsatz der einzelnen Steuergeräte im Feld gewährleisten zu können, sind die datenschutzrechtlichen Anforderungen bereits ab dem Entwicklungsbeginn zu berücksichtigen. Die "Richtlinie für die datenschutzrechtlichen Anforderungen bei der (Weiter-)Entwicklung von Steuergeräten mit Speicherfunktion" ist einzuhalten (KGAS_3966).

5.2 Projektmanagement

[A: KGAS_3169]

Eine Projektplanung und Abschätzung der Aufwände für das Gesamtprojekt müssen bis zum Start der Entwicklung vorliegen.

[A: KGAS_3595]

Für alle Schätzungen müssen die zugrundeliegenden Annahmen dokumentiert werden.

[A: KGAS_3163]

Ein Projektstrukturplan muss vor dem Start der Entwicklung eines Releases vollständig vorliegen.

[A: KGAS_3593]

Alle Arbeitspakete, die zur Entwicklung von Features beitragen, müssen mindestens die Aktivitäten Spezifikation, Implementierung sowie mindestens Verifikation, Validierung oder Review beinhalten.

[A: KGAS_3146]

Für alle Arbeitspakete müssen vorhandene Abhängigkeiten zu anderen Arbeitspaketen ersichtlich sein.

[A: KGAS_3148]

Für alle Arbeitspakete muss ersichtlich sein, welche Arbeitsprodukte damit erstellt oder geändert werden.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

[A: KGAS_3167]

Für Änderungs- und Problemlösungsumfänge müssen angemessene Pauschalaufwände eingeplant sein.

[A: KGAS_3594]

Wenn ein Feature über mehrere Releases umgesetzt wird, so muss dieses Feature in der Feature-Release-Planung weiter verfeinert werden, so dass pro Release ein exakt zu prüfender Umfang umgesetzt werden kann.

[A: KGAS_3157]

Die in der Feature-Release-Planung enthaltenen Features müssen den Anforderungen aus der System- und Softwareanforderungsspezifikation zugeordnet werden.

[A: KGAS_3158]

Die Schnittstellen und Verantwortlichkeiten im Projekt müssen dokumentiert sein (z. B. RACI-Matrix, VMI-Matrix).

[A: KGAS_3177]

Der Terminplan muss alle Aktivitäten beinhalten, die sich aus Einträgen des Problemlösungsmanagements und des Änderungsmanagements ergeben.

[A: KGAS_3178]

Es müssen eindeutige Definitionen für Erfüllungsgrade von Arbeitspaketen und Aktivitäten existieren und angewendet werden.

[A: KGAS_3191]

Projektrisiken müssen nachweislich identifiziert, bewertet und mit entgegenwirkenden Maßnahmen versehen werden.

5.3 Dokumentation des Lieferumfangs

[A: KGAS_4115]

Die Dokumentation erfolgt in den ReleaseNotes KGAS_4116, sofern zwischen Auftraggeber und Auftragnehmer nicht anders vereinbart.

[A: KGAS_3214]

Der Freigabelevel des Lieferumfangs (z.B. Entwicklungsstand ohne Straßennutzung, Entwicklungsstand mit Straßennutzung oder Serienfreigabe) muss dokumentiert sein.

[A: KGAS_3215]

Die umgesetzten Änderungen des Lieferumfangs müssen dokumentiert sein, inklusive Beschreibung etwaiger Fehlerbehebungen.

[I: KGAS_3938]

Zur Dokumentation zählen auch die Releasenotes und Feature-Übersichten aller Umfänge (z.B. Module) von Unterauftragnehmer.

[A: KGAS_3216]

Die für den Lieferumfang ausgeführten Tests und deren Testergebnisse müssen dokumentiert sein.

[A: KGAS_3218]

Der Konfigurationsstand des Lieferumfangs (Version der Software und ggf. Hardware, Mechanik usw.) muss dokumentiert sein (inkl. Version, Baseline, Stand der zugrundeliegenden Anforderungen, der gültigen Architektur, usw.).

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

[A: KGAS_3219]

Jede mit der Softwareversion des Lieferumfangs kompatible Hardwareversion muss dokumentiert sein.

[A: KGAS_3220]

Jede mit der Hardwareversion des Lieferumfangs kompatible Softwareversion muss dokumentiert sein.

[A: KGAS_3221]

Alle Einschränkungen des Lieferumfangs für Inbetriebnahme und Betrieb müssen dokumentiert sein.

[A: KGAS_3222]

Die bekannten Fehler des Systems bzw. der Software sowie deren Auswirkungen müssen dokumentiert sein (siehe auch KGAS_3430).

[A: KGAS_3223]

Die Version der zugrundeliegenden Software, auf der die Entwicklung der ausgelieferten Software erfolgte, muss dokumentiert sein.

[A: KGAS_3888]

Die Buildumgebung, Buildkonfiguration, Definitionen, Compileroptionen und -optimierungen müssen inkl. Änderungshistorie dokumentiert sein.

5.4 System- und Softwareanforderungsspezifikation

[A: KGAS_3406]

Alle getroffenen Annahmen müssen als Anforderungen spezifiziert und mit dem Auftraggeber abgestimmt werden.

[A: KGAS_3548]

Eigene Anforderungen des Auftragnehmers (z. B. Anforderungen zur Fertigung, Anforderungen aus Plattformanteilen, usw.) müssen in den System- und Softwareanforderungsspezifikationen dokumentiert sein.

[A: KGAS_3266]

Alle Anforderungen müssen nachweislich unter Berücksichtigung mindestens folgender Aspekte erstellt und analysiert werden:

- Machbarkeit
- Verifizierbarkeit
- Widerspruchsfreiheit
- Verständlichkeit
- Eindeutigkeit
- Atomarität

[A: KGAS_3535]

Alle Anforderungen müssen einem Release bzw. Feature zugeordnet sein.

[A: KGAS_3259]

Alle Anforderungen müssen zu ihrer Quelle rückverfolgbar sein.

[A: KGAS_3260]

Alle Anforderungen müssen in die daraus abgeleiteten Arbeitsprodukte verfolgbar sein.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

[A: KGAS_3256]

Für alle Anforderungen müssen die Verifikationskriterien inklusive einer textuellen Beschreibung dokumentiert sein.

[A: KGAS_3600]

Alle Anforderungen müssen bezüglich ihrer Auswirkungen auf die System- und Softwarearchitektur bewertet werden.

[A: KGAS_3558]

Alle Anforderungen müssen priorisiert und kategorisiert sein.

[A: KGAS_3257]

Mindestens folgende Kategorien bzw. Typen von Anforderungen sind zuzuordnen:

- Safetyrelevanz
- Gesetzesrelevanz
- Securityrelevanz

[A: KGAS_3263]

Für jede funktionale Anforderung müssen sowohl die positiven als auch die negativen Fälle spezifiziert sein, sofern dieser technisch existiert (z. B. Fehlerfall, Alternativpfad, Grenzfälle und Worst-Case Szenarien).

[A: KGAS_3262]

Anforderungen dürfen von einer höheren Anforderungsebene zu einer niedrigeren Anforderungsebene nicht zusammengefasst werden, wenn dadurch Informationsverlust entsteht.

[A: KGAS_3264]

Jede nichtfunktionale Anforderung muss in daraus abgeleiteten Anforderungen und Arbeitsprodukten nachweislich berücksichtigt werden.

[A: KGAS_3267]

Jede Spezifikation von System- und Softwareanforderungen sowie System- und Softwareelementen und Komponenten muss einem definierten Schema folgen (z. B. [Bedingung] [soll bzw. muss bzw. wird] [das System bzw. die Software bzw. die Komponenten] [Tätigkeit bzw. Vorgang bzw. Schnittstellenanforderung]).

5.5 System- und Softwarearchitekturspezifikation

[A: KGAS_3272]

Jedes Systemelement der Systemarchitekturspezifikation muss zu den zugehörigen Systemanforderungen rückverfolgbar sein.

[A: KGAS_3537]

Jedes Softwareelement der Softwarearchitekturspezifikation muss zu den zugehörigen Softwareanforderungen rückverfolgbar sein.

[A: KGAS_3275]

Für die Beschreibung der System- und Softwareelemente innerhalb der System- bzw. Softwarearchitekturspezifikationen müssen Syntax und Semantik definiert sein.

[A: KGAS_3278]

Jedes System- und Softwareelement muss eine textuelle Beschreibung mit mindestens Ziel/Zweck enthalten.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

[A: KGAS_3583]

Die Schnittstellen aller Systemelemente, Softwareelemente, Komponenten und Units müssen beschrieben sein.

[A: KGAS_3276]

Jede Schnittstelle muss statisch beschrieben sein, mindestens (sofern jeweilig anwendbar): Typ, Wertebereich, Format, Strukturbeschreibung, Datenbeschreibung physikalisch und logisch, Auflösung, Fehlerwerte, Offset, Initwerte, logische Abhängigkeiten.

[A: KGAS_3274]

Das dynamische Verhalten an jeder Schnittstelle muss beschrieben sein (z.B. Aufrufreihenfolgen, zeitliches Verhalten, Abhängigkeiten).

[A: KGAS_3279]

Gemeinsam genutzte Ressourcen (z. B. globale Variablen) sind als Schnittstellen anzusehen und müssen bezüglich schreibenden und/oder lesenden Zugriffen vollständig beschrieben sein.

[A: KGAS_3943]

Fehlererkennungsmechanismen (error detection) müssen innerhalb als auch außerhalb der Fahrzeuggrenzen (z.B. Backend, Cloud, App) auf allen Ebenen spezifiziert werden. Beispiel: Kommunikations-, Hardware- und Softwareebene.

[A: KGAS_3944]

Fehlerbehandlungsmechanismen (error handling) müssen innerhalb als auch außerhalb der Fahrzeuggrenzen (z.B. Backend, Cloud, App) auf allen Ebenen spezifiziert werden. Beispiel: Kommunikations-, Hardware- und Softwareebene.

[A: KGAS_3294]

Entwurfsentscheidungen in der System- und Softwarearchitekturspezifikation müssen textuell dokumentiert und den zugehörigen System- bzw. Softwareelementen zugeordnet werden können.

[A: KGAS_3281]

Verifikationskriterien für die System- und Softwarearchitektur müssen textuell beschrieben sein.

[A: KGAS_3282]

Für alle Softwareelemente müssen die Anforderungen für den entsprechenden Ressourcenbedarf spezifiziert sein. Diese müssen mindestens den maximalen CPU-Zeitverbrauch, den maximalen flüchtigen Speicherverbrauch, den maximalen nicht-flüchtigen Speicherverbrauch beinhalten.

[A: KGAS_3270]

Die Systemarchitekturspezifikation muss mindestens durch den System-Integrationstestenden geprüft werden.

[A: KGAS_3536]

Die Softwarearchitekturspezifikation muss mindestens durch den Software-Integrationstestenden geprüft werden.

