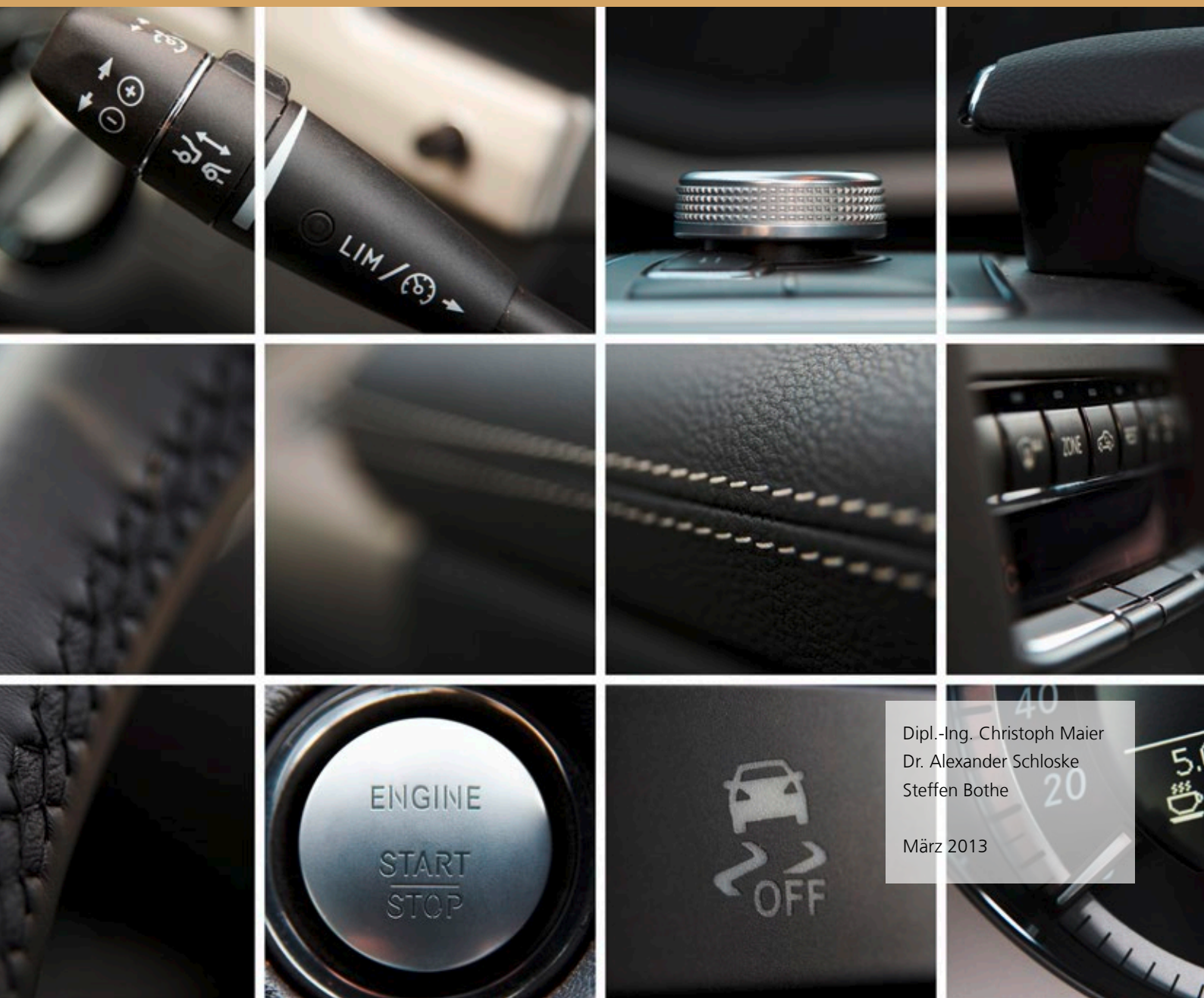
Fraunhofer
IPA

FRAUNHOFER-INSTITUT FÜR PRODUKTIONSTECHNIK UND AUTOMATISIERUNG IPA

STUDIE ZUR FUNKTIONALEN SICHERHEIT IN DER AUTOMOBILBRANCHE (ISO 26262)



Dipl.-Ing. Christoph Maier
Dr. Alexander Schloske
Steffen Bothe

März 2013

INHALT

1. EINLEITUNG

Aufgrund der immer größeren Anzahl von elektronischen Systemen in Automobilen, steigt stetig die Bedeutung der „Funktionalen Sicherheit“ (kurz FuSi) [Reif, K. 2011]. Bei der FuSi steht die korrekte Funktion mechatronischer Systeme im Vordergrund, bei denen gefahrbringende Situationen durch systematische und zufällige Abweichungen von elektronischen Komponenten ausgeschlossen bzw. auf ein unvermeidbares Maß reduziert werden müssen [ISO 26262:2011]. Nicht zuletzt durch die Erscheinung der Norm ISO 26262 im November 2011 hat das Thema an Bedeutung zugenommen. Der Funktionalen Sicherheit muss nun während der Entwicklungsphase gesteigerte Aufmerksamkeit geschenkt werden, um später kostspielige Rückrufaktionen zu vermeiden [Baumann,U. 2007], [Baumann, U. 2011], [Bücheler, R. 2008], [Schachtner, M. 2011], [Stockburger, C. 2011].

