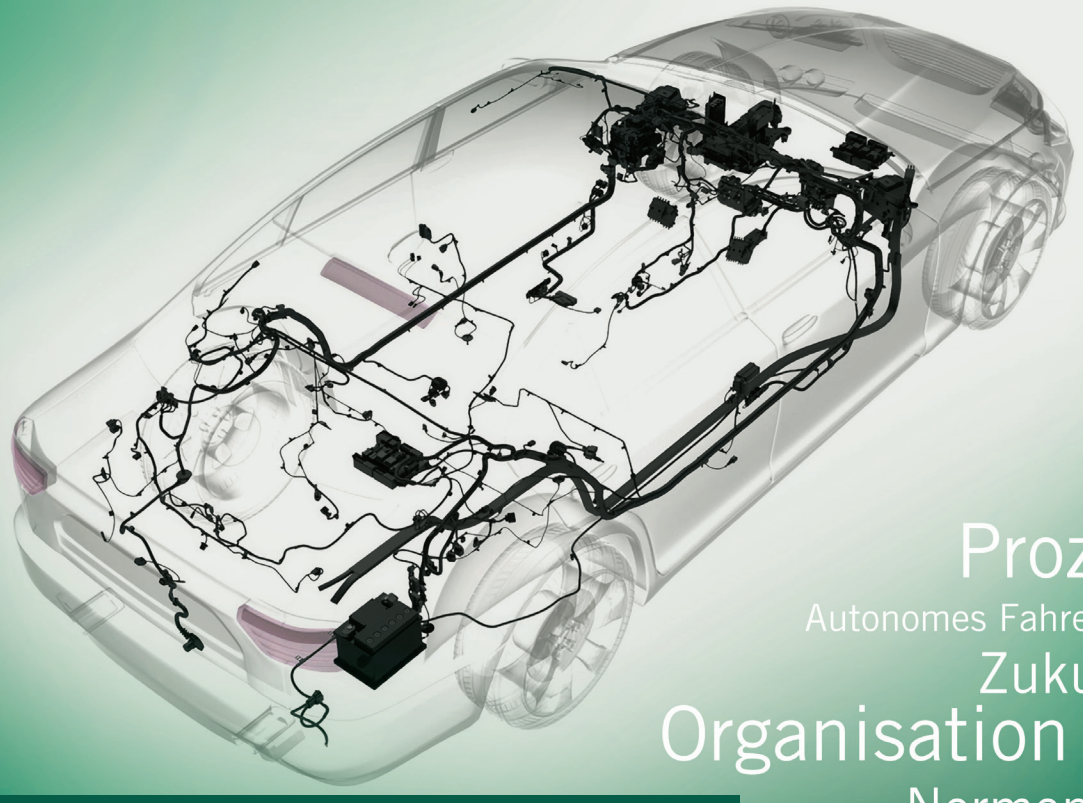


Umdenken

Funktionale Sicherheit benötigt eine neue Prozessorganisation

Durch autonomes und hochautomatisiertes Fahren ergeben sich insbesondere in Bezug auf sicherheitsrelevante Funktionen neue Anforderungen im Automobilbereich. Doch mit welchen Mitteln begegnet man diesen Herausforderungen? Eine mögliche Antwort auf diese Frage liegt in der nicht immer trivialen Umsetzung der Norm ISO 26262, wie sie Dräxlmaier am Beispiel der Bordnetzentwicklung beschreibt.

ERGÄNZUNG ETABLIERTER STANDARDS

Mit dem SAE Level 3 „Conditional Automation“ rückt der nächste Meilenstein auf dem Gebiet des automatisierten Fahrens näher: das sogenannte hochautomatisierte Fahren. Mit diesem Entwicklungsschritt geht eine wesentliche Veränderung der Umgebungsbeobachtung während des Fahrens einher: Statt des Fahrers übernehmen diese Aufgabe nun eine Vielzahl von Sensoren.