5.6 Softwarefeinspezifikation (Detailed Design)

[A: KGAS_3285]

Die Softwarefeinspezifikation muss für jede Komponente sowie jede darin enthaltene Unit eine textuelle Beschreibung mit Ziel, Zweck und internem Aufbau enthalten.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

[A: KGAS_3288]

Wenn grafische Beschreibungen in der Softwarefeinspezifikation verwendet werden, müssen Syntax und Semantik dieser Beschreibungen definiert sein.

[A: KGAS_3289]

Alle zu implementierenden Units und Unitelemente müssen in der Softwarefeinspezifikation beschrieben sein.

[A: KGAS_4061]

Die Softwarefeinspezifikation muss den Lösungsansatz (KGAS_4062) für das nach außen wahrnehmbare Verhalten einer Unit beschreiben.

[I: KGAS_4062]

Der Lösungsansatz definiert Algorithmen, Berechnungen, Schnittstellen, Funktionsaufrufe und Makros und das Verhalten im Fehlerfall, soweit jeweils anwendbar.

[A: KGAS_4063]

Alle notwendigen Informationen zur Umsetzung eines Lösungsansatzes (KGAS_4062) sind zu beschreiben oder zu referenzieren.

[A: KGAS_3291]

Die Verifikationskriterien müssen textuell für jede Komponente und für jede Unit beschrieben sein.

[A: KGAS_3298]

Die Softwarefeinspezifikation muss die Schnittstellen der Units beschreiben (Parameter, globale und komponentenglobale Variablen, und aufgerufene Funktionen, Methoden, Prozeduren, usw.).

[A: KGAS_3299]

Die Softwarefeinspezifikation muss Abhängigkeiten der Units zu anderen Units inklusive Libraries enthalten.

[A: KGAS_3302]

Die Softwarefeinspezifikation muss die komponentenglobalen Variablen mit Initialwert, Wertebereich, Fehlerwerten und physikalischer Abbildung enthalten.

[A: KGAS_3455]

Die Softwarefeinspezifikation muss auch im Falle einer grafischen bzw. modellbasierten Programmierung erstellt werden.

[A: KGAS_3682]

Für alle Schnittstellen muss eine Gültigkeitsprüfung gegenüber der Schnittstellenbeschreibung (KGAS_3276) spezifiziert sein.

[A: KGAS_3683]

Bei negativen Gültigkeitsprüfungen von Schnittstellen muss ein definiertes System- bzw. Softwareverhalten spezifiziert sein.

5.7 Softwareerstellung

5.7.1 Programmiersprachen

[A: KGAS_2050]

Als Programmiersprache des Softwareprodukts muss eine international standardisierte (z. B. ISO/IEC) Hochsprache verwendet werden.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

[A: KGAS_2837]

Die Verwendung anderer Programmier- oder Scriptsprachen im Softwareprodukt ist nur nach Begründung, Eignungsnachweis und Genehmigung durch den Auftraggeber zulässig.

5.7.2 Manuelle Quellcodeerstellung

[R: KGAS_3948]

Dieses Kapitel gilt nur für Software (Lieferumfang), bei denen Methoden der handcodierten Programmierung zum Einsatz kommen.

[A: KGAS_3909]

Der Auftragnehmer muss eine Analyse und Bewertung existierender Codierrichtlinien in Hinblick auf Eignung für das Projekt durchführen. Diese Analyse muss mindestens die für das Projekt anwendbaren MISRA-Richtlinien beinhalten (Richtlinien unter KGAS_3908).

[A: KGAS_3910]

Der Auftragnehmer muss für die gesamte Quellcodeerstellung nachweislich für das Projekt geeignete Codierrichtlinien anwenden (siehe KGAS_3909).

[A: KGAS_3911]

Der Auftragnehmer muss sicherstellen, dass die Ergebnisse der Analyse und Bewertung (KGAS_3909) bei der Auswahl bzw. Definition der angewendeten Richtlinie(n) (KGAS_3910) berücksichtigt werden.

[A: KGAS_3878]

Alle Abweichungen von den angewandten Codierrichtlinien müssen begründet und dokumentiert werden.

[A: KGAS_3330]

Jede Unit innerhalb des Quellcodes muss der Softwarefeinspezifikation entsprechen.

[A: KGAS_3561]

Der Quellcode darf keine Inhalte ohne Bezug zur Softwarefeinspezifikation enthalten.

[A: KGAS_3322]

Für alle Units muss eine bidirektionale Traceability zwischen Unit (mindestens Header-Ebene) und Softwarefeinspezifikation erstellt werden.

[A: KGAS_3323]

Für Units mit einer hohen Komplexität bzw. Größe (z.B. mindestens in solchen Fällen mit zyklomatischer Komplexität >10), muss eine Traceability in einer höheren Granularität umgesetzt werden, d.h. mindestens Traceability zwischen Unitelementen und Softwarefeinspezifikation.

[A: KGAS_3324]

Jede Unit muss nachweislich durch ein Quellcodereview geprüft werden.

[I: KGAS_3562]

Mögliche Ziele von Quellcodereviews (KGAS_3324) können z.B. sein: Prüfung nicht funktionaler Anforderungen, Prüfung Einhaltung nicht automatisch prüfbarer Codierrichtlinien, Prüfung ob der Quellcode der Softwarefeinspezifikation entspricht.

[A: KGAS_3328]

Jede Unit muss mit mindestens einer Kurzbeschreibung der Unit, der Inputparameter und der Rückgabewerte kommentiert werden.

[A: KGAS_3329]

Alle Kommentierungen im Quellcode müssen konsistent mit der Softwarefeinspezifikation sein.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

[A: KGAS_3321]

Innerhalb des Quellcodes müssen definierte Namensregeln verwendet werden (z.B. für Funktionsnamen, Makros, Variablen, Typdefinition).

[A: KGAS_3325]

Der Quellcode muss an allen Entscheidungspunkten bezüglich der Bedeutung bzw. Logik kommentiert werden (z. B. bei if-else, for, switch, while).

[A: KGAS_3326]

Der Quellcode muss bei allen Berechnungen mit mindestens fünf Variablen oder Parametern bezüglich der Bedeutung bzw. Logik kommentiert werden.

[A: KGAS_3327]

Jede Variable muss hinsichtlich Inhaltes und Verwendung bei der Definition kommentiert werden.

5.7.2.1 Quellcodemetriken

[A: KGAS_4099]

Die Quellcodemetriken dienen zur Messbarkeit der Qualität des Quellcodes.
Die Metriken sind Indikatoren gemäß der Qualitätskriterien der ISO 25010 (KGAS_3043).

[R: KGAS_3587]

Die Quellcodemetriken gelten für die Programmiersprache "C". Für andere Programmiersprachen sind sie sinngemäß zu übertragen.

[A: KGAS_4100]

Bei manueller Quellcodeerstellung muss der Auftragnehmer geeignete Quellcodemetriken nach Stand der Technik mit definierten Grenzwerten anwenden.

[A: KGAS_3570]

Die Auswahl und Eignung der Quellcodemetriken (KGAS_4100) muss begründet sein (z.B. in einem entsprechenden Strategiedokument).

[A: KGAS_4065]

Grenzwertverletzungen sind nachvollziehbar zu dokumentieren.

[A: KGAS_4101]

Grenzwertverletzungen müssen auf der Ebene nachvollziehbar begründet werden, auf der diese erfasst werden.

[A: KGAS_4102]

Grenzwertverletzungen müssen bezüglich Risiken und Auswirkungen bewertet werden.

[A: KGAS_3571]

Basierend auf Risikobetrachtungen müssen angemessene Maßnahmen getroffen werden, um die Softwarequalität sicherzustellen.

[A: KGAS_4103]

Wenn der Auftragnehmer keine geeigneten Quellcodemetriken (siehe KGAS_4100) anwendet, gelten die Metriken gemäß KGAS_4104.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft

5.7.3 Grafische und modellbasierte Programmierung

[R: KGAS_3947]

Dieses Kapitel gilt nur für Software (Lieferumfang), bei denen Methoden der grafischen Programmierung und/oder modellbasierten Programmierung zum Einsatz kommen.

[A: KGAS_3861]

Der Auftragnehmer muss eine Analyse und Bewertung existierender Modellierungsrichtlinien in Hinblick auf Eignung für das Projekt durchführen. Diese Analyse muss mindestens die für das Projekt anwendbaren MISRA-Richtlinien und Richtlinien von Tool-Herstellern beinhalten (Richtlinien unter KGAS_3908).

[A: KGAS_3862]

Der Auftragnehmer muss für die gesamte Modellierung nachweislich für das Projekt geeignete Modellierungsrichtlinien anwenden.

[A: KGAS_3863]

Der Auftragnehmer muss sicherstellen, dass die Ergebnisse der Analyse und Bewertung (KGAS_3861) bei der Auswahl bzw. Definition der angewendeten Richtlinie(n) (KGAS_3862) berücksichtigt werden.

[A: KGAS_3886]

Alle Abweichungen von der/den angewandten Modellierungsrichtlinie(n) (KGAS_3862) müssen begründet und dokumentiert werden.

[I: KGAS_3889]

Die Hierarchieebene im Modell, aus der Code generiert wird, wird als Implementierung angesehen. Diese Implementierungsebene besteht i.d.R. aus Basisobjekten, die nicht weiter verfeinert werden können, und stellt das letzte menschlich erstellte Artefakt in der Softwareerstellungskette dar.

[A: KGAS_3312]

Jedes Modellelement muss der Softwarefeinspezifikation entsprechen.

[A: KGAS_3894]

Für alle Modellelemente muss eine bidirektionale Traceability zur Softwarefeinspezifikation erstellt werden.

[A: KGAS_3313]

Jedes Modellelement muss nachweislich durch ein Review geprüft werden.

[A: KGAS_3314]

Für jedes Modellelement muss eine Beschreibung existieren, die mindestens Ziel und Zweck enthält.

[A: KGAS_3456]

Im Modell müssen alle Entscheidungspunkte bezüglich der Bedeutung bzw. Logik kommentiert werden.

5.7.3.1 Metriken für Grafische Programmierung

[I: KGAS_4105]

Die Modellmetriken dienen zur Messbarkeit der Qualität der grafischen Programmierung.
Die Metriken sind Indikatoren gemäß der Qualitätskriterien der ISO 25010 (siehe KGAS_3043).

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft

[A: KGAS_3865]

Bei der grafischen Programmierung muss der Auftragnehmer geeignete Modellmetriken nach Stand der Technik mit definierten Grenzwerten anwenden.

[A: KGAS_3866]

Die Auswahl und Eignung der Modellmetriken (KGAS_3865) muss begründet sein (z.B. in einem entsprechenden Strategiedokument).

[A: KGAS_4064]

Grenzwertverletzungen sind nachvollziehbar zu dokumentieren.

[A: KGAS_3902]

Grenzwertverletzungen müssen auf der Ebene nachvollziehbar begründet werden, auf der diese erfasst werden.

