ISO 26262 – Quo vadis?

Stefan Kriso

Center of Competence „Functional Safety“
Robert Bosch GmbH
CoC-FS, CC/EVD
Robert-Bosch-Allee 1
74232 Abstatt
stefan.kriso@de.bosch.com

Abstract: Die ISO 26262 ist veröffentlicht und trägt damit einerseits zum Stand der Technik bei der Entwicklung sicherer elektrischer/elektronischer Systeme im Automobil bei. Andererseits sind einige Anforderungen der ISO 26262 visionär formuliert, so dass es nicht möglich ist, die Norm zu ihrem Veröffentlichungszeitpunkt umgesetzt zu haben, sondern es ist ein Einführungszeitraum notwendig. In dieser Zeit ist die Branche aufgefordert, praktikable und umsetzbare Interpretation der ISO 26262 zu finden, die der Intention der Norm möglichst nahe kommen sowie die Produktsicherheit nicht gefährden. Der Artikel nennt hierfür Beispiele und mögliche Lösungen.

1 Situationsbeschreibung

Die ISO 26262 wurde im November 2012 veröffentlicht und trägt damit zum Stand der Technik bei der Entwicklung sicherheitsrelevanter elektrischer/elektronischer Systeme in Straßenfahrzeugen bei. Ihre Umsetzung ist zur Reduktion unberechenbarer Produkthaftungsrisiken dringend angeraten [KS09] und sie steht deshalb derzeit im Fokus der Automobilbranche wie kaum eine andere Norm zuvor.

Neben dieser formaljuristischen Sicht auf die ISO 26262 gibt es allerdings noch die technisch-inhaltliche: Ein Teil ihrer Anforderungen wurde – teils bewusst, teils unbewusst – abstrakt und visionär formuliert. Dies bedingt, dass eine vollständige Umsetzung der ISO 26262 zu ihrem Veröffentlichungstermin nicht abgeschlossen sein kann, sondern dass ein Einführungszeitraum notwendig ist, während dessen die Anforderungen der Norm interpretiert und auf die tatsächlich vorhandenen Gegebenheiten in den jeweiligen Organisationen angepasst werden müssen [Re11].

Unterschiedliche Interpretationen verschiedener Beteiligter (OEM, Zulieferer, …) führen insbesondere an deren Schnittstellen zu Inkompatibilitäten, welche zu Reibungsverlusten führen, die der Produktsicherheit eher ab- als zuträglich sind. Es sollten daher gemeinsame Interpretationen der ISO 26262 gefunden werden, die einerseits der

Produktsicherheit dienen, andererseits aber Wettbewerbsdifferenzierung ermöglichen und Innovationsfähigkeit erhalten [KHK11, KH11].

Bis dahin gilt es, die abstrakten und visionären Anforderungen der ISO 26262 zu benennen und entsprechend ihrer Intention umzusetzen. Im Folgenden werden hierfür Beispiele genannt und Lösungsmöglichkeiten aufgezeigt.

2 ASIL-Einstufung

Die Vorgehensweise zur Ermittlung der ASIL-Einstufung einer Fehlfunktion eines E/E-Systems ist durch die ISO 26262 vorgegeben. Nach Bestimmung der Parameter für die Häufigkeit der Situation (Exposure „E"), der Beherrschbarkeit der Fehlfunktion (Controllability „C") und der Schwere der Auswirkung (Severity „S") ergibt sich der ASIL gemäß folgender Tabelle:

Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Abbildung 1: Tabelle zur Ermittlung des ASIL aus den Parametern S, E, C [ISO11].

Diese Vorgehensweise erscheint nur auf den ersten Blick objektiv. Die Ermittlung der Parameter E, C und S ist äußerst subjektiv, wie folgendes Beispiel zeigt: Versuchen zwei Personen die Häufigkeit der Situation „Bergabfahrt" zu ermitteln, von denen die eine aus dem norddeutschen Flachland kommt, die andere aber aus den Südtiroler Alpen, so werden sie möglicherweise auf Grund ihres persönlichen Erfahrungshintergrunds zu signifikant unterschiedlichen E-Einstufungen kommen. Wie aus Abbildung 1 ersichtlich ist, kann eine Varianz im Parameter E (wie auch bei den anderen beiden Parametern) direkt auf den ASIL durchschlagen: beispielsweise würde eine Variation in E von E1 bis E3 eine Variation im ASIL von A bis C bewirken (bei C3 und S3). Vor diesem Hintergrund ist es nicht verwunderlich, wenn dieselbe Fehlfunktion von unterschiedlichen Beteiligten mit unterschiedlichem ASIL eingestuft wird. Verstärkt