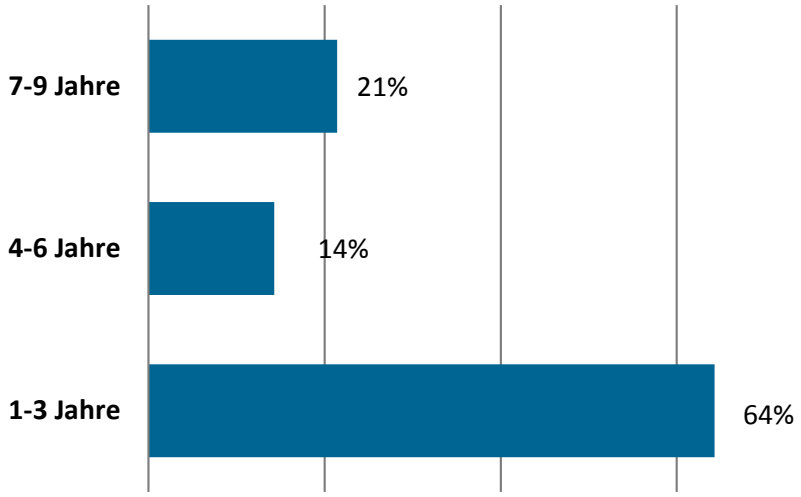
Den meisten Herstellern ist die Gefahr einer unzureichenden Integration der Funktionalen Sicherheit durchaus bewusst [Kowaleski, S. 2008]. Dennoch treten bei der Betrachtung der Funktionalen Sicherheit immer wieder Probleme auf, die die Entwicklung behindern bzw. erschweren und somit die Sicherheit der Kunden gefährden [Löw, P. 2010].

Deshalb befragte das Fraunhofer-Institut für Produktionstechnik und Automatisierung IPA in Stuttgart im März 2013 innerhalb einer Marktstudie 15 Unternehmen, sowohl OEMs als auch Zulieferer, um deren größten Probleme bei der Entwicklung von funktional sicheren Produkten zu erfassen und auszuwerten.

2. AUSGANGSLAGE

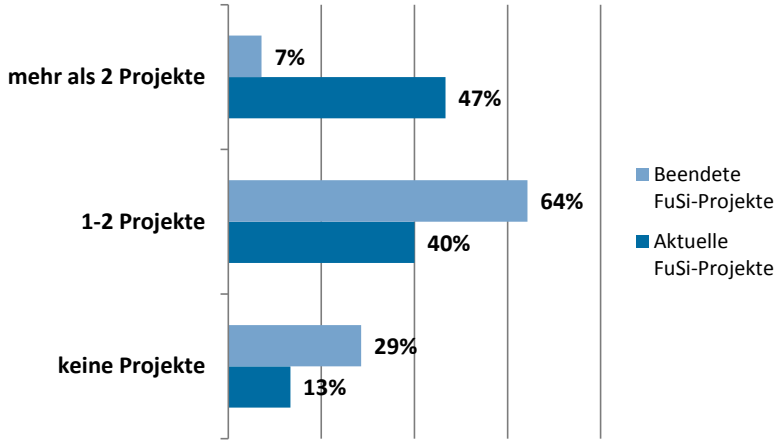
Zunächst einmal ist erkennbar, dass der Beginn der systematischen Betrachtung der Funktionalen Sicherheit stark zwischen den Unternehmen variiert, wie in Abbildung 1 dargestellt ist. Der Großteil (64%) der befragten Unternehmen teilte mit, sich erst seit maximal drei Jahren mit Funktionaler Sicherheit zu befassen. Nur ca. 20% der Unternehmen gab nach eigener Aussage an, bereits seit mehr als sieben Jahren funktional sichere Produkte zu entwickeln. Ein möglicher Grund ist, dass die maßgebliche Norm ISO 26262 („Road vehicles – Functional safety“) erst 2011 veröffentlicht wurde und seitdem gesetzlich verbindlich ist.

Abbildung 1: Erfahrungszeitraum mit Projekten im Kontext der Funktionalen Sicherheit in Jahren



Bei der Befragung nach bereits abgeschlossenen FuSi-Projekten gab der Großteil der befragten Unternehmen an, bis zum Zeitpunkt der Studie (März 2013) entweder noch keine (29%) oder maximal zwei (64%) FuSi-Projekte beendet zu haben (siehe Abbildung 2). Aufgrund des teilweise kurzen Erfahrungszeitraums (siehe Abbildung 1) teilten nur 7% der Unternehmen mit, dass sie schon mehr als zwei Projekte abgeschlossen haben.