[A: KGAS_4106]

Grenzwertverletzungen müssen bezüglich Risiken und Auswirkungen bewertet werden.

[A: KGAS_3867]

Basierend auf Risikobetrachtungen müssen Maßnahmen getroffen werden, um die Softwarequalität sicherzustellen.

5.7.4 Maschinelles Lernen (ML)

[R: KGAS_4009]

Dieses Kapitel gilt nur für Software (Lieferumfang), bei denen Maschinelles Lernen (ML), Neuronale Netze (NN) oder vergleichbare datenbasierte Komponenten zum Einsatz kommen. Dabei wird von offline trainierten Komponenten ausgegangen.

5.7.4.1 Terminologie

[I: KGAS_4069]

ML-Modell
Als ML-Modell wird eine Komponente, wie z.B. ein Neuronales Netz, bezeichnet, bei welcher Maschinelles Lernen oder vergleichbare datenbasierte Ansätze zum Einsatz kommen.

[I: KGAS_4022]

Trainingsdaten
Die Trainingsdaten sind Daten, welche zum Trainieren des ML-Modells (z.B. Neuronalen Netzes) verwendet werden.

[I: KGAS_4023]

Validierungsdaten
Die Validierungsdaten sind Daten, welche zur Überprüfung und Steuerung der Generalisierungsfähigkeit des ML-Modells (z.B. Neuronalen Netzes) in der Lernphase verwendet werden.

[I: KGAS_4024]

Testdaten
Die Testdaten sind Daten eines zusätzlichen Testdatensatzes, der in der Testphase zur Feststellung der Leistung und Generalisierungsfähigkeit des ML-Modells (z.B. Neuronalen Netzes) dient.

[I: KGAS_4025]

Online Training
Das Online Training entspricht Datenpunkt-basiertem Lernen, bei welchem Adaptionen noch im produktiven Einsatz durchgeführt werden (das Training sich somit also auch auf den Zeitraum des produktiven Einsatzes ausweitet).

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

[I: KGAS_4026]

Offline Training
Das Offline Training entspricht Datensatz-basiertem Lernen, bei welchem keine weiteren Adaptionen im produktiven Einsatz durchgeführt werden (das Training somit vor dem produktiven Einsatz abgeschlossen ist).

[I: KGAS_4028]

Lernen
Das Lernen bezeichnet jede Veränderung in einem System, die diesem erlaubt bei der nächsten Wiederholung desselben Vorgangs dieselbe Aufgabe oder eine Aufgabe derselben Art effizienter oder effektiver auszuführen.

[I: KGAS_4029]

Überwachtes Lernen
Überwachtes Lernen beschreibt Lernen, bei dem in einem Trainingsmodus das ML-Modell gezielt bestimmten Stimuli ausgesetzt wird und die Reaktion des ML-Modells in einem Soll/Ist-Vergleich zu entsprechenden Veränderungen führt.

[I: KGAS_4030]

Unüberwachtes Lernen
Unüberwachtes Lernen beschreibt Lernen, bei dem in einem Trainingsmodus das Model Zusammenhänge in nicht gelabelten Daten lernt.

[I: KGAS_4070]

Gelabelte Daten
Gelabelte Daten sind Daten mit annotierten Labels, wobei ein Label im Klassifikationsfall eine Zielklasse repräsentiert und im Regressionsfall einen Zielwert.

[I: KGAS_4071]

Baseline Modelle
Baseline Modelle bilden eine Referenz hinsichtlich der Performanz des ML-Modells. Sie können dabei neben dem Stand der Technik auch aus nicht ML-basierten Ansätzen entstehen. (Eine Baseline eines Klassifizierungsproblems zwischen A und B mit einer Verteilung von 90% A und 10% B wäre z.B. 90% Genauigkeit, da diese Genauigkeit auch erreicht wird, wenn immer A ausgegeben würde.)

[I: KGAS_4031]

Alle verwendeten Terminologien in Anlehnung an VDI/VDE Richtlinie 3550, Blatt 1.

5.7.4.2 Datenakquise

[A: KGAS_4010]

Es muss eine Datenakquisestrategie existieren, die Ziele und Vorgehen für die Generierung, Beschaffung, Filterung und Aufbereitung der Daten unter Berücksichtigung der Aspekte Vollständigkeit, Repräsentativität und Ausgewogenheit enthält.

[I: KGAS_4072]

Vollständigkeit beschreibt das Ziel, die Daten entsprechend aller daran gestellten Anforderungen zu generieren, zu beschaffen, zu filtern und aufzubereiten. Vollständigkeit schließt somit die Existenz von gestellten Anforderungen an die Daten mit ein.

[I: KGAS_4073]

Repräsentativität ist dann gegeben, wenn die generierten, beschafften, gefilterten und aufbereiteten Daten das spezifizierte Einsatzgebiet abbilden

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

[I: KGAS_4074]

Ausgewogenheit ist dann gegeben, wenn die generierten, beschafften, gefilterten und aufbereiteten Daten den Anforderungen entsprechend verteilt sind.

[A: KGAS_4075]

Die Datenakquisestrategie muss Ziele und ein Vorgehen für das Labeln der Daten enthalten, auch im Falle von unüberwachtem Lernen ist über die Notwendigkeit einzelner gelabelter Daten zu entscheiden und gegebenenfalls ein entsprechendes Vorgehen zu definieren.

[A: KGAS_4076]

Die Datenakquisestrategie muss Ziele und ein Vorgehen für die Aufteilung der Daten in Trainings-, Test- und Validierungsdaten enthalten.

[A: KGAS_4077]

Die Datenakquisestrategie muss Ziele und ein Vorgehen für die Archivierung der Daten (Trainings-, Test-, und Validierungsdaten) und Einbeziehung dieser in das Konfigurationsmanagement enthalten.

[A: KGAS_4078]

Die Datenakquisestrategie muss Ziele und ein Vorgehen für die Modifikation der Trainingsdaten und Validierungsdaten entsprechend der Trainingsstrategie enthalten.

[A: KGAS_4015]

Es muss eine Datenschutzstrategie definiert und angewendet werden. Die Datenschutzstrategie muss die DSGVO und vergleichbare gültige Normen und Gesetze erfüllen.

[A: KGAS_4011]

Es müssen Nachweise der korrekten Anwendung der Datenakquisestrategie dokumentiert und auf Verlangen dem Auftraggeber zur Verfügung gestellt werden z.B. in Form eines Review Protokolls.

5.7.4.3 Training und Testing

[A: KGAS_4012]

Es muss eine Trainingsstrategie existieren, die Eingangsbedingungen enthält.

[A: KGAS_4081]

Die Trainingsstrategie muss Trainingsendkriterien enthalten.

[A: KGAS_4082]

Die Trainingsstrategie muss Ziele und ein Vorgehen für die Auswahl der Architektur, inkl. der Evaluation gegenüber sogenannten „Baseline Modellen“ enthalten.

[A: KGAS_4083]

Die Trainingsstrategie muss Ziele und ein Vorgehen für Trainingsiterationen inkl. Validierung enthalten.

[A: KGAS_4084]

Die Trainingsstrategie muss Ziele und ein Vorgehen für die Modifikation der Hyperparameter enthalten.

[A: KGAS_4086]

Die Trainingsstrategie muss Ziele und ein Vorgehen für die Erstellung und Archivierung von Trainingsbaselines inklusive trainierter Gewichte, Sätzen von Hyperparametern, benutzter Metriken und KPIs enthalten.

[A: KGAS_4016]

Die Teststrategie muss auch die Tests auf Zielplattform und die Tests für die Überprüfung der Vorhalte von Hardware Ressourcen beinhalten (siehe auch KGAS_3556).

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

[A: KGAS_4013]

Es müssen Nachweise der korrekten Anwendung der Trainingsstrategie gemäß der Teststrategie dokumentiert und auf Verlangen dem Auftraggeber zur Verfügung gestellt werden z.B. in Form eines Review Protokolls.

[A: KGAS_4014]

Es muss die Möglichkeit geschaffen werden, den korrekten Betrieb der Komponente vor Kunde zu überwachen z.B. durch ein online Monitoring oder aussagekräftiges Logging.

5.7.5 Tool-Qualifizierung

[A: KGAS_3117]

Jedes softwarebasierte Tool in der Softwareerstellungs-Toolkette muss qualifiziert sein basierend auf den normativen Anforderungen der ISO 26262:2018 (KGAS_3895) sowie den Anforderungen der ISO/SAE 21434 (KGAS_4094).
Für nicht FUSI-relevante und nicht Security-relevante Lieferumfänge muss jedes durch das Tool generierte Arbeitsprodukt durch eine geeignete Verifikationsmethode (z. B. Review, Test, Validierungstool) geprüft werden, um sicherzustellen, dass dieses hinsichtlich des Ausgangsarbeitsprodukts und der Generierungsregeln korrekt erstellt wurde.

[A: KGAS_3481]

Herstellerinformationen (z. B. Handbücher, Richtlinien, Fehlerverzeichnis) jedes softwarebasierten Tools müssen im Projekt nachweislich berücksichtigt werden.

5.7.6 Nachprüfung der Anforderungen der Softwareerstellung

[A: KGAS_3585]

Der Auftragnehmer muss vor jeder Softwarelieferung an den Auftraggeber nachweislich die Einhaltung der projektrelevanten Codierrichtlinien, Quellcodemetriken, Modellierungsrichtlinien und Modellierungsmetriken überprüfen und dokumentieren.

[I: KGAS_3586]

Für die Erfüllung der Anforderung KGAS_3585 sollten Analyse-Werkzeuge zur Metrik- bzw. Defektanalyse nach Stand der Technik in den Software-Erstellungsprozess integriert werden.

[R: KGAS_51]

Der Auftragnehmer muss dem Auftraggeber die Möglichkeit einräumen, die Einhaltung der KGAS durch Quellcodeanalysen, werkzeuggestützte Analysen und andere geeignete Verfahren zu überprüfen.

[R: KGAS_4000]

Der Auftraggeber kann seine Analysen (KGAS_51), die sich aus der KGAS ergeben, vollständig oder teilweise durch Dritte wahrnehmen lassen.

[R: KGAS_2949]

Der Auftragnehmer muss die Analyse (KGAS_51) durch die Bereitstellung des Quellcodes in der entsprechenden Steuergerätekonfiguration in Räumen und in Anwesenheit des Auftragnehmers unterstützen.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft

5.8 Test

5.8.1 Testplanung

[A: KGAS_3556]

Ein Testplan inklusive Teststrategie gemäß ISO/IEC/IEEE 29119 (KGAS_3479) muss erstellt werden.

[A: KGAS_3334]

Der Testplan muss projektspezifische Testziele enthalten.

[A: KGAS_3335]

Der Testplan muss eine Beschreibung enthalten, wie die vollständige Testabdeckung der Spezifikationen (z. B. Pflichtenheft, Schnittstellenspezifikation, Softwareanforderungsspezifikation, Softwarearchitekturspezifikation, Softwarefeinspezifikation) erreicht wird.