wird dies durch eine momentane Unsicherheit in der Ermittlung der E-, C- und S-Parameter, da die ISO 26262 sich hierzu im normativen Teil nicht äußert und sich daher nach und nach verschiedene Vorgehensweisen in der Branche herausbilden (z.B. rein qualitative Betrachtungen vs. Durchführung von Fahrversuchen). Diese unterschiedlichen Vorgehensweisen sind zwar im Allgemeinen jede für sich normkonform und sinnvoll, sie führen jedoch teilweise zu unterschiedlichen und nicht vergleichbaren Ergebnissen. Insgesamt ist dies nicht ohne Konsequenzen:

- Hat sich in der Branche bezüglich einer bestimmen Fehlfunktion eine ASIL-Einstufung weitgehend etabliert und es weicht ein einzelner Hersteller mit seiner ASIL-Einstufung von diesem impliziten Branchenkonsens nach unten ab (d.h. er stuft die Fehlfunktion geringer, möglicherweise gar als QM ein) und es kommt gerade bei diesem Hersteller zu einem Produkthaftungsfall, so wird er möglicherweise dem Vorwurf ausgesetzt sein, er hätte die geringere Einstufung aus Gründen der Kosteneinsparung vorgenommen. Weiter könnte ihm vorgeworfen werden, den Stand der Technik nicht berücksichtigt zu haben, denn hätte er sich an den Einstufungen der anderen Hersteller orientiert und sein Produkt dementsprechend entwickelt, so wäre der Unfall möglicherweise vermeidbar gewesen.

- Der umgekehrte Fall, dass ein Hersteller sein Produkt bzw. die entsprechende Fehlfunktion höher einstuft als der Rest der Branche, scheint zunächst unkritisch. Er betreibt in diesem Fall mehr Entwicklungsaufwand als es nach Branchenmeinung offensichtlich notwendig wäre, und das Produkt wird möglicherweise teurer, aber nicht unbedingt sicherer. Unter Umständen wird aber durch die höhere Einstufung ein neuer Stand der Technik geschaffen, den dann auch die anderen umsetzen müssen, um nicht die Verkehrsfähigkeit ihrer Produkte zu gefährden. Die Folge der Höhereinstufung eines Einzelnen könnte also in diesem Fall zu einem Pushen der ASIL-Einstufung in der gesamten Branche nach oben führen, ohne dass es notwendigerweise zu einem Sicherheitsgewinn kommt. Als weitere Folge könnte dies mittel- bis langfristig zu einem „Hochschaukeln“ der ASIL-Einstufungen führen, womit im Extremfall die Idee des ASILs ad absurdum geführt wäre; das Ziel und der Benefit der ASIL-Einstufungen, nämlich den Entwicklungsaufwand an Hand der Sicherheitsrelevanz des Produkts zu skalieren, wäre weniger stark bis gar nicht mehr gegeben.

- Insbesondere für einen Zulieferer ergibt sich die zusätzliche Schwierigkeit, dass er von seinen Kunden für dieselbe Fehlfunktion mit unterschiedlichen ASIL-Einstufungen konfrontiert wird. Möchte er mit einer Plattformentwicklung aber mehrere Kunden bedienen, stellt sich für ihn die Frage, nach welchem ASIL er diese entwickelt. Orientiert er sich am höchsten ASIL, steckt er möglicherweise für diejenigen Kunden, die einen geringeren ASIL fordern, mehr Aufwand in die Entwicklung als der Kunde bereit ist zu zahlen. Entwickelt er aber nach dem

geringeren ASIL[1], wird er diejenigen Kunden, die einen höheren ASIL fordern, ohne weitere Zusatzmaßnahmen nicht bedienen können.

Aus vorgenannten Gründen liegt es im Brancheninteresse, ein einheitliches Bild über die ASIL-Einstufungen verschiedener Fahrzeugfunktionen zu bekommen. Zumindest für die rudimentären Grundfunktionen sollten fahrzeugunabhängige ASIL-Einstufungen nach einer einheitlichen Methodik vorgenommen werden, um zum einen ein einheitliches „ASIL-Gefüge" zu bekommen, um zum anderen aber auch eine Methodik bereitzustellen, nach der neue Fahrzeugfunktionen klassifiziert werden können, die dann ebenfalls in dieses ASIL-Gefüge passen.

Selbstverständlich ist die letztendliche ASIL-Einstufung fahrzeugabhängig und kann (und wird) von einem Katalog harmonisierter ASIL-Einstufungen abweichen. Dennoch kann ein solcher in einem ersten Schritt als Orientierungshilfe zur Einstufung neuer Systeme dienen.