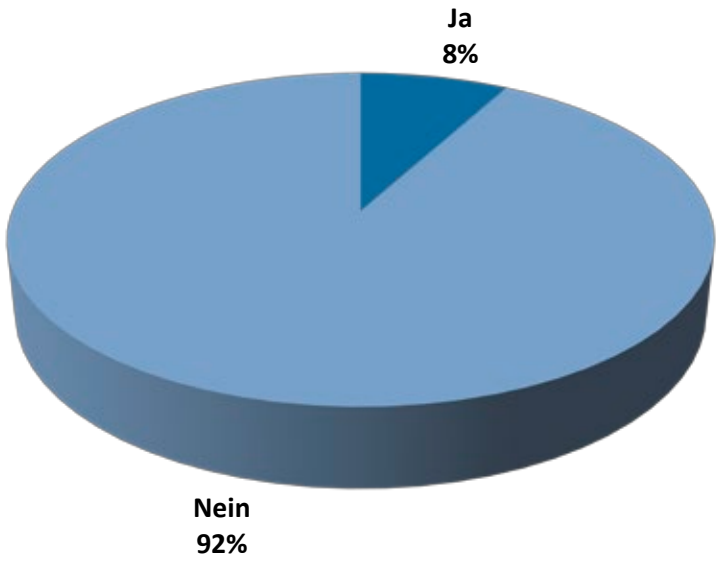
Abbildung 2: Vergleich aktuell entwickelte und bereits beendete Projekte im Kontext der Funktionalen Sicherheit



Die geänderten gesetzlichen Vorschriften und die steigenden Erfahrungen durch die Arbeit mit funktional sichereren Produkten führen zu einem gesteigerten Projektaufkommen in diesem Bereich. Nur noch 13% der befragten Unternehmen antworteten, dass sie im Moment kein Projekt im Kontext der Funktionalen Sicherheit bearbeiten. Fast die Häfte (47%) der befragten Unternehmen gaben an, dass sich aktuell mehr als vier FuSi-Projekte in der Entwicklung befinden, wie in Abbildung 2 dargestellt.

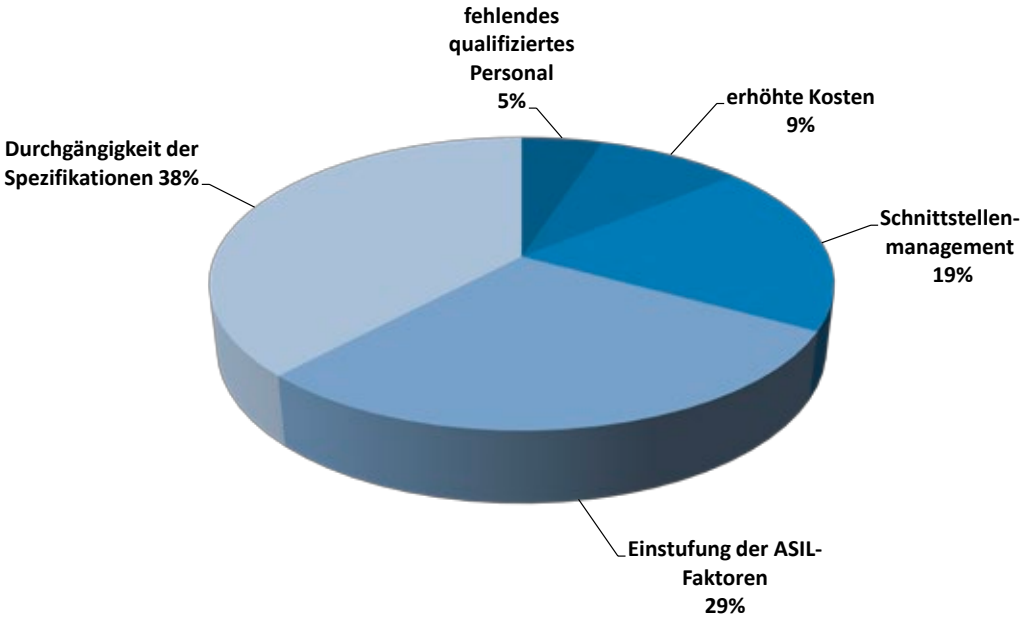
Da in den heutigen Automobilen eine immer größere Anzahl an elektronischen Bauteilen und Steuergeräten verbaut werden und auch eine steigende Vernetzung der einzelnen Elektronik-Komponenten untereinander festzustellen ist, nimmt die Entwicklungskomplexität stetig zu [Richter, H. 2005]. Der Trend, der Zunahme von FuSi-Projekten, wird allerdings durch die begrenzte Verfügbarkeit von qualifiziertem Personal ausgebremst. Mehr als 90% aller befragten Unternehmen gaben an, zu wenig Fachpersonal zu Verfügung zu haben (siehe Abbildung 3). Dieser Engpass verlangsamt oder stoppt nach Angabe einiger Unternehmen die Entwicklung zusätzlicher FuSi-Projekte.

Abbildung 3: Bedarf an qualifiziertem Personal



In der Befragung nannten die Unternehmen vor allem drei Themenschwerpunkte innerhalb der Funktionalen Sicherheit, die in der Praxis bei ihnen zu Problemen führen. Die drei Hauptprobleme sind laut den befragten Unternehmen: die Durchgängigkeit der Spezifikationen, die Einstufung der ASIL-Faktoren und das Schnittstellenmanagement und (siehe Abbildung 4).