[I: KGAS_3657]

Der Testplan (KGAS_3556) kann eine gemeinsame Teststrategie des Auftraggebers und Auftragnehmers beinhalten.

[A: KGAS_3336]

Der Testplan muss die Abgrenzung des Testumfangs der einzelnen Teststufen (z. B. System-, Systemintegrations-, Software-, Softwareintegrations- und Unittest) zueinander enthalten.

[A: KGAS_3338]

Der Testplan muss die Methoden zur Testfallerstellung, zur Auswahl der Testfälle, zur Erstellung der Testdaten und zur Testdurchführung beinhalten.

[A: KGAS_3339]

Die Black-Box-Testspezifikationen müssen anhand der Anforderungen bzw. anhand der Architektur und der Softwarefeinspezifikation erstellt sein.

[A: KGAS_3554]

Der Testplan muss mindestens die folgenden Softwarefehlerarten berücksichtigen: Division durch Null, Bereichsüberschreitungen, Wertebereichsverletzungen, Endlosschleifen, Typ-Fehler, Initialisierungsfehler, unberechtigte Zugriffe, unerreichbarer Quellcode.

[A: KGAS_3350]

Innerhalb des Testplans müssen die einzelnen Testumgebungen den Teststufen zugeordnet sein.

[I: KGAS_3351]

Die Testfälle sollten auf allen Teststufen so weit wie möglich automatisiert sein, damit so die Vergleichbarkeit der Testergebnisse erhöht und der Aufwand für die Testdurchführung reduziert werden kann.

5.8.2 Testfallspezifikation

[A: KGAS_3500]

Die Testfalldokumentation muss die Anforderungen der ISO/IEC/IEEE 29119 (KGAS_3479) erfüllen.

[A: KGAS_54]

Jede Testfallspezifikation muss von jemandem erstellt werden, der das Testobjekt weder umgesetzt noch spezifiziert hat.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft

[A: KGAS_3367]

Jede Testfallspezifikation muss eine textuelle Beschreibung in natürlicher Sprache beinhalten.

[A: KGAS_3355]

Jede Anforderung muss auf ihrer Ebene (z. B. System, Software) durch mindestens einen dedizierten Testfall verifiziert sein.

[A: KGAS_3357]

Das Ziel jedes Testfalls muss dokumentiert sein.

[A: KGAS_3358]

Das erwartete Ergebnis (Sollverhalten) muss für jeden Testfall dokumentiert sein.

[A: KGAS_3538]

Die Testschritte jedes Testfalls müssen dokumentiert sein.

[A: KGAS_3359]

Etwaige Grenzwerte müssen für jede(n) Anforderung, Schnittstelle, Parameter, Unit und Entscheidungspunkt getestet sein.

[A: KGAS_3362]

Die Vor- und die Nachbedingungen müssen für jeden Testfall dokumentiert sein.

[A: KGAS_3363]

Jeder Testfall muss eigenständig ausführbar sein. Abhängigkeiten von Testfällen untereinander sind nicht zulässig. Die Bildung von Testketten zur Erfüllung der Testvorbedingungen nachgelagerter Testfälle ist zulässig, sofern dadurch keine anderweitigen Einflüsse auf das Testergebnis entstehen.

[A: KGAS_3364]

Black-Box-Tests müssen vor White-Box-Tests spezifiziert werden.

[A: KGAS_3366]

Falls mehr als 10 Testfälle für die Verifikation einer Anforderung notwendig sind, muss die Qualität der Anforderung überprüft werden (z. B. daraufhin, ob diese atomar ist). Wenn die Anforderung nicht optimiert werden kann, muss eine geeignete Strukturierung der Testfälle verwendet werden.

5.8.3 Testdurchführung allgemein

[A: KGAS_3360]

Alle Anforderungen müssen vollständig gemäß Teststrategie getestet bzw. verifiziert sein (z.B. durch Äquivalenzklassenbildung, positiv/negativ Testfälle).

[A: KGAS_3361]

Bei Einsatz von Äquivalenzklassen zur Reduzierung der Testvektoren müssen mindestens der untere Wert, der obere Wert und ein zufälliger Wert aus dem Zwischenbereich verwendet werden.

[A: KGAS_3369]

Jedes Testergebnis muss dokumentiert sein (z. B. "ok"; "not ok").

[A: KGAS_3370]

Jedes Testergebnis muss einem eindeutigen Konfigurationsstand des Testobjekts (Version der Software und ggf. Hardware, Mechanik usw.) zugeordnet sein.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

[A: KGAS_3372]

Die Testumgebung muss dokumentiert sein (z.B. welche Testumgebung, an welchem Prüfstand, Software- und Hardwareversion).

[A: KGAS_3685]

Wenn für einen Lieferumfang Testfälle fehlgeschlagen sind, muss der Auftragnehmer die damit verbundenen Risiken analysieren und diese dem Auftraggeber mitteilen.

5.8.4 Unittest

[A: KGAS_3376]

Die Unittests müssen eine 100%ige Abdeckung der Softwarefeinspezifikation nachweisen.

[A: KGAS_3377]

Die Unittests müssen mindestens eine 100%ige Zweigabdeckung (C1 oder Branch Coverage) des Quellcodes nachweisen.

[A: KGAS_3378]

Abweichungen von der in KGAS_3377 geforderten 100%igen Zweigabdeckung müssen begründet sein.

[A: KGAS_3584]

Durch Black-Box-Tests nicht abgedeckter Quellcode (siehe auch KGAS_3378) muss durch White-Box-Tests verifiziert werden.

5.8.5 Softwareintegrationstest

[A: KGAS_3502]

Die Schnittstellen aller Softwareelemente und Komponenten müssen hinsichtlich statischer Struktur, Inhalt und Zeitverhalten getestet sein.

[A: KGAS_3519]

Der hierarchische Aufbau jedes Softwareelements muss verifiziert sein.

[A: KGAS_3383]

Softwareintegrationstests müssen gegen alle Anforderungen testen, die durch die Softwarearchitekturspezifikation erstellt werden. Dazu zählen unter anderem Datenschnittstellen (inkl. Strukturen, zeitlicher Verlauf), Funktionsaufrufe, Zugriffe auf globale Variablen, Aufrufreihenfolgen, Ressourcenauslastung, Performance, Scheduling von Tasks, Prozesse und Interrupt Service Routines (ISR).

[A: KGAS_3636]

Für alle Tasks, Prozesse und Interrupt Service Routines (ISR) müssen die maximalen und durchschnittlichen Nettolaufzeiten (siehe KGAS_3638) auf der Zielhardware für jedes Release ermittelt und dokumentiert sein.

[I: KGAS_3638]

Die Nettolaufzeiten sind die Laufzeiten abzüglich der Laufzeitveränderungen, die durch die Messungen verursacht werden.

[A: KGAS_3637]

Die maximalen und durchschnittlichen Ressourcenverbräuche (KGAS_3282) aller Softwareelemente müssen auf der Zielhardware für jedes Release ermittelt, dokumentiert und gegen die Ressourcenanforderungen (KGAS_3282) geprüft sein.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

5.8.6 Softwaretest

[A: KGAS_3503]

Die Softwaretests müssen eine 100%ige Anforderungsabdeckung der Softwareanforderungen nachweisen.

5.8.7 Systemintegrationstest

[A: KGAS_3619]

Die Schnittstellen jedes Systemelements müssen hinsichtlich statischer Struktur, Inhalt und Zeitverhalten getestet sein.

5.8.8 Systemtest

[A: KGAS_3506]

Die Systemtests müssen eine 100%ige Anforderungsabdeckung der Systemanforderungen nachweisen.

5.9 Qualitätssicherung und -management

5.9.1 Qualitätsmanagement

[A: KGAS_53]

Die Prozess- und Produktqualitätssicherung des Auftragnehmers muss von der Entwicklung des Produkts personell und hierarchisch unabhängig sein.

[A: KGAS_2904]

Die Ziele, Bewertungsmethoden, -aktivitäten und -kriterien der Qualitätssicherung des Auftragnehmers dürfen nicht durch die Projektleitung beeinflusst werden.

[A: KGAS_3129]

Die Ziele der Qualitätssicherung müssen messbar sein.

[A: KGAS_3130]

Ein Ziel der Qualitätssicherung muss sein, dass alle vom Prozess vorgeschriebenen Arbeitsprodukte rechtzeitig und entsprechend der Prozessbeschreibungen erstellt und qualitätsgesichert sind.

[A: KGAS_3133]

Ein Ziel der Qualitätssicherung muss sein, dass nur qualitätsgesicherte Produkte an den Auftraggeber ausgeliefert werden.

[A: KGAS_2911]

Die Qualitätssicherung des Auftragnehmers muss am Freigabeprozess der Software-Lieferung beteiligt sein (mindestens in Form einer Qualitätsaussage).

[A: KGAS_2913]

Mitarbeitende der Qualitätssicherung des Auftragnehmers müssen die fachlichen Qualifikationen besitzen, um die fachgerechte Durchführung (inhaltlich und formal) der Reviews bestätigen zu können.

[A: KGAS_3140]

Die Eskalationskriterien und die Eskalationswege der Qualitätssicherung müssen ab der untersten Stufe (Ebene Sachbearbeitende Qualitätssicherung) dokumentiert sein.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

5.9.2 Review der Arbeitsprodukte

[A: KGAS_3225]

Alle vom Prozess vorgeschriebenen Arbeitsprodukte müssen gemäß den Prozessvorgaben durch ein Review überprüft werden.

[A: KGAS_3508]

Die Prüfkriterien eines Reviews müssen mindestens die folgenden Punkte enthalten:

- Formale Anforderungen
- Inhaltliche Anforderungen
- Konsistenz
- Plausibilität (sowohl innerhalb des Arbeitsproduktes als auch zu dem Arbeitsprodukt, aus dem es abgeleitet wurde)
- Eindeutigkeit
- Widerspruchsfreiheit
- Wartbarkeit
- Verständlichkeit

[A: KGAS_3234]

Jede im Projekt verwendete Review-Methode (z. B. Walkthrough, Inspection) muss definiert und dokumentiert sein.

[A: KGAS_3134]

Für alle in KGAS_3225 identifizierten Arbeitsprodukte muss der aktuelle Reviewstatus dokumentiert sein und in einer entsprechenden Übersicht abrufbar sein.

[A: KGAS_3658]

Die in KGAS_3134 geforderten Statusinformationen müssen aktuell abrufbar sein, mindestens jedoch wochenaktuell.

[A: KGAS_2941]

Die Reviews müssen insoweit von der Qualitätssicherung begleitet werden, so dass eine fachgerechte Durchführung der Reviews bestätigt werden kann.

[A: KGAS_3135]

Jedes Review muss hinsichtlich Prüfgegenstand, Prüfmethode, Termin, Aufwand und Teilnehmer geplant werden.