Die Anforderungen und Beispiele in der ISO 26262 orientieren sich im Wesentlichen an Personenkraftwagen bis 3500 kg zul. Gesamtmasse. Dementsprechend wurde auch der Scope der ISO 26262 formuliert: „*ISO 26262 is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production passenger cars with a maximum gross vehicle mass up to 3 500 kg*." [ISO11]. Es herrscht jedoch Branchenkonsens, dass die ISO 26262 grundsätzlich auch auf andere Fahrzeugklassen, z.B. LKW oder Motorräder, angewendet werden kann und soll[2]. Unsicherheit besteht lediglich noch bei einigen Anforderungen in der Art und Weise, wie diese bei den anderen Fahrzeugklassen umzusetzen sind, so z.B. auch bei der Methodik der ASIL-Einstufung: Geht man beispielsweise bei der ASIL-Einstufung implizit von mehrspurigen Fahrzeugen aus, so mögen bestimmte Fehlfunktionen relativ einfach beherrschbar sein oder eine geringe Auswirkungsschwere haben. Bei einem Motorrad dagegen kann dasselbe System unter Umständen eine deutlich höhere ASIL-Einstufung bekommen, weil beispielsweise die Beherrschbarkeit schlechter oder die Auswirkungsschwere höher ist. Es ist also darauf zu achten und es sollte auch dementsprechend in der Beschreibung der Methodik berücksichtigt werden, dass durch Erweiterung auf die übrigen Fahrzeugklassen einerseits keine Inkonsistenzen entstehen, andererseits die Spezifika der unterschiedlichen Fahrzeugklassen ausreichend und angemessen berücksichtigt werden. Vordringliche Aufgabe für die nächste Überarbeitung der ISO 26262 ist daher nicht nur die Berücksichtigung der übrigen Fahrzeugklassen im Scope der Norm, auch in den Anforderungen an sich müssen diese adäquat Berücksichtigung finden.

[1] Hier sei angenommen, dass eine geringere Einstufung des Kunden dadurch gerechtfertigt ist, weil er in seinem System, das außerhalb des Fokus des Zulieferers liegt, weitere Maßnahmen implementiert hat, die auf Gesamtsystemebene einen höheren ASIL ergeben (ASIL-Dekomposition). Andernfalls sollte der Zulieferer abwägen, ob eine Entwicklung nach dem höheren ASIL nicht doch gerechtfertigt ist.

[2] Siehe z.B. [BMW12]: „Erstmals bei einem Zweirad mit elektrischem Antrieb kommen hier die von den führenden Automobilherstellern erarbeiteten Standards für Hochvoltsicherheit (> 60 Volt Gleichspannung) und Funktionssicherheit zum Tragen. Die Entwicklung gemäß ISO 26262 ist bei (Elektro-) Zweirädern bisher einmalig und stellt sicher, dass sämtliche funktionsrelevanten Umfänge normgerecht und nach dem Stand von Wissenschaft und Technik entwickelt werden."

3 Qualifikation von Software-Werkzeugen

An vielen Stellen im Entwicklungsprozess elektrischer/elektronischer Systeme kommen Software-Werkzeuge zum Einsatz. Hiermit sind alle Werkzeuge gemeint, die in Software realisiert sind – nicht nur diejenigen, die in der Software-Entwicklung eingesetzt werden, sondern überall bei der Entwicklung elektrischer/elektronischer Systeme. Neben Werkzeugen für die Software-Entwicklung schließt dies zum Beispiel Anwendungen, die bei der Hardware-Entwicklung, der Steuergerätekalibrierung oder auf Systemebene, z. B. für das Anforderungsmanagement eingesetzt werden, mit ein. Das Ziel der Qualifikation von Software Tools ist es, durch Absicherung der Werkzeuge und deren geeignete Verwendung Fehler, die durch den Einsatz dieser Tools in das Produkt gelangen könnten, zu verhindern. Hierfür sieht die Norm folgende Fallunterscheidung vor: Einerseits kann, zum Beispiel durch entsprechende Maßnahmen in der Entwicklung, vermieden werden, dass das Werkzeug selbst Fehler erzeugt, andererseits können durch das Werkzeug erzeugte Fehler durch geeignete Absicherungsschritte (z.B. Verifikation, Test, Review) in einem nachgelagerten Prozessschritt oder durch organisatorische Maßnahmen identifiziert und behoben werden. Um mit der ISO 26262 konform zu sein, müssen alle Software-Werkzeuge, die bei der Entwicklung eines sicherheitsrelevanten elektronischen Produkts zum Einsatz kommen, im Kontext des spezifischen Entwicklungsprozesses dieses Produkts betrachtet werden. Eine generelle „ISO 26262-Konformität“ von Werkzeugen unabhängig vom jeweiligen Anwendungsfall ist gemäß der Norm nicht möglich – auch die häufig verwendete Qualifikation in so genannten „Referenzprozessen“ erfüllt dieses Ziel für den spezifischen Entwicklungsprozess eines Herstellers nicht; es muss immer ein Abgleich des Referenzprozesses mit dem tatsächlich vorhandenen spezifischen Entwicklungsprozess stattfinden. Jedoch kann aus Gründen der Wiederverwendung von Ergebnissen eine Vorabqualifikation von Werkzeugen für Standardanwendungsfälle sinnvoll sein, wenn sich deren Einsatz im Entwicklungsprozess aus einer Standardkonfiguration ableiten lässt. Sie kann beispielsweise die Zertifizierung eines Tools im Rahmen eines ISO 26262-konformen Prozesses bei richtiger Auslegung deutlich erleichtern.