Was dies für sicherheitsrelevante Funktionen wie das Lenken und Bremsen bedeutet, liegt auf der Hand: Hier gewinnt der Aspekt der funktionalen Sicherheit zum Schutz der Passagiere erheblich an Bedeutung. Im Hinblick darauf, dass die SAE-Stufen 4 und 5, die bald folgen werden, eine noch weitreichendere Automation von Fahrfunktionen vorsehen, wird das Thema Sicherheit sogar noch weiter in den Fokus rücken, **BILD 1**.

In Anbetracht der Komplexität heutiger Bordnetzsysteme führt dies zu einer deutlichen Erhöhung des Entwicklungsaufwands, da die Toleranz gegenüber etwaigen Systemfehlern sinkt. So gut die heutigen Qualitäts- und Prozessmanagement-Methoden auch sind, so stoßen diese hier an ihre Grenzen. Aus diesem Grund wurde die Norm ISO 26262:2011 verfasst, welche noch dieses Jahr in einer aktualisierten Version erscheint. Sie basiert im Wesentlichen auf einem V-Modell, das spezielle Anforderungen an die Projektdurchführung enthält, **BILD 2**.

AUTOREN

Oliver Druhm
ist Teamleiter Konzeptentwicklung Bordnetze bei der Dräxlmaier Group in Vilsbiburg.

Dr. Martin Gall
ist CTO der Dräxlmaier Group in Vilsbiburg.

Georg Scheidhammer
leitet das Ressort Strategie und Innovationen der Entwicklung bei der Dräxlmaier Group in Vilsbiburg.

Während die ISO 26262 im Bereich der Steuergeräteentwicklung bereits angewendet wird, bieten die etablierten Prozesse derzeit keine ausreichenden Lösungen, um auf die Herausforderungen auf Gesamtfahrzeugebene und in Bezug auf das gesamte Bordnetz zu reagieren. Der in der Entwicklung verbreitete Standard Automotive Spice ist zwar eine wesentliche Voraussetzung, um die funktionale Sicherheit von Produkten zu gewährleisten, er greift jedoch nicht weit genug. Einen Schritt weiter gehen bereits die Bestimmungen der IATF 16949 – aber nur die ISO 26262 stellt sicher, dass, bezogen auf sicherheitsrelevante Funktionen, der gesamte Sicherheitslebenszyklus betrachtet wird. Darunter fallen auch die der Entwicklung und Produktion nachgelagerten Prozesse während der Nutzungsdauer, beispielsweise in den Bereichen Betrieb, Service und Außerbetriebnahme des Fahrzeugs, **BILD 3**.