Abbildung 4: Die am häufigsten genannten Probleme bei der Funktionalen Sicherheit

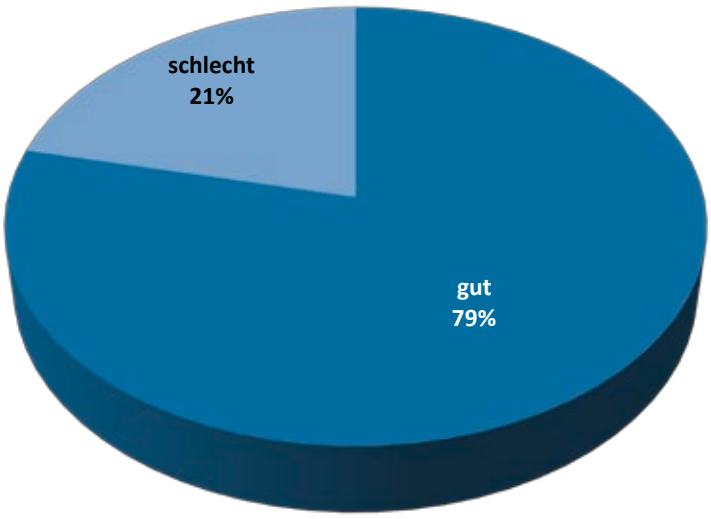


2.1 ASIL

Als eines der drei Hauptprobleme wurde die Einstufung des Automotive Safety Integrity Levels (kurz ASIL) identifiziert. Der ASIL ist das Ergebnis der Gefahren- und Risikountersuchung und gibt die Entwicklungsanforderungen eines Produkts bzw. einer Systemkomponenten an [Löw, P. 2010]. Dieser legt fest, mit welcher Qualität bzw. welchem Aufwand die Systemfunktionen hinsichtlich ihrer Sicherheit ausgelegt werden müssen. Deshalb ist die richtige ASIL-Einstufung von zentraler Bedeutung.

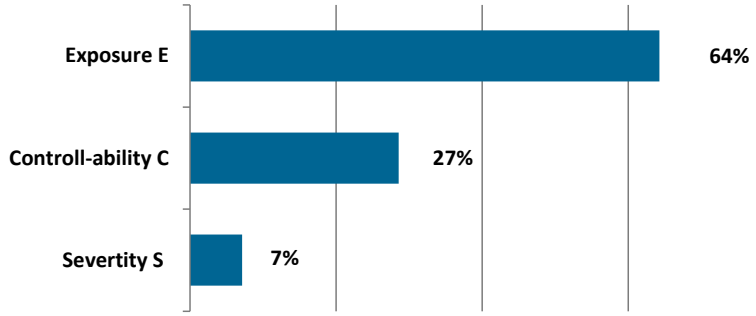
Für die meisten der befragten Unternehmen ist die Einteilung des ASILs wie es die Norm vorgibt gut nachvollziehbar. Fast 80% gaben an, mit der Einteilung des ASILs kein größeres Problem zu haben, wie in Abbildung 5 dargestellt ist.

Abbildung 5: Nachvollziehbarkeit der ASIL-Einstufung in der Norm ISO 26262



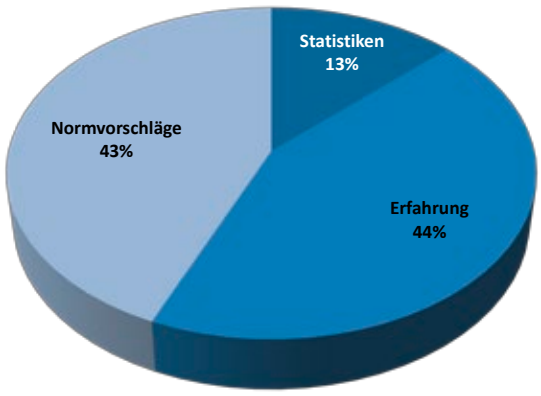
Betrachtet man die einzelnen Faktoren des ASIL aber separat, so lässt sich festhalten, dass die Einschätzung der Häufigkeit des Ausgesetztseins der Fahrsituation (Exposure E) am problematischsten ist. Mehr als 60% der befragten Unternehmen gaben an, dass dieser Faktor für Sie am schwierigsten zu bewerten ist (siehe Abbildung 6) und ca. die Hälfte bemängelt, dass die Norm nicht genügend Orientierung bei der Einschätzung der Exposure gibt. Vor allem unterscheidet die Norm bei der Einstufung des Exposure-Faktors nicht die unterschiedlichen Zielmärkte (z. B. Europa, Amerika, etc.), in denen die Fahrzeuge eingesetzt werden sollen. Die Norm geht davon aus, dass die Exposure weltweit identisch ist [Löw, P. 2010].

Abbildung 6: Der am schwierigsten zu bewertende ASIL-Faktor



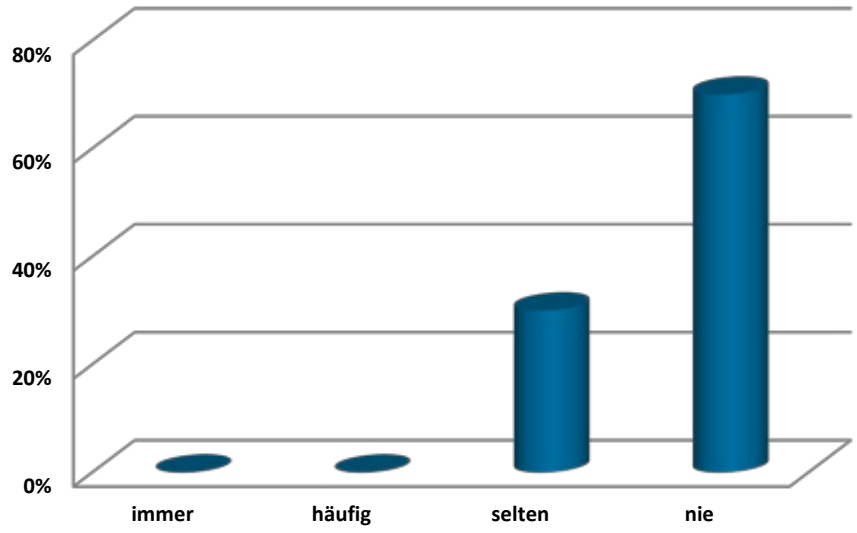
Trotz der fehlenden Detaillierung der Norm verwenden fast die Hälfte der Unternehmen diese zur ASIL-Einstufung. Abbildung 7 zeigt, dass nur 11% der Unternehmen eigene Statistiken zur detaillierten Ermittlung der Exposure einsetzen, um den unterschiedlichen Anforderungen der differenzierten Zielmärkte gerecht zu werden.