Die ISO 26262 beschreibt in Teil 8 Kapitel 11 „Confidence in the use of software tools“ die Aktivitäten, die hier durchzuführen sind:

Bei der Qualifikation werden im ersten Schritt alle Anwendungsfälle, bei denen ein Werkzeug zum Einsatz kommt, klassifiziert. Zum Beispiel: Als nicht sicherheitsrelevant wird eingestuft, wenn ein Textverarbeitungsprogramm, das zur Dokumentation verwendet wird, beim Abspeichern die Schriftart verändert. Anders stellt sich der Fall dar, wenn beim Abspeichern relevante Informationen verfälscht werden. Im ersten Fall beeinflusst das Werkzeug den Inhalt des Ergebnisses nicht und es sind keine weiteren Qualifizierungsmaßnahmen notwendig. Im zweiten Fall muss geklärt werden, mit welcher Wahrscheinlichkeit in einem späteren Schritt im Entwicklungsprozess fehlerhafte Inhalte, die vom Werkzeug ausgegeben werden, zum Beispiel durch Reviews oder Tests entdeckt werden können.

Absicherungsmaßnahmen lassen sich durch ein weiteres Werkzeug oder einen überlagerten Prozessschritt (z. B. Plausibilisierung) vornehmen. Wenn Werkzeugfehler

durch geeignete Verifikationsschritte im Entwicklungsprozess nicht mit hoher Wahrscheinlichkeit ausgeschlossen werden können, sind Maßnahmen für die Werkzeugqualifizierung erforderlich. Das Ergebnis der Klassifizierung (siehe Abbildung 2) hängt wesentlich davon ab, in welchem Zusammenhang ein Software Tool im Entwicklungsprozess verwendet wird.

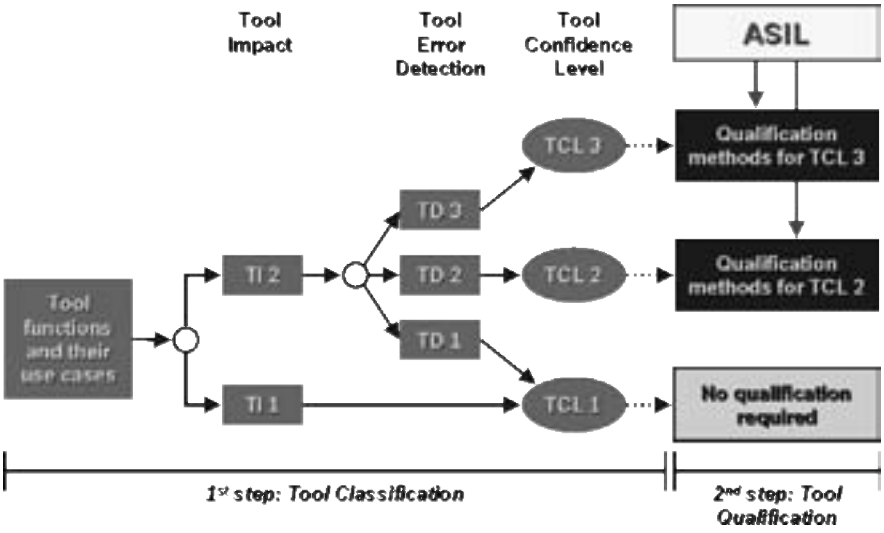

Abbildung 2: Ablauf bei der Qualifikation von Software-Werkzeugen nach ISO 26262.