ZUVERLÄSSIGKEIT IM FOKUS

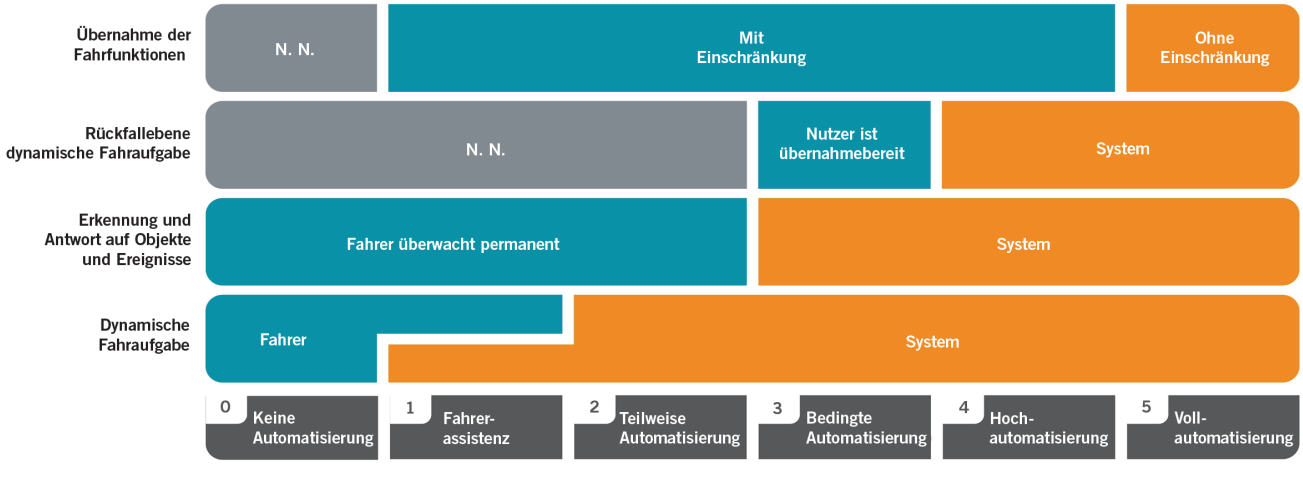
Um am Ende des Entwicklungsprozesses ein funktional sicheres System zu erhalten, ist es von besonderer Wichtigkeit, mögliche Fehlerquellen bereits im Vorfeld zu erkennen. Hierzu werden zwei Fehlerkategorien unterschieden: die zufälligen Fehler und die systematischen Fehler. Zufällige Fehler werden gemäß der ISO 26262 anhand ihrer FIT-Raten (Failure in Time) analysiert und ausgewertet. Diese dienen im Kern dazu, die richtigen Materialien und Komponenten auszuwählen. FIT-Raten wurden und werden unter definierten Bedingungen bestimmt und festgelegt. Darüber hinaus ist für eine Nutzung in jedem Projekt der zugehörige Anwendungsfall zu definieren. Nur dann, und unter der Voraussetzung, dass für die definierten FIT-Raten die dazugehörigen Prozesse eingehalten werden, besitzen diese Gültigkeit in der Gesamtsystembetrachtung. Systematische Fehler dagegen können beim Entwurf, bei der Herstellung oder beim Betrieb eines Systems auftreten und sind nahezu immer vorhersehbar. Dies unterscheidet sie von den zufälligen Fehlern.

Basierend auf Anwendungsfällen entlarvt eine Gefahren- und Risikoabschätzung gemäß ISO 26262 potenzielle Gefährdungen und ermittelt, wo Risiken notwendigerweise reduziert werden müssen. Um die definierten Ziele zu erreichen, gibt es spezielle Vorgaben, mit denen systematische und auch zufällige Fehler vermieden werden sollen. Am Ende dieses Prozesses steht eine Einstufung in den Automotive Safety Integrity Level (ASIL). Dieser ordnet dem zu entwickelnden System ein FIT-Ratenbudget zu und bestimmt zugleich, welche Maßnahmen systematisch zu ergreifen sind.

PROZESSUALER WERKZEUGKASTEN

Die ISO 26262 stellt einen prozessualen Werkzeugkasten zur Verfügung, um die notwendigen Systeme entwickeln, produzieren und betreiben zu können. Dieser umfasst unter anderem Forderungen an den Entwicklungsprozess, wie die Etablierung eines Sicherheitslebenszyklus, die Fehlerbeherrschung und das Anforderungsmanagement. Dadurch kann das Sicherheitsmanagement im Sinne der ISO 26262 nicht isoliert von normalen Engineering-, Test- und Produktionsprozessen betrachtet werden. Es ergänzt und verbessert vielmehr die bereits bestehenden Prozesse. Die ISO 26262 definiert hierzu erforderliche Aktivitäten und Ergebnisse, sogenannte Work Products,

BILD 1 Autonomiestufen 0 bis 5 nach SAE J3016 (© ATZelektronik)