[A: KGAS_3242]

Jedes Review muss dokumentiert sein und für jedes Review müssen mindestens die folgenden Aspekte ersichtlich sein:

- Datum
- Teilnehmer
- Rollen
- Prüfgegenstand (inkl. Identifikator und Version)
- Reviewumfang (z.B. Kapitel, Funktion, Deltaumfang)
- Prüfmethode (z.B. Inspection, Walkthrough)
- Prüfkriterien
- Kriterienerfüllung
- Aufwand
- Dauer
- Abweichungen (inkl. Art, Referenz, Schwere, verletzte Prüfkriterien, Maßnahmen, Verfolgung)

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

[A: KGAS_3227]

Für jedes Review muss das Ergebnis ersichtlich und die weitere Verwendbarkeit des Arbeitsproduktes ersichtlich sein.

[A: KGAS_3245]

Jedes zu prüfende Arbeitsprodukt muss nach der Erstellung oder nach einer Modifikation durch ein Review überprüft werden, spätestens bis zum Release des Auftraggebers.

5.9.3 Prüfung der Entwicklungsprozesse

[A: KGAS_3477]

Jeder Prozess muss regelmäßig, mindestens alle 2 Monate, durch die Qualitätssicherung des Auftragnehmers geprüft werden.

[A: KGAS_2922]

Der Auftragnehmer muss den Auftraggeber über alle für den Auftraggeber relevanten Projektrisiken informieren, die aus identifizierten Prozessdefiziten resultieren.

5.10 Konfigurationsmanagement

[I: KGAS_3510]

Konfigurationselemente sind einzelne Arbeitsprodukte, Binärdateien, Testumgebungen und Entwicklungswerkzeuge, die unter Konfigurationsmanagement gestellt werden müssen.

[A: KGAS_3482]

Für alle vom Prozess vorgeschriebenen Arbeitsprodukte muss der Konfigurationsstatus ersichtlich sein und eine mindestens wochenaktuelle Übersicht über alle Konfigurationsstatus muss vorhanden sein.

[A: KGAS_3389]

Zu jedem Projektmeilenstein, Qualitätsmeilenstein und Release müssen die Konfigurationselemente reproduzierbar und wiederherstellbar sein.

[A: KGAS_3390]

Zu jeder Baseline muss der Status jedes Konfigurationselements dokumentiert sein (z. B. "in Arbeit", "in Review", "Freigegeben").

5.11 Problemlösungsmanagement

[A: KGAS_3608]

Der Auftragnehmer muss dem Auftraggeber bei Auslieferung alle offenen, für den Auftraggeber relevanten Produktprobleme mitteilen.

[A: KGAS_3410]

Das Problemmanagementsystem des Auftragnehmers muss das Bewertungssystem des Auftraggebers bezüglich Produktproblemen hinreichend abbilden und dokumentieren können, so dass ein Informationsverlust durch unzureichende Schnittstellen ausgeschlossen werden kann.

[A: KGAS_3411]

Die Problembewertung aller Produktprobleme beim Auftragnehmer muss mit der Problembewertung des Auftraggebers konsistent sein.

[A: KGAS_3412]

Die in allen Testebenen gefundenen Produktprobleme müssen durch den Problemlösungsmanagementprozess bearbeitet werden.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

[A: KGAS_3415]

Alle Prozessabweichungen, die im Rahmen der Entwicklungs- oder unterstützenden Prozesse gefunden wurden, müssen durch den Problemlösungsmanagementprozess bearbeitet werden.

[A: KGAS_3417]

Die Problembeschreibung muss den Prozessschritt enthalten, in dem das Produktproblem oder die Arbeitsproduktabweichung gefunden wurde (z. B. Softwarefeinspezifikation-Review, Quellcode-Review, Unittest, Softwaretest, Systemtest).

[A: KGAS_3418]

Bei allen Produktproblemen müssen folgende Informationen ersichtlich/nachvollziehbar sein:

- Hardwareversion
- Softwareversion
- Ausgangssituation
- Fehlerschwere
- Durchgeführte Schritte
- Erwartete Ergebnisse
- Beobachtete Ergebnisse
- Bezüge zu verletzten Spezifikationen
- Informationen zur Reproduzierbarkeit des Problems
- Quelle des Problems

[A: KGAS_3421]

In allen Beschreibungen von Produktproblemen müssen für die Reproduzierbarkeit notwendige Logdateien, Traces und Messergebnisse verlinkt sein.

[I: KGAS_3609]

Die Quelle des Problems ist das erste, originäre fehlerhafte Arbeitsprodukt (z. B. Anforderung, Spezifikation, Quellcode, Testspezifikation).

[A: KGAS_3955]

Falls ein Fehler durch Prozessverletzung aufgetreten ist, müssen die Fehlerursachen analysiert und sichergestellt werden, dass die Prozessverletzungen nicht wieder auftreten.

[A: KGAS_3426]

Der Änderungsmanagementprozess der Problemlösung muss alle notwendigen Prozessschritte enthalten, die für die Korrektur einer Abweichung auszuführen sind (z. B. Überarbeitung und Review der Softwareanforderungsspezifikation, Überarbeitung und Review der Softwarefeinspezifikation, Überarbeitung und Review des Quellcodes, Überarbeitung und Review der Unittestspezifikation).

[A: KGAS_3430]

Falls ein Fehler Systemauswirkungen (Automotive SPICE® Sys-Ebene) hat, muss der Auftraggeber innerhalb von 2 Werktagen informiert werden.

[A: KGAS_3431]

Probleme im Prozess müssen systematisch ermittelt werden, um eine kontinuierliche Prozessverbesserung zu erzielen.

[I: KGAS_3432]

Beispiel zu KGAS_3431: Es ist als Abweichung identifiziert, dass eine Anforderung in der Softwarearchitektur keinem Softwareelement zugeordnet ist. Hierzu muss untersucht werden, ob dies ein Einzelfall ist oder ob ein systematischer Fehler vorliegt und andere Anforderungen ebenfalls nicht zugeordnet sind.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

[A: KGAS_3434]

Problembeschreibungen und Problemanalyse sind Arbeitsprodukte der Projektentwicklung und müssen daher unter Konfigurationsmanagement gestellt werden und stichprobenartig (in der Regel 1 von 5 Problemen) qualitätsgesichert sein.

5.12 Änderungsmanagement

[A: KGAS_3518]

Alle vom Prozess vorgeschriebenen Arbeitsprodukte müssen gemäß der Prozessvorgaben unter Änderungsmanagement gestellt werden.

5.13 Software von Dritten

[R: KGAS_3940]

Dieses Kapitel gilt für Systeme und Software (Lieferumfang), bei denen Software von Dritten zum Einsatz kommt.

[I: KGAS_3941]

Free and Open Source Software (siehe Kapitel 5.14) ist eine Variante von Software von Dritten.

[A: KGAS_3438]

Der Auftragnehmer ist verpflichtet, jede verwendete Software von Dritten in Softwareelementen einzukapseln.

[A: KGAS_3883]

Die Kapselung (KGAS_3438) ist so auszulegen, dass nur die durch Softwareanforderungen und Softwarearchitektur spezifizierten Funktionen und Schnittstellen der eingekapselten Software angesprochen werden können.

[A: KGAS_3442]

Vom Auftragnehmer entwickelte Systeme dürfen nur komplette Softwareelemente von Dritten verwenden. Eine teilweise Verwendung (z. B. über Copy & Paste Ansätze) ist nicht erlaubt.

[A: KGAS_3142]

Jedes verwendete Softwareelement von Dritten muss in der Softwarearchitekturspezifikation einzeln gekennzeichnet werden.

[A: KGAS_3531]

Für jedes verwendete Softwareelement von Dritten müssen Herkunft und Urheber bzw. Rechtsinhaber dokumentiert werden.

[A: KGAS_3437]

Für alle Softwareelemente von Dritten müssen die ursprünglichen Anforderungen, nach denen die Software von Dritten entwickelt wurde, den Softwareanforderungen zugeordnet werden.

[A: KGAS_3440]

Die Auswahl der verwendeten Softwareelemente von Dritten (inkl. Version und Patch Level) muss begründet und mit dem Auftraggeber abgestimmt werden.

[A: KGAS_3443]

Der Auftragnehmer muss sicherstellen, dass alle Softwareelemente von Dritten daraufhin geprüft werden, dass diese nur die spezifizierten Funktionen erbringen und keine anderen, möglicherweise unerwünschten Funktionen beinhalten.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

[R: KGAS_3446]

Bei der Verwendung von Softwareelementen von Dritten muss der Einsatz aller für die Softwareentwicklung notwendigen Testmethoden und Teststufen für die Gesamtsoftware weiterhin möglich sein.

[R: KGAS_3923]

Der Auftragnehmer trägt die alleinige Verantwortung dafür, dass die Nutzung der Gelieferten Software vertrags- und bestimmungsgemäß zulässig ist.

[I: KGAS_3924]

Der Auftraggeber ist verantwortlich für die technische Beschaffenheit der Beistellsoftware als solche.

5.14 Free and Open Source Software

[R: KGAS_3942]

Dieses Kapitel gilt für Systeme und Software (Lieferumfang), bei denen Free and Open Source Software zum Einsatz kommt (siehe KGAS_3820).

[A: KGAS_3822]

Die Verwendung von FOSS ist nur zulässig, wenn der Auftraggeber vor Verwendung der FOSS schriftlich entsprechend der von ihm vorgegebenen Prozesse vom Auftragnehmer informiert wird und dieser dabei bestätigt, dass die Verwendung der FOSS lizenzgerecht erfolgt. Der Auftragnehmer verpflichtet sich, die Prozesse des Auftraggebers zu bedienen und dabei insbesondere mögliche schriftliche Zustimmungserfordernisse zu beachten.

[I: KGAS_3821]

Eine Copyleft-Lizenz ist eine Form von Nutzungs- und Lizenzbestimmungen für Open Source Software, die dazu führen kann, dass mit der jeweiligen Open Source Software integrierte oder verbundene Softwareelemente ebenfalls nur unter den jeweiligen Nutzungs- und Lizenzbestimmungen dieser Copyleft-Lizenz verbreitet werden dürfen.

[I: KGAS_3840]

Ein Copyleft-Effekt bezeichnet die Verwendung von Free and Open Source Software, die unter einer Copyleft-Lizenz steht, und aufgrund dessen jede Bearbeitung ("jedes abgeleitete Werk") ebenfalls als unter einer Copyleft-Lizenz stehende Free and Open Source Software eingestuft werden muss (siehe auch KGAS_3821).

[A: KGAS_3833]

Der Auftragnehmer muss bestätigen, dass durch kein Softwareelement der Gelieferten Software ein Copyleft-Effekt ausgelöst wird, der dazu führt, dass das Softwareprodukt insgesamt als unter einer Copyleft-Lizenz stehende FOSS einzustufen ist.

[R: KGAS_3830]

Der Auftragnehmer darf in der Gelieferten Software nur solche FOSS einsetzen, die die vertrags- und bestimmungsgemäße Nutzung seiner Leistung durch den Auftraggeber und Unternehmen der Volkswagen Gruppe nicht beschränkt.