Für die bei „TCL2“ oder „TCL3“ an die Klassifizierung anschließende Qualifizierung von Werkzeugen stehen nach ISO 26262 vier Methoden zur Auswahl („Increased confidence from use“, „Evaluation of the development process“, „Validation of the software tool“ und „Development in compliance with a safety standard“). Welche der alternativen Maßnahmen für eine Qualifizierung in Betracht kommen, wird durch die ASIL-Einstufung des zu entwickelnden Produkts und durch das Ergebnis der Werkzeugklassifizierung bestimmt. Abbildung 3 gibt eine Übersicht über die Qualifizierungsmethoden, die für Werkzeuge der Klasse „TCL 3“ für die verschiedenen ASIL empfohlen werden.

	Methods	ASIL			
		A	B	C	D
1a	Increased confidence from use in accordance with 11.4.7	++	++	+	+
1b	Evaluation of the tool development process in accordance with 11.4.8	++	++	+	+
1c	Validation of the software tool in accordance with 11.4.9	+	+	++	++
1d	Development in accordance with a safety standard*	+	+	++	++

* No safety standard is fully applicable to the development of software tools. Instead, a relevant subset of requirements of the safety standard can be selected.

EXAMPLE Development of the software tool in accordance with ISO 26262, IEC 61508 or RTCA DO-178.

Abbildung 3: Empfohlene Maßnahmen zur Qualifizierung von Software-Werkzeugen für TCL3 [ISO11].

Die Qualifikation von Software-Werkzeugen kann auf Grund der Menge der eingesetzten Werkzeuge sehr aufwändig werden. Bei Bosch sind z.B. in 56 Organisationseinheiten im Automobilbereich ca. 1500 Software-Werkzeuge im Einsatz. Bei einer systematischen Betrachtung wurden im ersten Schritt alle Werkzeuge klassifiziert. Hierbei zeigte sich, dass ca. 98% der Werkzeuge in TCL1 eingestuft werden können, da durch ihre Verwendung im Entwicklungsprozess bzw. durch ihre Einbettung in Werkzeugketten sichergestellt werden kann, dass fehlerhafte Ausgaben eines Werkzeugs in nachgelagerten Review-, Test- oder Plausibilisierungsschritten gefunden werden und sich somit nicht mehr sicherheitskritisch im Endprodukt manifestieren können. Nur für die restlichen 2% der Tools mit einer TCL2- oder TCL3-Einstufung musste ein aufwändigerer Qualifikationsschritt durchgeführt werden. Der im ersten Klassifikationsschritt entstandene Aufwand wurde also dadurch mehr als kompensiert, dass für den zweiten Schritt der Qualifikation in Summe deutlich reduzierte Aufwände entstanden sind.

4 Änderungen an bestehenden Systemen

Bezüglich Modifikationen erwähnt der Scope der ISO 26262: „*For further development or alterations based on systems and their components released for production prior to the publication date of ISO 26262, only the modifications will be developed in accordance with ISO 26262*.“ [ISO11]. In der Realität heißt das, dass bei einer Änderung lediglich die Änderung nach ISO 26262 durchgeführt wird. Insbesondere bei einer Änderung an einem schon bestehenden, vor Normveröffentlichung freigegebenen System führt dies nicht zwangsläufig zu einem „Reengineering“ des bestehenden, unveränderten Altsystems. Doch wie kann eine Änderung einerseits normkonform, andererseits aber auch effizient durchgeführt werden? Abbildung 4 zeigt in einem Ablaufdiagramm, wie bei einer Änderung an einem bestehenden System vorgegangen werden kann:

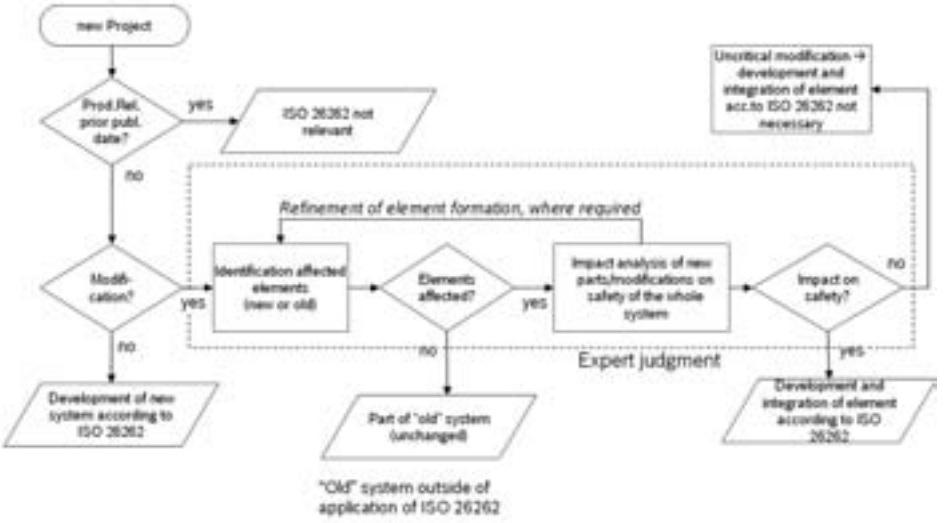

Abbildung 4: Ablauf bei einer Änderung an einem bestehenden Produkt.

Im ersten Schritt wird entschieden, ob die ISO 26262 überhaupt anzuwenden ist (Produktionsfreigabe nach Normveröffentlichung) und ob es sich um eine Änderung an einem bestehenden System handelt. In diesem Fall sind zunächst diejenigen Systemelemente zu identifizieren, die von der Änderung betroffen sind. Die nicht betroffenen Elemente sind Teil des unveränderten „Altsystems", welches nicht im Scope der ISO 26262 ist.

Für die von der Änderung betroffenen Systemelemente ist der Einfluss der Änderung auf das Gesamtsystem zu analysieren. Hierbei kann es sich durchaus ergeben, dass Systemelemente, die zunächst dem unveränderten „Altsystem" zugerechnet waren, sich doch als von der Änderung betroffen erweisen – somit sollte bei der Einflussanalyse von einer iterativen Vorgehensweise ausgegangen werden.

Kann durch eine Expertenbewertung gezeigt werden, dass die geplanten Änderungen definitiv keinen Einfluss auf die Sicherheit des Gesamtsystems haben, können diese Änderungen als unkritisch angesehen werden, und für die Entwicklung bzw. Integration der geänderten Anteile ist nicht unbedingt die formale Anwendung der ISO 26262 notwendig. Dies hätte für die Produktsicherheit keinerlei Mehrwert, d.h. keine Erhöhung der Systemsicherheit zur Folge.

Ein Beispiel für eine solche unkritische Änderung könnte eine Software-Parameteränderung sein. Bei neuen Parametern handelt es sich um eine Änderung, bei der rein formal die ISO 26262 angewendet werden müsste. Findet diese Parameteränderung in einer wohlbekannten Plattform statt und bewegen sich die Änderungen in bekannten Parametergrenzen anderer Plattformprojekte, so mag es möglich sein durch eine Expertenbewertung und durch Felderfahrungen bekannter Referenzprojekte zu zeigen, dass diese Parameteränderungen unkritisch sind und eine

formale Anwendung der ISO 26262 hier keinen Benefit bringt. Somit könnte in diesem Fall auf die formale Anwendung der ISO 26262 verzichtet werden.

5 Open Source Software und Tools

Bei Anwendung der ISO 26262 stellt sich die Frage, wie mit Open Source Software und Open Source Tools umgegangen werden muss und ob diese überhaupt bei der Entwicklung sicherheitsrelevanter Systeme eingesetzt werden dürfen. Die Anforderungen der ISO 26262 machen hier prinzipiell keine Ausnahme bezüglich Open Source bzw. stellen keine expliziten Anforderungen. Open Source Software ist daher prinzipiell genau so zu behandeln wie die übrige Software, für die Tools gilt dasselbe entsprechend:

- Open Source Codefragmente können verwendet werden, wenn deren Entwicklung gemäß ISO 26262-6 (Software development) abläuft.

- Open Source Softwarekomponenten können in einem nicht-sicherheitsrelevanten Software-Teil verwendet werden, wenn die „Freedom from interference“ (ISO 26262-6, Kap. 7, ISO 26262-9, Kap. 6) zum sicherheitsrelevanten Software-Teil gezeigt werden kann. Sie müssen qualifiziert werden (ISO 26262-8, Kap. 12), wenn der sicherheitsrelevante Software-Teil nicht weggekapselt werden kann. Voraussetzung ist, dass die Open Source Softwarekomponente gemäß eines „angemessenen“ nationalen/internationelen Standards (z.B. CMMI, Spice, …) entwickelt wurde.

- Open Source Tools können eingesetzt werden, wenn sie gemäß ISO 26262-8, Kap. 11 („Confidence in the use of software tools“) qualifiziert wurden (siehe oben).