Abbildung 7: Verwendete Hilfsmittel zur ASIL-Einstufung



Eine weitere Problematik beim ASIL ist in der hohen Anzahl an Zulieferern innerhalb der Fertigungsketten in der Automobilbrache zu sehen. Bei der Untersuchung stellte sich heraus, dass die Hälfte der Zulieferbetriebe den ASIL durch den OEM oder den übergelagerten Tier vorgegeben bekommt. Jedoch gaben alle Zulieferer an, entweder selten (30%) oder nie (70%), die Datengrundlagen für die ASIL-Einstufung bekommen zu haben, wie es in Abbildung 8 dargestellt ist.

Abbildung 8: Austauschhäufigkeit der Datengrundlage bei der ASIL-Einstufung

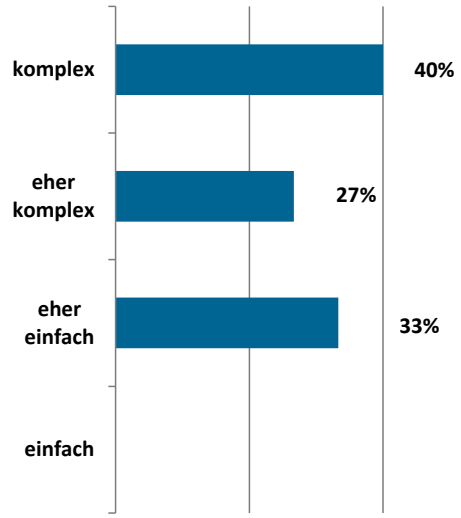


2.2 SCHNITTSTELLEN

Als zweiter Schwerpunkt wurde die Schnittstellenproblematik untersucht. Da Projekte im Kontext der Funktionalen Sicherheit meistens nicht von einem Hersteller allein entwickelt werden, müssen Schnittstellen für den Austausch im System definiert werden [Löw, P. 2010]. Als Schnittstellen kommen die verschiedenen Bussysteme, analoge und digitale Ein- und Ausgänge, Druckluft, Kühlmittel, Öl, Wasser, Spannungsversorgung, etc. in Frage.

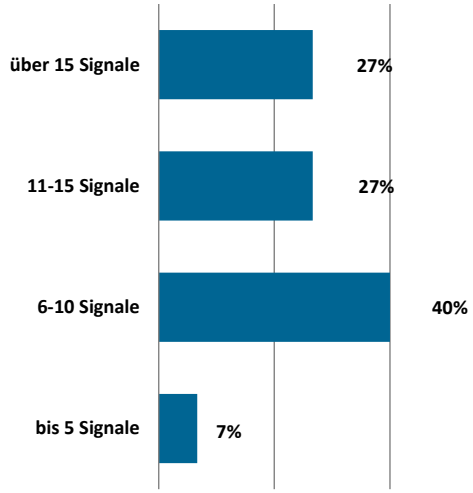
Keines der befragten Unternehmen gab an, ein funktional sicheres Produkt mit einfacher Komplexität zu entwickeln (siehe Abbildung 9). Nur ein Drittel antwortete, dass sie eher einfache FuSi-Produkte entwickeln. Die überwiegende Mehrheit der befragten Unternehmen gaben an, entweder komplexe (40%) oder eher komplexe (27%) Produkte im Kontext der Funktionalen Sicherheit zu entwickeln.

Abbildung 9: Komplexität der FuSi-Projekte



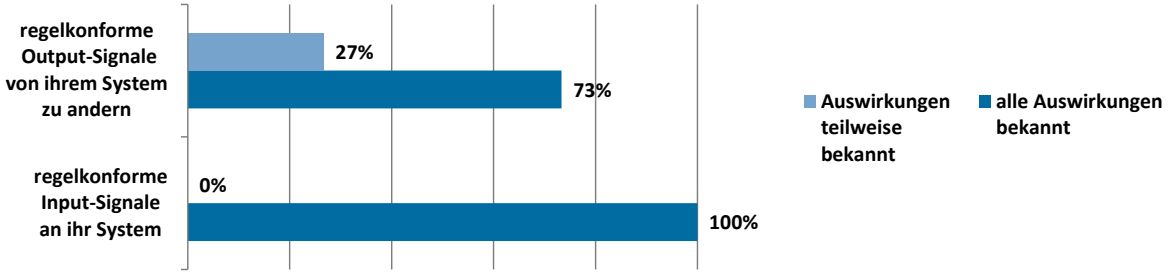
Betrachtet man nur die Datenkanäle (Bussysteme, digitale Ein- und Ausgänge) im Speziellen, ergibt sich ein ähnliches Bild. Nur ein kleiner Teil der befragten Unternehmen gaben an, weniger als fünf elektrische Messwerte und Daten mit anderen Komponenten des FuSi-Projekts auszutauschen. Der Großteil (66 %) der Unternehmen gab an, zwischen 6 und 15 Messwerte und Daten auszutauschen, wie in Abbildung 10 dargestellt ist. Aufgrund der hohen Komplexität der funktional sicheren Produkte teilte ein Viertel der befragten Unternehmen sogar mit, mehr als 15 Mess- und Datensignale auszutauschen.