[A: KGAS_4097]

Der Auftragnehmer erteilt dem Auftraggeber mit Lieferung der Software das unterlizenzierbare und übertragbare Recht, in den Vertragsprodukten enthaltene proprietäre Software für den eigenen Gebrauch zu modifizieren und Reverse Engineering zum Zwecke der Fehlerbehebung (Debugging) solcher Bearbeitung vorzunehmen, soweit diese proprietäre Software mit unter der GNU Lesser General Public License v2.1 (LGPL-2.1) lizenzierten Software Komponenten verbunden ist.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

[A: KGAS_4098]

Der Auftragnehmer stellt sicher, dass er dem Auftraggeber dieses Recht (KGAS_4097) auch in Bezug auf etwaige Softwarebestandteile Dritter einräumen kann.

[I: KGAS_4005]

Die in der Allow-List (siehe KGAS_4003) enthaltenen FOSS-Lizenzen können vom Auftragnehmer in der Regel eingesetzt werden. Die Allow-List ersetzt jedoch keine geltenden Prozesse und befreit nicht von einer Prüfung durch den Auftraggeber.

[A: KGAS_3801]

Der Auftragnehmer muss dem Auftraggeber Informationen über alle in der Gelieferten Software verwendeten Free and Open Source Softwareelemente zur Verfügung stellen. Für jedes verwendete FOSS-Element müssen mindestens die folgenden Informationen enthalten sein:

- Name
- Eindeutige Versionskennzeichnung
- Lizenzname mit eindeutiger Lizenzversionsnummer
- Vollständiger Lizenztext
- Download-Link des Lizenztexts sowie des Quellcodes inklusive letztem Zugriffsdatum
- Quellcode und Urheberrechtsvermerke
- Information, ob Quellcode und Urheberrechtsvermerke weiterzugeben bzw. zu veröffentlichen sind
- Etwaige Subelemente, die zur Verwendung des Softwareelements erforderlich sind, inklusive der vorgenannten Angaben zur Lizenzierung
- Information, ob die Lizenz eine obligatorische Bereitstellung der Lizenzinformationen an den Endkunden vorschreibt
- Schnittstelleninformationen zur Integration von Open Source Softwareelementen unter Ausschluss der Auslösung von Copyleft-Effekten
- Etwaige Dateien, die in dem Softwareelement enthalten sind und unter abweichender Lizenz stehen, inklusive der vorgenannten Angaben zur Lizenzierung.

[A: KGAS_3834]

Der Auftragnehmer muss dem Auftraggeber die in KGAS_3801 geforderten Informationen mit jeder bereitgestellten Version der Software (Release, Update, Version etc.) sowie auf Anfrage des Auftraggebers zur Verfügung stellen, wobei jeweils sowohl eine vollständige Übersicht zur Verfügung gestellt werden muss als auch eine Delta-Übersicht, welche die Änderungen im Vergleich zum vorherigen Stand kenntlich macht.

[A: KGAS_3884]

Der Auftragnehmer muss sicherstellen, dass die Gelieferte Software keine Lizenzinkompatibilitäten beinhaltet.

[A: KGAS_3824]

Der Auftragnehmer muss die Gelieferte Software vor Auslieferung mit einer marktüblichen Analysesoftware dahingehend überprüfen, dass alle enthaltenen FOSS Elemente inklusive deren Abhängigkeiten und etwaiger Subelemente (u.a. Dateien) identifiziert wurden.

[A: KGAS_3828]

Auf Anfrage des Auftraggebers muss der Auftragnehmer dem Auftraggeber die Angaben, Materialien, Unterlagen und Ergebnisse der durchgeführten Analyse (KGAS_3824) zur Verfügung stellen.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft

[A: KGAS_3807]

Auf Anfrage des Auftraggebers muss der Auftragnehmer dem Auftraggeber die Möglichkeit einräumen, gemeinsam mit dem Auftragnehmer toolbasierte Analysen über den gesamten Quellcode in Räumen des Auftragnehmers durchzuführen.

[R: KGAS_3810]

Wenn der Auftragnehmer eine vom Auftraggeber patentierte oder zum Patent angemeldete technische Lösung umsetzt, dürfen keine Open Source Software Lösungen verwendet werden, deren Lizenzen die kostenpflichtige Lizenzierung des Patentes verhindern.

[R: KGAS_3827]

Der Auftragnehmer trägt die alleinige Verantwortung dafür, dass die Nutzung der Gelieferten Software vertrags- und bestimmungsgemäß zulässig ist. Der Auftraggeber nimmt seine Lizenzpflichten gegenüber den Endkunden wahr.

[A: KGAS_3925]

Soweit Beistellsoftware enthalten ist, wird der Auftraggeber für die Software-Komponente der Beistellsoftware die erforderlichen Lizenzinformationen und Urheberinformationen beibringen.

5.15 Cybersecurity-relevante Entwicklung

5.15.1 Allgemeine Cybersecurity-Anforderungen

[R: KGAS_3687]

Dieses Kapitel gilt für Systeme und Software (Lieferumfang), die von der Marken-Security-Abteilung des Auftraggebers als Cybersecurity-relevant eingestuft wurden.

[A: KGAS_4109]

Sollte zur Vergabe des Lieferumfangs noch keine Festlegung der Cybersecurity-Relevanz erfolgt sein, so muss dies durch den Auftragnehmer aktiv kommuniziert und angefordert werden. Bis zur finalen Festlegung der Cybersecurity-Relevanz muss der Auftragnehmer annehmen, dass der Lieferumfang Cybersecurity-relevant ist. (siehe KGAS_3790)

[A: KGAS_3738]

Der Auftragnehmer muss Cybersecurity-Risikoanalysen (Kap. 5.15.5) für den Lieferumfang auf System- und Softwareebene (auf Basis von Anforderungen und Architektur) durchführen und dokumentieren.

5.15.2 Cybersecurity-Terminologie

[I: KGAS_3703]

Risikoanalyse
Eine Risikoanalyse ist ein methodisches Vorgehen, welches Cybersecurity-Ziele identifiziert und mögliche Schäden sowie entsprechende Bedrohungen abschätzt.

[I: KGAS_3704]

Wert
Werte sind für eine Institution im Sinne der Cybersecurity schützenswerte Güter.

[I: KGAS_3705]

Schutzziel
Ein Schutzziel ist eine konkrete Eigenschaft eines Wertes, um den Schutz des Lieferumfangs zu gewährleisten.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

[I: KGAS_3706]

Bedrohung
Eine Bedrohung ist ein möglicher Umstand oder ein Ereignis, der oder das mindestens ein Schutzziel verletzen kann.

[I: KGAS_3868]

Backdoor
Eine Backdoor ist ein Zugang zu einer Software oder zu einem Hardwaresystem, die den spezifizierten Zugriff umgeht. Dabei kann der Zugang gewollt implementiert oder heimlich installiert sein.

[I: KGAS_3708]

Angriff
Ein Angriff ist eine unerwünschte oder unberechtigte Handlung, welche eine Bedrohung realisiert.

[I: KGAS_3709]

Angriffsvektor
Ein Angriffsvektor ist ein potenzieller Weg, einen Angriff durchzuführen.

[I: KGAS_3710]

Risiko
Ein Risiko ist eine bezüglich möglicher Schäden durch Verletzung von Schutzzielen sowie bezüglich des für eine erfolgreiche Umsetzung nötigen Angriffsaufwands bewertete Bedrohung oder die Zusammenfassung mehrerer bewerteter Bedrohungen.

[I: KGAS_3969]

Cybersecurity-Information
Alle Informationen, die im Rahmen des Monitoring-Prozesses erfasst werden und deren Cybersecurity Relevanz (potenzielle Schwachstelle) noch nicht eingestuft ist.

[I: KGAS_3970]

Cybersecurity-Event
Cybersecurity-Information, welche als potenzielle Schwachstellen (ohne Risikobewertung) für das Unternehmen oder seine Produkte als relevant eingestuft wird und eine weitere Behandlung (CSI-Prozess, Information Assessment, etc.) bedingt.

[I: KGAS_3971]

Cybersecurity-Schwachstelle
Fehler im Cybersecurity-Konzept (technisch, organisatorisch, prozessual) eines Wertes.

[I: KGAS_3707]

Cybersecurity ausnutzbare Schwachstelle
Die Schwachstelle eines Wertes, die durch eine oder mehrere Bedrohungen (Threat) ausgenutzt werden kann.

[I: KGAS_3927]

Cybersecurity-Vorfall
Einzelne oder eine Reihe unerwünschter oder unerwarteter Cybersecurity-Ereignisse, die die Ausnutzung einer ausnutzbaren Schwachstelle belegen und einen signifikanten Einfluss auf die Cybersecurity eines Bauteils/Funktion haben könnten (z. B. eine Schädigung des Wertes hervorrufen).

[I: KGAS_3811]

Reaktionsprozess
Ein Reaktionsprozess ist ein definierter Prozess, der das Ziel hat, Cybersecurity Informationen und Cybersecurity-Events zu bewerten und in Entwicklung und in Serie befindliche Produkte bei einer

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft

erkannten Schwachstelle schnellstmöglich anzupassen. Damit sollen die Risiken minimiert werden (evtl. mit funktionalen Einschränkungen) und die Schwachstellen unter Wiederherstellung der vollen Funktionalität beseitigt werden.

[I: KGAS_3711]

Cybersecurity-Anforderung
Cybersecurity-Anforderungen definieren Anforderungen an den Lieferumfang, die Eigenschaften zur Abwendung bzw. Reduktion von Bedrohungen spezifizieren.

[I: KGAS_3712]

Cybersecurity-Maßnahme
Eine Cybersecurity-Maßnahme beschreibt die (technische) Umsetzung von Cybersecurity-Anforderungen zur Reduzierung von Risiken und bildet eine logische Gruppierung für Cybersecurity-Anforderungen, die notwendig sind, um diese Cybersecurity-Maßnahme umzusetzen.

[I: KGAS_3713]

Cybersecurity-Konzept
Das Cybersecurity-Konzept ist ein Arbeitsergebnis zur Dokumentation der Cybersecurity-relevanten Aspekte des Lieferumfangs, die Bedrohungen entgegenwirken. Es umfasst insbesondere Cybersecurity-Maßnahmen, berücksichtigte Einschränkungen, Architekturen sowie die getroffenen Annahmen und Randbedingungen.

[I: KGAS_3715]

Schützenswerte Daten
Schützenswerte Daten sind Daten, die durch das Cybersecurity-Konzept bzw. durch Cybersecurity-Maßnahmen geschützt werden müssen.

[I: KGAS_3717]

Vertrauenswürdig
Als vertrauenswürdig kann ein System, eine Datenquelle, usw. eingestuft werden, wenn ein Nachweis existiert, dass sich auf dieses bis zu einem bestimmten Ausmaß verlassen werden kann und keine Kompromittierung vorliegt.