Prinzipiell steht die ISO 26262 der Verwendung von Open Source Software nicht im Wege; die Anforderungen der ISO 26262 sind so formuliert, dass sie auch auf Open Source Software anwendbar sind. In wie weit diese in der Praxis insbesondere bei Open Source Codefragmenten und Softwarekomponenten umsetzbar sind, muss kritisch geprüft werden, insbesondere wenn die Konformität der Open Source Entwicklungsprozesse mit der ISO 26262 (bei Codefragmenten) bzw. mit „angemessenen“ nationalen/internationalen Standards nur schwer gezeigt werden kann.

Die größere Hürde bei der Verwendung von Open Source Software stellen lizenz- und urheberrechtliche Anforderungen dar, die es kritisch zu prüfen und umzusetzen gilt.

6 Unabhängigkeit bei Functional Safety Audits und Assessments

Die ISO 26262 fordert bei der Entwicklung sicherheitsrelevanter Systeme die Durchführung verschiedener Bestätigungsmaßnahmen, insbesondere – bei Systemen mit ASIL C- und ASIL D-Einstufung – von „Functional Safety Audits“ und „Functional Safety Assessments“. Das Functional Safety Audit betrachtet hierbei die Umsetzung der geforderten Prozesse, wobei das Functional Safety Assessment die erreichte Sicherheit des entwickelten Produkts beurteilen soll. Abhängig von der Sicherheitsrelevanz des zu entwickelnden Produkts (Automotive Safety Integrity Level = ASIL) ist das Functional Safety Audit und das Functional Safety Assessment von entsprechend unabhängigen Personen durchzuführen: Je höher das vom Produkt ausgehende Risiko, umso höher die geforderte Unabhängigkeit.

Confirmation measures	Degree of independency[a] applies to ASIL				Scope
	A	B	C	D	
Functional safety audit in accordance with 6.4.8 Independence with regard to the developers of the item and project management	—	I0	I2	I3	Applies to the highest ASIL among the safety goals of the item
Functional safety assessment in accordance with 6.4.9 Independence with regard to the developers of the item and project management	—	I0	I2	I3	Applies to the highest ASIL among the safety goals of the item

[a] The notations are defined as follows:
— —: no requirement and no recommendation for or against regarding this confirmation measure;
— I0: the confirmation measure should be performed; however, if the confirmation measure is performed, it shall be performed by a different person;
— I1: the confirmation measure shall be performed, by a different person;
— I2: the confirmation measure shall be performed, by a person from a different team, i.e. not reporting to the same direct superior;
— I3: the confirmation measure shall be performed, by a person from a different department or organization, i.e. independent from the department responsible for the considered work product(s) regarding management, resources and release authority.

[b] A software tool development is outside the item's safety lifecycle whereas the qualification of such a tool is an activity of the safety lifecycle.

Abbildung 5: Geforderte Unabhängigkeit bei Functional Safety Audits und Functional Safety Assessments. Auszug aus [ISO11].

Insbesondere beim Unabhängigkeitsgrad „I3“ (Person aus einer anderen Abteilung oder Organisation) stellt sich die Frage, wie dies umgesetzt werden kann. Diesen Unabhängigkeitsgrad generell mit „firmenextern“ gleichzusetzen, ist weder von der ISO 26262 gewollt, noch notwendig, noch in jedem Fall zielführend. Hier sei insbesondere das Functional Safety Assessment genannt: Zur Beurteilung der erreichten Produktsicherheit ist sowohl Unabhängigkeit als auch in besonderem Maße Produktwissen notwendig. Fehlende Unabhängigkeit bei der Bewertung kann dazu führen, dass das Assessment nicht hinreichend objektiv durchgeführt wird. Andererseits führt fehlendes Produktwissen beim Functional Safety Assessment zu einem nutzlosen Ergebnis, da es ohne detailliertes Verständnis der im Produkt implementierten Sicherheitsmechanismen nicht möglich ist, deren Angemessenheit und Wirksamkeit zu beurteilen. Generelles Grundproblem ist, dass je unabhängiger eine Person ist, umso weniger detailliertes Produktwissen vorhanden sein wird – und umgekehrt.