Abbildung 10: Anzahl der verwendeten Signalkanäle



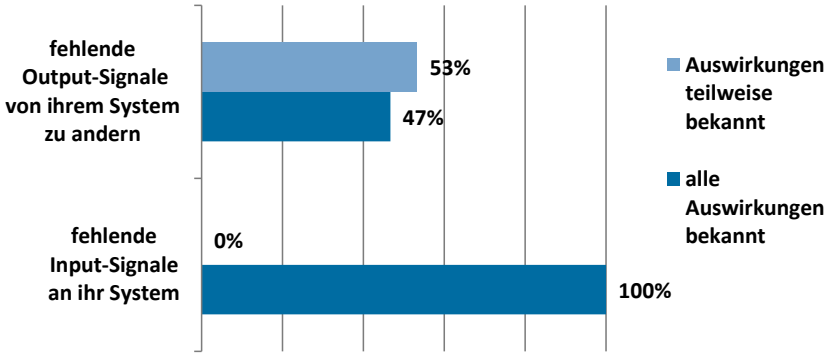
Alle befragten Unternehmen gaben an, von allen Auswirkungen bei regelkonformen Input-Signalen auf ihr System Kenntnis zu haben, wie in Abbildung 11 dargestellt ist. Der Großteil (73%) antwortete ebenfalls, alle Auswirkungen auf andere Komponenten zu kennen, falls ihr System regelkonforme Output-Signale liefert.

Abbildung 11: Bekannte Auswirkungen bei regelkonformen Datensignalen



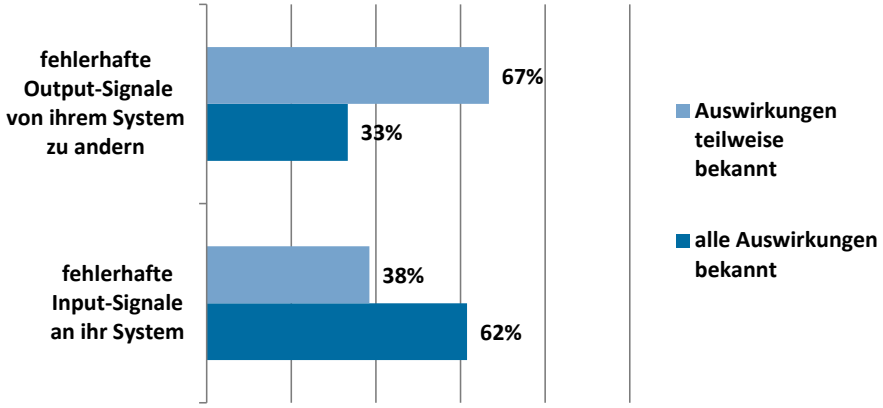
Ein ähnliches Bild ergibt sich, wenn die Unternehmen nach den bekannten Auswirkungen bei fehlenden Datensignalen gefragt werden. Jedes der befragten Unternehmen gab an, dass es alle Auswirkungen auf sein System kennen, falls ihm kein Input-Signal geliefert wird, wie in Abbildung 12 dargestellt ist. Falls ihr System keine Daten-Signale an das Gesamtsystem liefert, gaben noch ca. die Hälfte (47%) der befragten Unternehmen an, alle Auswirkungen zu kennen.

Abbildung 12: Bekannte Auswirkungen bei fehlenden Datensignalen



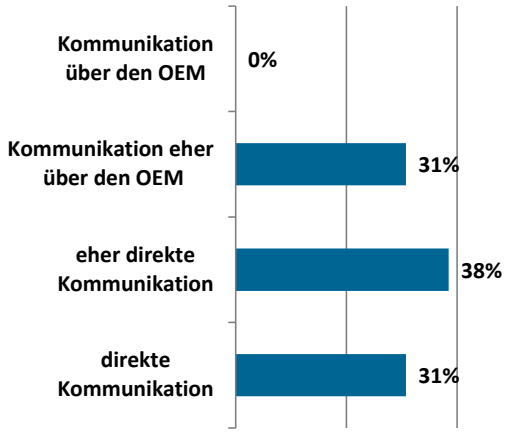
Erst wenn fehlerhafte Signale betrachtet werden, ergibt sich ein kritischeres Ergebnis. So gaben, wie in Abbildung 13 zu sehen, bei einem fehlerhaften Inputsignal nur ca. 60% der befragten Unternehmen an, alle Auswirkungen auf ihr eigenes System zu kennen. Und nur noch ein Drittel der Unternehmen gab an, alle Auswirkungen auf das Gesamtsystem zu kennen, wenn ihr System fehlerhafte Output-Signale an ein anderes System liefert.