[I: KGAS_3718]

Vertrauensgrenze
Eine Vertrauensgrenze beschreibt den Übergang zwischen verschiedenen Ebenen des Vertrauens.

[I: KGAS_3720]

OWASP (Open Web Application Security Project)
OWASP ist eine Online Community, die unter anderem einen Standard zur Durchführung von Sicherheitsverifizierungen auf Applikationsebene zur Verfügung stellt.
Referenz: https://www.owasp.org/

[I: KGAS_3721]

CWE (Common Weakness Enumeration)
CWE ist eine Sammlung von Softwareschwachstellen, die durch eine Online Community zur Verfügung gestellt wird.
Referenz: https://cwe.mitre.org/

[I: KGAS_3904]

CVE (Common Vulnerabilities and Exposures)
CVE® ist eine Liste von Einträgen, die jeweils eine Identifikationsnummer, eine Beschreibung und mindestens eine öffentliche Referenz für bekannte Schwachstellen in Bezug auf Cybersecurity enthalten.
Referenz: https://cve.mitre.org/

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft

5.15.3 Cybersecurity-Management

[A: KGAS_3725]

Zur Strukturierung Cybersecurity-relevanter Projekte muss ein Cybersecurity-Plan erstellt werden.

[A: KGAS_3726]

Cybersecurity-Aktivitäten, Ressourcen und Arbeitsprodukte müssen geplant und dokumentiert werden (KGAS_3725).

[A: KGAS_3727]

Der Fortschritt und offene Punkte der Cybersecurity-Aktivitäten müssen mindestens alle zwei Wochen aktualisiert werden.

[A: KGAS_3728]

Der Auftragnehmer muss zur Entwicklung Cybersecurity-relevanter Systeme und Software die notwendigen Qualifikationen identifizieren und ausschließlich entsprechend geschultes Personal einsetzen.

[A: KGAS_3729]

Cybersecurity-Aspekte müssen im Projektrisikomanagement betrachtet und kenntlich gemacht werden.

[A: KGAS_3815]

Es muss ein Rechte- und Rollenkonzept für das Konfigurationsmanagement umgesetzt sein und alle zwei Wochen auf Aktualität überprüft werden.

[A: KGAS_3851]

Nach einem erkannten unautorisierten Zugriff auf das Konfigurationsmanagementsystem muss der ursprüngliche Zustand der Konfigurationselemente wiederhergestellt werden und der Auftraggeber ist darüber zu informieren.

[A: KGAS_3733]

Ein Verantwortlicher für Cybersecurity-Aktivitäten des Projektes muss benannt sein.

[A: KGAS_3735]

Der Cybersecurity-Verantwortliche (KGAS_3733) muss die Verfolgung und Einhaltung des Cybersecurity-Plans (KGAS_3725) sicherstellen.

5.15.4 Cybersecurity-Risikoanalysen und Cybersecurity-Konzept

[A: KGAS_3736]

Der Auftragnehmer muss die Cybersecurity-relevanten Stakeholder-Anforderungen auf Verständlichkeit und Korrektheit analysieren und Unstimmigkeiten zur Klärung bringen.

[A: KGAS_3853]

Cybersecurity-Anforderungen müssen als solche identifizierbar und kategorisiert sein.

[I: KGAS_3737]

Es empfiehlt sich, das Verständnis in einem kooperativen Prozess mit dem Auftraggeber zu klären und zu dokumentieren. Hierbei müssen durch entsprechende Analysen alle Inkonsistenzen und Unklarheiten zu allen, auch (bisher) nicht als Cybersecurity-relevant eingestuften, bestehenden Anforderungen aufgelöst werden.

[A: KGAS_3973]

Im Rahmen der Cybersecurity-Risikoanalysen sind alle zu schützenden Werte zu identifizieren.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft

[A: KGAS_3740]

Im Rahmen der Cybersecurity-Risikoanalysen sind alle verarbeiteten Daten zu identifizieren und nach den Cybersecurity-Schutzzielen zu klassifizieren.

[A: KGAS_3741]

Im Rahmen der Cybersecurity-Risikoanalysen sind alle Schnittstellen und Vertrauensgrenzen von und zu der beauftragten Software zu identifizieren und zu dokumentieren.

[A: KGAS_3742]

Für jede Schnittstelle sind Bedrohungen in den Security-Risikoanalysen systematisch zu identifizieren und zu dokumentieren.

[A: KGAS_3974]

Der Auftragnehmer muss aktuelle Bedrohungs- und Maßnahmenkataloge pflegen.

[A: KGAS_3743]

Für jede Bedrohung in einer Cybersecurity-Risikoanalyse ist das Risiko systematisch nach einem vom Auftragnehmer spezifizierten Bewertungsschema zu bewerten.

[A: KGAS_3744]

Der Auftragnehmer muss identifizierte und/oder vorgegebene Cybersecurity-Anforderungen in den Cybersecurity-Risikoanalysen berücksichtigen.

[A: KGAS_3749]

Für alle in den Cybersecurity-Risikoanalysen identifizierten und nicht akzeptierbaren Risiken muss eine Cybersecurity-Maßnahme definiert werden.

[A: KGAS_3750]

Cybersecurity-Maßnahmen müssen nachweislich zu Cybersecurity-Anforderungen führen.

[A: KGAS_3751]

Das Cybersecurity-Konzept des Auftragnehmers muss den Umgang mit den Risiken enthalten.

5.15.5 Cybersecurity-Risikomanagement

[A: KGAS_3745]

Nach Änderungen auf System- und/oder Softwareebene müssen die Cybersecurity-Risikoanalysen sowie das Cybersecurity-Konzept entsprechend aktualisiert werden.

[A: KGAS_3746]

Werden im Laufe der Entwicklung neue Angriffsvektoren gegen die verwendeten Technologien bekannt, müssen alle Cybersecurity-Risikoanalysen sowie das Cybersecurity-Konzept entsprechend aktualisiert werden.

[A: KGAS_3980]

Identifizierte Schwachstellen müssen bis zur akzeptablen Minimierung des Risikos nachweislich gemanagt werden.

[A: KGAS_3981]

Die Akzeptanz von Restrisiken muss begründet werden.

5.15.6 Cybersecurity-Architektur und Cybersecurity-Design

[A: KGAS_3753]

Systemarchitektur, Softwarearchitektur und Fein-Design müssen nachweislich alle Cybersecurity-Anforderungen abdecken.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

[A: KGAS_3755]

Alle Datenquellen müssen identifiziert und als vertrauenswürdig oder nicht vertrauenswürdig klassifiziert werden.

[I: KGAS_3855]

Datenquellen, die sich außerhalb der definierten Vertrauensgrenzen befinden, sind nicht vertrauenswürdig, und Datenquellen, die sich innerhalb der definierten Vertrauensgrenzen befinden, sind vertrauenswürdig. Der Lieferumfang muss nicht zwingend eine Vertrauensgrenze bilden. Der Lieferumfang kann auch mehrere Vertrauensgrenzen haben, z.B. bei mehreren µC.

[A: KGAS_3756]

Alle Daten, die aus nicht vertrauenswürdigen Quellen stammen, müssen vor der Verarbeitung validiert werden.

[A: KGAS_3758]

Nur spezifizierte Fehlermeldungen, Logeinträge und Diagnoseeinträge dürfen über die spezifizierten Schnittstellen ausgegeben werden.

[A: KGAS_3759]

Für alle Softwareelemente muss die verwendete Version und ggf. Patch Level dokumentiert sein.

[A: KGAS_3957]

Der Lieferumfang darf keine bekannten Schwachstellen enthalten. Abweichungen müssen in den Risikoanalysen berücksichtigt und begründet werden.

[A: KGAS_3929]

Für die Analyse seines Lieferumfangs muss der Auftragnehmer geeignete Quellen für die Identifikation von Schwachstellen bestimmen und gegen diese prüfen.

[I: KGAS_3930]

Quellen für die Identifikation von Schwachstellen können unter anderem Publikationen der CWE (KGAS_3721) oder der CVE (KGAS_3904) oder Meldungen des Auftraggebers sein.

[A: KGAS_3761]

Es muss sichergestellt sein, dass keine Backdoors vorhanden sind.

[A: KGAS_3896]

Es muss sichergestellt sein, dass kein unbenutzter Code (z.B. unzugänglicher oder toter Code) vorhanden ist.

5.15.7 Cybersecurity-Implementierung

[A: KGAS_3762]

Neben der Anwendung geeigneter Codierrichtlinien (KGAS_3909) oder Modellierungsrichtlinien (KGAS_3861) muss der Auftragnehmer Cybersecurity-Codierrichtlinien anwenden.

[A: KGAS_3772]

Der Auftragnehmer muss Codeanalysen durchführen, in denen die Einhaltung der KGAS_3762 geprüft wird.

[I: KGAS_3872]

Die Cybersecurity-Codeanalysen können sowohl manuell als auch toolgestützt durchgeführt werden.

[A: KGAS_3764]

Jede Abweichung von der Cybersecurity-Codierrichtlinie (KGAS_3762) muss begründet und dokumentiert werden.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

[A: KGAS_3765]

Umfasst der beauftragte Lieferumfang eine Web-Applikation, müssen die Richtlinien der OWASP (KGAS_3720) eingehalten werden.

5.15.8 Cybersecurity-Integration und Cybersecurity-Verifikation

[A: KGAS_3769]

Der Auftragnehmer muss seine Cybersecurity-Teststrategien parallel mit der System- und Softwarespezifikation erstellen und anwenden.

[A: KGAS_3770]

Die Cybersecurity-Tests müssen aus den Cybersecurity-Anforderungen abgeleitet werden und mit diesen verknüpft sein.

[A: KGAS_3771]

Für jedes Release muss ein Cybersecurity-Testbericht erstellt werden, der alle durchgeführten Cybersecurity-Tests mit Ergebnissen zusammenfasst.

5.15.9 Cybersecurity-Nachweis

[A: KGAS_3775]

Ein Cybersecurity-Nachweis muss vom Auftragnehmer zum Meilenstein "Function Complete" (100 % Software-Funktionalität ist implementiert) erbracht werden.

[A: KGAS_3931]

Der Cybersecurity-Nachweis muss spätestens zur 0-Serie, um den Nachweis des gegen unbefugte Zugriffe und Manipulation abgesicherten Flash Prozesses, ergänzt werden.

[A: KGAS_3818]

Der Cybersecurity-Nachweis muss bei Änderungen bis Serienlieferung stetig aktualisiert werden.

[A: KGAS_3776]

Der Cybersecurity-Nachweis muss die Ergebnisse der im Cybersecurity-Plan geplanten Cybersecurity-Aktivitäten (KGAS_3725) beinhalten.

[A: KGAS_3817]

Der Cybersecurity-Nachweis muss eine Zusammenfassung der Ergebnisse der Cybersecurity-Risikoanalysen beinhalten.