Als Lösung bietet sich hier an, als verantwortlichen Functional Safety Assessor jemanden auszuwählen, der die notwendige und geforderte Unabhängigkeit mitbringt und der gegebenenfalls durch ein Expertenteam unterstützt wird, das ihn mit dem notwendigen Produktwissen unterstützt. Hierbei kann insbesondere in großen Organisationen, zum Beispiel bei einem typischen OEM oder Tier1-Zulieferer die geforderte Unabhängigkeit durchaus konzernintern dargestellt werden, wie diverse Beispiele aus der Praxis zeigen [MR11, KU12]. Insbesondere sei in diesem Zusammenhang darauf hingewiesen, dass die ISO 26262 keinerlei Zertifizierung fordert, also weder von Prozessen, noch von Produkten, Personen oder Software-Werkzeugen. Generell ist ein Zertifikat immer dahingehend zu hinterfragen, ob es das leistet, was es zu versprechen scheint – beispielsweise ob und wie in einem zugelieferten Produkt diejenigen Sicherheitsanforderungen implementiert sind, die für die funktional sichere Integration in ein übergeordnetes System notwendig sind. Ein blindes Vertrauen auf ein Zertifikat ist hier wenig sinnvoll und darf die Sorgfaltspflicht des Entwicklers bzw. Integrators nicht ersetzen.

7 Zusammenfassung und Ausblick

Die ISO 26262 wurde im November 2011 veröffentlicht und trägt aus juristischer seither zum Stand der Technik bei der Entwicklung elektrischer/elektronischer Systeme im Automobil bei. Aus technisch-inhaltlicher Sicht ist es jedoch so, dass einige Anforderungen der ISO 26262 visionär (bis hin zu illusionär) formuliert sind. Somit ist eine Umsetzung der ISO 26262 zum Veröffentlichungszeitpunkt nicht möglich, es ist eine Einführungsphase notwendig. In dieser Zeit gilt es gemeinsame Brancheninterpretationen zu finden, die der Intention der ISO 26262 möglichst nahe kommen ohne die Produktsicherheit zu gefährden. Diese stattfindende Harmonisierung bei der Entwicklung sicherer E/E-Systeme trägt maßgeblich dazu bei, dass insbesondere im ausgeprägten Netzwerk der OEM-/Zuliefererverflechtungen ein gemeinsames Verständnis entsteht, wie die ISO 26262 zu interpretieren ist und effizient umgesetzt werden kann.

Um diese Harmonisierung weiter voranzutreiben, wurde bereits die Arbeit an der 2nd Edition der ISO 26262 begonnen, mit deren Veröffentlichung ca. 2016/2017 gerechnet werden kann. In dieser ist angedacht, die übrigen Fahrzeugklassen (LKW, Busse, Motorräder) zu berücksichtigen, um auch hier ein einheitliches Branchenverständnis zu erreichen.

Eine neue Herausforderung in diesem Umfeld ergibt sich durch die stark wachsende Vernetzung von Fahrzeugen – sowohl innerhalb des Fahrzeugs selbst auch des Fahrzeugs mit seiner Umgebung (Car-2-X Kommunikation). Dies bietet vermehrt Angriffspunkte für Angriffe von außen auf das System, die – gewollt oder als Seiteneffekt – die Safety des Fahrzeugs kompromittieren können. Hier ist in Zukunft eine verstärkte Zusammenarbeit der Domänen Safety und Security notwendig [Kl12].

Literaturverzeichnis

[BMW12] BMW Gruppe: Der neue BMW C evolution. Pressemitteilung vom 27.07.2012.

[ISO11] International Organization for Standardization: ISO 26262:2011(E) – Road vehicles – Functional safety. Geneva, 2011.

[KHK11] Klauda M.; Hamann R.; Kriso S.: ISO 26262 – Was kommt da auf uns zu? In: VDI-Berichte 2132, 2011, S. 285-297.

[KH11] Kriso S.; Hamann R.: Die ISO 26262 ist veröffentlicht - Konsequenzen für OEMs und Zulieferer. In: VDI-Berichte 2132, 2011, S. 299-308.

[Kl12] Klauda, M. et al.: Automotive Safety und Security aus Sicht eines Zulieferers. In: Automotive 2012, Karlsruhe, 11/2012.

[KS09] Kriso, S.; Sauler, J.: Die Norm zur funktionalen Sicherheit ISO 26262. In: Elektronik-Praxis Sonderheft Embedded Software Engineering. Vogel-Verlag, Würzburg, 2009; S. 32-36.

[KU12] Kriso, S.; Unruh, J.: Implementation of Functional Safety Audits and Assessments at Bosch. In: IQPC-Konferenz „Experiences with ISO 26262“, München, 03/2012

[MR11] Molle, E.; Rau, M.: Bestätigungsmaßnahmen der ISO 26262 und organisatorische Umsetzungsbeispiele. In: Safetronic 2011, München, 11/2011

[Re11] Reuter, A.: Rechtliche Aspekte bei der Umsetzung der ISO 26262. Euroforum-Konferenz ISO 26262, Stuttgart, 2011.