Abbildung 13: Bekannte Auswirkungen bei fehlerhaften Datensignalen



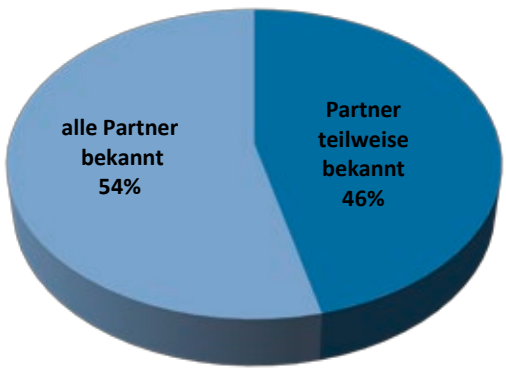
Ein möglicher Grund für die fehlenden Kenntnisse über die Auswirkungen liegt im Schnittstellenmanagement. Die Kommunikation zwischen den verschiedenen Projektpartnern läuft in fast einem Drittel (31%) der Fälle eher über den OEM oder dem übergelagerten Tier (siehe Abbildung 14). Dieses Kommunikationsdreieck führt dazu, dass die Informationen nicht oder nicht korrekt weitergereicht werden. Der Großteil der Unternehmen gab an, entweder direkt (31%) oder eher direkt (38%) mit seinen Projektpartner zu kommunizieren.

Abbildung 14: Kommunikationswege beim Schnittstellenmanagement



Bemerkenswert ist zudem, dass nur ca. die Hälfte (54%) der befragten Unternehmen angaben, alle Partner zu kennen, die bei einem FuSi-Projekt zusammen arbeiten. So ist eine direkte Kommunikation laut der Aussage einiger Unternehmen in diesen Fällen nicht möglich.

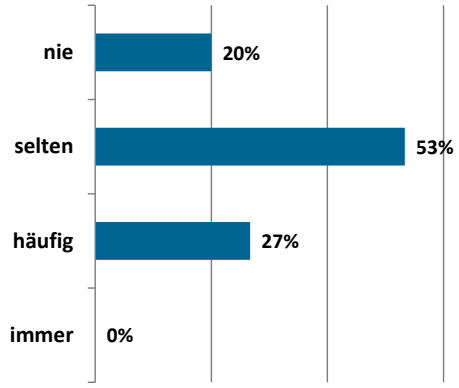
Abbildung 15: Kenntnisse über Projektpartner



2.3 SPEZIFIKATIONEN

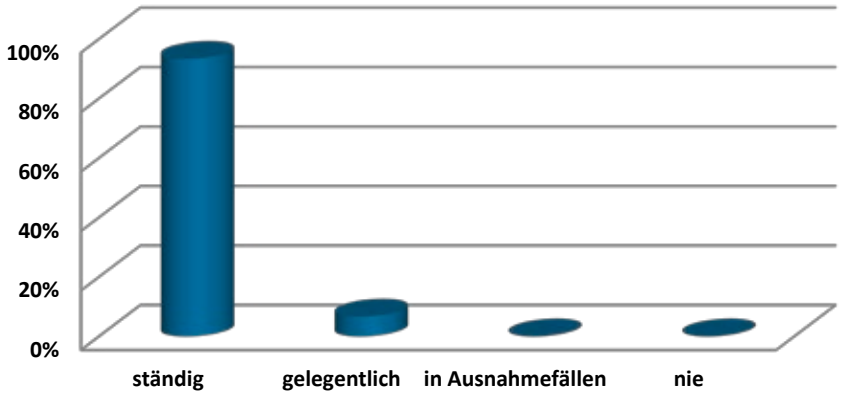
Als letzer Schwerpunkt wurde die Durchgängigkeit der Requirements bzw. der Spezifikationen betrachtet. Keines der befragten Unternehmen gab an, dass sie immer mit einem vollständigen Lastenheft die Entwicklung von funktional sichereren Produkten beginnen (siehe Abbildung 16). Der Großteil der befragten Unternehmen gab an, nur selten (53%) oder häufig (27%) zu Beginn der Entwicklung mit einem vollständigen Lastenheft zu arbeiten. 20% der Befragten teilten mit, dass sie nie mit einem vollständigen Lastenheft mit allen Spezifikationen beginnen.

Abbildung 16: Vorhandensein des vollständigen Lastenheftes zu Entwicklungsbeginn



Des Weiteren gaben die befragten Unternehmen an, dass das Lastenheft in über 90% aller Fälle ständig an laufende Veränderungen innerhalb des Projekts angepasst wird, wie in Abbildung 17 dargestellt ist.