[A: KGAS_3983]

Der Cybersecurity-Nachweis muss die Angemessenheit und die Effektivität der Cybersecurity-Maßnahmen beinhalten.

[I: KGAS_3873]

Die Risikoanalysen sowie die detaillierten Ergebnisse der Risikoanalysen können im Rahmen einer Technischen Revision beim Auftragnehmer eingesehen werden.

[A: KGAS_3777]

Der Cybersecurity-Nachweis muss aufzeigen, dass die Cybersecurity-Anforderungen umgesetzt und verifiziert wurden.

[A: KGAS_3819]

Der Cybersecurity-Nachweis muss aufzeigen, dass die Cybersecurity-Codierrichtlinien (Codierrichtlinien siehe KGAS_3762) eingehalten wurden.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

[A: KGAS_3932]

Der Cybersecurity-Nachweis muss aufzeigen, dass der Reaktionsprozess zum Umgang mit identifizierten Schwachstellen (KGAS_3877) und die aktive Überwachung des Lieferumfangs (KGAS_3784) etabliert sind.

[A: KGAS_3984]

Der Cybersecurity-Nachweis muss durch eine vom Projekt unabhängige Instanz geprüft werden.

5.15.10 Cybersecurity-Aktivitäten nach der Entwicklungsphase (Serien-/Feldbetreuung)

[A: KGAS_3874]

Der Auftragnehmer muss eine zentrale Kontaktstelle für Cybersecurity Incident Management an das entsprechende Cybersecurity Incident Management des Volkswagen Konzerns (KGAS_3890) zu Beginn des Projektes kommunizieren.

[A: KGAS_3985]

Der Auftragnehmer muss zum Austausch vertraulicher Daten die von VW eingesetzten Mechanismen und Standards zur E-Mail-Verschlüsselung gem. IT-Sicherheitsrichtlinien unterstützen.
(siehe KGAS_4087 und KGAS_4088)

[A: KGAS_3877]

Der Auftragnehmer muss einen bidirektionalen Reaktionsprozess zum Umgang mit identifizierten Cybersecurity Schwachstellen, ausnutzbaren Schwachstellen und Vorfällen etablieren.

[A: KGAS_3784]

Der Auftragnehmer muss für den Lieferumfang einen Prozess zur aktiven und kontinuierlichen Überwachung auf mögliche Cybersecurity Information, Events, Schwachstellen, ausnutzbare Schwachstellen und Vorfällen etablieren, der die Punkte der (KGAS_3929) und (KGAS_3930) umfasst.

[A: KGAS_3785]

Beim Auftreten von Cybersecurity-Informationen, Events, Schwachstellen, ausnutzbare Schwachstellen und Vorfällen muss der etablierte Reaktionsprozess (KGAS_3877) durchlaufen werden.

[A: KGAS_3933]

Sollte der Auftragnehmer eine Unterauftragnehmerkette benötigen, um das Produkt für den Auftraggeber zu liefern, stellt der Auftragnehmer die Reaktionsfähigkeit und Effektivität auch in seiner Unterauftragnehmerkette sicher.

[A: KGAS_3934]

Cybersecurity-Schwachstellen, ausnutzbare Schwachstellen und Incidents müssen innerhalb eines angemessenen Zeitraums an das entsprechende Cybersecurity Incident Management des Volkswagen Konzerns (KGAS_3890) kommuniziert werden.

[A: KGAS_3986]

Wenn die Meldung (KGAS_3934) durch den Auftraggeber erfolgt, kann der Auftraggeber eine Frist festlegen.

[A: KGAS_3988]

Der Auftragnehmer muss innerhalb einer angemessenen Zeit eine Eingangsbestätigung versenden. Die Eingangsbestätigung muss eine eindeutige Referenz enthalten. Der Auftraggeber und der Auftragnehmer einigen sich auf eine eindeutige Referenz, die bei der Kommunikation herangezogen wird.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft

[A: KGAS_3939]

Jegliche Kommunikation des Auftragnehmers zu Cybersecurity-Schwachstellen, ausnutzbare Schwachstellen und Vorfällen hat auf Need-to-know-Basis zu erfolgen.

[A: KGAS_3936]

Die Kommunikation nach außen, die ausschließlich den Auftraggeber betrifft, ist mit dem entsprechenden Cybersecurity Incident Management des Volkswagen Konzerns (KGAS_3890) abzustimmen. Hiervon ist die Kommunikation aufgrund gesetzlicher Anforderungen ausgenommen. Über eine Kommunikation aufgrund gesetzlicher Anforderungen ist der Auftraggeber über das jeweilige Cybersecurity Incident Management in Kenntnis zu setzen.

[A: KGAS_3937]

Innerhalb von 10 Werktagen ist eine detaillierte technische Analyse inkl. Ursache, Auswirkungen und mögliche Abstellmaßnahmen an das entsprechenden Cybersecurity Incident Management des Volkswagen Konzerns (KGAS_3890) zu kommunizieren.

[A: KGAS_3989]

Die Risikobewertung (KGAS_3937) muss folgende Mindestinformationen enthalten:
- Beschreibung der Schwachstelle
- Beschreibung des Angriffsweges
- Beschreibung der Auswirkung
- Einschätzung der Eintrittswahrscheinlichkeit
- Resultierendes Risiko bezogen auf den Lieferumfang des Auftragnehmers

[A: KGAS_3990]

Bei einer durch den Auftragnehmer bereitgestellten Lösung ist auf Nachfrage eine ausführliche Dokumentation dieser bereitzustellen und enthält:
- Unterschied zu vorher und nachher der Veränderung des Produktes (Bspw. bei Soft- oder Hardware)
- Beschreibung der Tests/Szenarien zur Wirksamkeitskontrolle
- die Testergebnisse

[A: KGAS_3991]

Der Auftragnehmer muss auf Anfrage Hard- und/oder Software-Muster zur Verfügung stellen, die es der Volkswagen AG ermöglichen, die bereitgestellte Lösung sowie die Schwachstelle zu verifizieren.

[A: KGAS_3992]

Identifizierte Cybersecurity-Schwachstellen müssen in aktuellen Entwicklungen berücksichtigt werden (Siehe KGAS_3746).

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft

6 Referenzierte Unterlagen

6.1 Dokumente der Volkswagen AG

[I: KGAS_2834]

Formel Q Fähigkeit Software: Qualitätsfähigkeit Lieferanten Beurteilungsrichtlinie für Software-Entwicklungsprozesse [Volkswagen AG; Software-Qualitätssicherung]
Erhältlich unter http://www.vwgroupsupply.com/

[I: KGAS_3908]

Liste von Codier-/Modellierungsrichtlinien: Auflistung üblicher Codierrichtlinien und Modellierungsrichtlinien im Automotive Kontext [Volkswagen AG; Software-Qualitätssicherung]
Erhältlich unter http://www.vwgroupsupply.com/

[I: KGAS_4093]

Smart Quality Analytics (SQA): Das ist der Mindestsatz von Projektmetriken. [Volkswagen AG; Software-Qualitätssicherung]
Erhältlich unter http://www.vwgroupsupply.com/

[I: KGAS_4116]

ReleaseNotes: Dokumentation des Lieferumfangs und definierter Metriken.
[Volkswagen AG; Software-Qualitätssicherung]
Erhältlich unter http://www.vwgroupsupply.com/

[I: KGAS_3966]

Richtlinie für die datenschutzrechtlichen Anforderungen bei der (Weiter-)Entwicklung von Steuergeräten mit Speicherfunktion
Erhältlich unter http://www.vwgroupsupply.com/

[I: KGAS_4003]

Allow-List FOSS-Lizenzen KGAS: Diese Liste enthält FOSS-Lizenzen, die vom Auftragnehmer in der Regel bedenkenlos eingesetzt werden können.
Erhältlich unter http://www.vwgroupsupply.com/

[I: KGAS_4087]

Leitfaden - Sicherer Datenaustausch
Erhältlich unter http://www.vwgroupsupply.com/

[I: KGAS_4088]

Nr. 02.06. Handlungsleitlinien für Dienstleister
Erhältlich unter http://www.vwgroupsupply.com/
(für Beschäftigte der Volkswagen AG siehe KGAS_4089)

[I: KGAS_4089]

Nr. 02.02 Handlungsleitlinien für Beschäftigte v.5.0 (Gültig für Volkwagen AG)
Erhältlich unter https://volkswagen-net.de/wikis/display/Security/Informationssicherheitsregelwerk+-+Handlungsleitlinien

[I: KGAS_4104]

VW SW Source Code Metrics: Das ist der Satz der Quellcodemetriken. [Volkswagen AG; Software-Qualitätssicherung]
Erhältlich unter http://www.vwgroupsupply.com/

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft Ablageverantwortliche Abteilung: K-GQS | KSU-Klasse: 4.5 – 15 Jahre

6.2 Dokumente des Verbands der Automobilindustrie (VDA)

[I: KGAS_3813]

Aktuelle Version des Blau-Gold Bandes der VDA Automotive SPICE® Guidelines

[I: KGAS_3887]

Automotive SPICE® Process Assessment / Reference Model (PAM/PRM) - RELEASE v3.1 - 01. November 2017 oder höher

[I: KGAS_4096]

Aktuelle Version des Blau-Gold Bandes der VDA Automotive SPICE for Cybersecurity® Guidelines

6.3 Dokumente der MISRA

[I: KGAS_2091]

Die **M**otor **I**ndustry **S**oftware **R**eliability **A**ssociation ist ein Arbeitsgremium der (hauptsächlich britischen) Automobilindustrie. Ihre Webpräsenz und die Veröffentlichungen sind unter http://www.misra.org.uk zu erreichen.

6.4 Internationale Standards und Normen

[I: KGAS_3043]

ISO/IEC 25010:2011 Systems and software engineering -- Systems and software Quality Requirements and Evaluation ("SQuaRE")

[I: KGAS_3479]

ISO/IEC/IEEE 29119:2022 Software and systems engineering - Software testing

[I: KGAS_3895]

ISO 26262:2018 Road vehicles -- Functional safety

[I: KGAS_4094]

ISO/SAE 21434:2021 Road vehicles – Cybersecurity engineering

[I: KGAS_3790]

ISO/IEC 7498:1994 Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model

Relevant für Security-relevante Systeme gemäß KGAS_3687.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft

7 Release Notes

[I: KGAS_4055]

Die Tabelle mit den Änderungen zur vorherigen Version finden sie unter http://www.vwgroup-supply.com/.

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.

© Volkswagen Aktiengesellschaft

8 Vertraulichkeitshinweis

[R: KGAS_3488]

Öffentlich. Alle Rechte vorbehalten. Weitergabe oder Vervielfältigung ohne vorherige schriftliche Zustimmung des Fachbereiches der Volkswagen Aktiengesellschaft verboten.
Only applies to English translation: The English translation is believed to be accurate. In case of discrepancies the German version shall govern.
© Volkswagen Aktiengesellschaft