Abbildung 17: Anpassungszyklen der Spezifikationen im Lastenheft

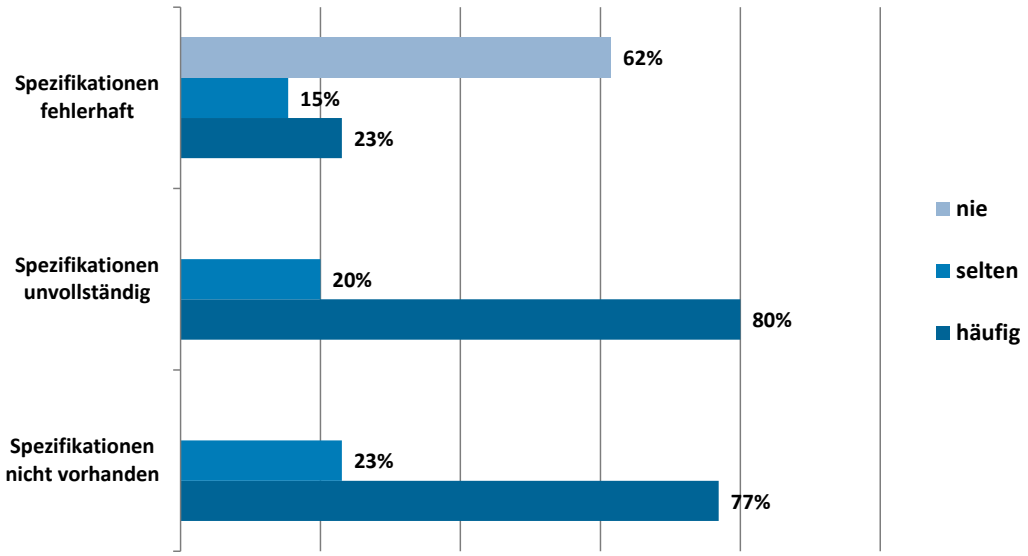


Betrachtet man die einzelnen Anpassungen des Lastenheftes, ist zu erkennen, dass zu Entwicklungsbeginn laut Aussagen der befragten Unternehmen häufig Teile der nötigen Spezifikationen im Lastenheft nicht vorhanden (77%) sind (siehe Abbildung 18). Nur ein kleiner Teil gab an, dass sie selten (23%) mit fehlenden Spezifikationen die Entwicklungsarbeit beginnen.

Ein nahezu identisches Bild ergibt sich bei der Betrachtung von unvollständigen Spezifikationen. Die befragten Unternehmen gaben an, entweder häufig (80%) oder selten (20%) mit unvollständigen Spezifikationen im Lastenheft die Entwicklung von funktional sicheren Produkten zu beginnen.

Dass fehlerhafte Spezifikationen im Lastenheft vorhanden sind, kommt laut Aussage der Unternehmen, größtenteils (62%) nie vor, wie in Abbildung 18 dargestellt ist. Nur ein kleiner Teil der befragten Unternehmen gaben an, dass sie selten (15%) oder häufig (23%) mit fehlerhaften Spezifikationen im Lastenheft konfrontiert werden.

Abbildung 18: Spezifikationen im Lastenheft



3. ABBILDUNGSVERZEICHNIS

4. LITERATURVERZEICHNIS

[Baumann, U. 2007] Baumann, Ulrich, Sensor-Ausfall - Ford-Mega-Rückruf. 2007. http://www.auto-motor-und-sport.de/news/ford-mega-rueckruf-sensor-ausfall-712702.html (22.03.2013)

[Baumann, U. 2011] Baumann, Ulrich, Verkabelung wird modifiziert - VW ruft US-Jetta zurück. 2011. http://www.auto-motor-und-sport.de/news/vw-ruft-us-jetta-zurueck-verkabelung-wird-modifiziert-3569519.html (22.03.2013)

[Bücheler, R. 2008] Bücheler, Ralf, XC90 mit Software-Problem - Volvo-Rückruf. 2008. http://www.auto-motor-und-sport.de/news/volvo-rueckruf-xc90-mit-software-problem-711983.html (22.03.2013)

[ISO 26262:2011] SO 26262:2011, Road vehicles - Functional safety

[Kowaleski, S. 2008] Kowaleski, Stefan; et al, Zuverlässigkeit von automotive embedded Systems. FAT-Schriftreihe 231, Aachen, 2008

[Löw, P. 2010] Löw, Peter; Pabst, Roland; Petry, Erwin, Funktionale Sicherheit in der Praxis – Anwendung von DIN EN 61508 und ISO/DIN 26262 bei der Entwicklung von Serienprodukten. 1. Aufl. Heidelberg: dpunkt.verlag, 2010

[Pohl, K. 2009] Pohl, Klaus; Rupp, Chris, Basiswissen Requirements Engineering. 1. Aufl. Heidelberg: dpunkt.verlag, 2009

[Reif, K. 2011] Reif, Konrad, Bosch Autoelektrik und Autoelektronik – Bordnetze, Sensoren und elektronische Systeme. 6. Aufl. Wiesbaden: Vieweg+Teuber, 2011

[Richter, H. 2005] Richter, Harald, Elektronik und Datenkommunikation im Automobil. Technical Report Series Ifl-09-05 , Clausthal, 2005

[Schachtner, M. 2011] Schachtner, Martin, CR-Z erneut mit Softwareproblem. 2011. http://www.autoservicepraxis.de/cr-z-erneut-mit-softwareproblem-1061174.html (22.03.2013)

[Stockburger, C. 2011] Stockburger, Christoph, Defekte Steckverbindungen: BMW ruft 750.000 Autos zurück. 2011. http://www.spiegel.de/auto/ werkstatt/rueckruf-von-1-3-millionen-autos-blamage-fuer-benz-a-349049.html (22.03.2013)

KONTAKT

Fraunhofer-Institut für Produktions-technik und Automatisierung IPA

Nobelstraße 12
70569 Stuttgart

Ansprechpartner
Dipl.-Ing. Christoph Maier

Telefon +49 711 970-1741
christoph.maier@ipa.fraunhofer.de

www.ipa.fraunhofer.de