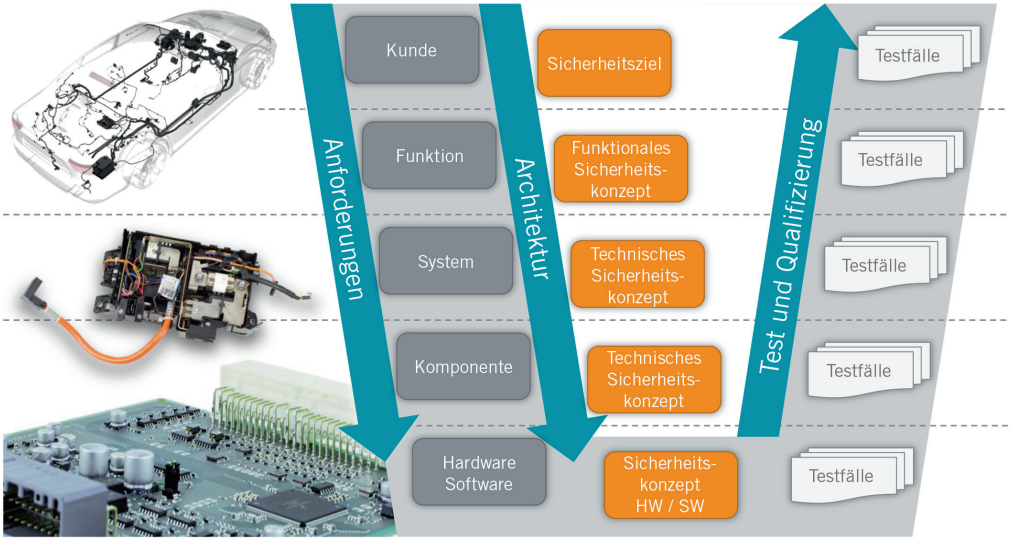


BILD 2 Die ISO 26262 kann nicht isoliert von normalen Engineering-, Test- und Produktionsprozessen betrachtet werden, sondern vielmehr als eine Weiterentwicklung dieser Prozesse (© Dräxlmaier)

spezifische Methoden für die Bereiche Engineering, Test und Produktion sowie Akquisitions- und Lieferantenprozesse. Ähnlich der Realisierung in einem gängigen Anforderungsmanagement, schenkt die ISO 26262 der „Traceability" und „Consistency" viel Aufmerksamkeit. Darüber hinaus fügt sich das Prozessmodell der ISO 26262 sehr gut in die bereits etablierten Methoden ein, die zum Beispiel im Standard Automotive Spice definiert werden.

EINFÜHRUNG EINER SICHERHEITSKULTUR

Die ISO 26262 ist jedoch weit mehr als ein reiner Werkzeugkasten zum Umgang mit zukünftigen Anforderungen: Sie ist auch mit der Forderung verbunden, eine Sicherheitskultur in Unternehmen und bei den beteiligten Projektpartnern zu etablieren. Der Projekterfolg hängt also nicht nur von einer rein formalen Adaption der ISO 26262 ab. Dabei darf diese Sicherheitskultur nicht mit dem ebenfalls geforderten Sicherheitsmanagement gleichgesetzt werden.

Die von der ISO 26262 geforderten neuen Prozesse und Rollen, wie zum Beispiel der Manager für funktionale Sicherheit oder der Sicherheitskoordinator, greifen mehr oder weniger stark in die Aufbau- und Ablauforganisation sowie in die Prozesse einer Organisation ein. Die Norm bestimmt die spezifischen Aktivitäten und Methoden, die angewendet werden müssen. Der Erfolg hängt aber maßgeblich von der Akzeptanz und dem Verständnis der Projektbeteiligten ab. Die ISO 26262 enthält nämlich noch eine zusätzliche Herausforderung: Während ein Sicherheitsmanagement – wie jeder Managementprozess – beschreibbar und erlernbar ist, muss der Etablierung einer Sicherheitskultur stets eine Veränderung der Denkweise aller Beteiligten vorausgehen, die sich über ein gemeinsames Verständnis und dementsprechende Verhaltensmuster definiert.

Es ist bemerkenswert, dass eine solche, nur schwer fassbare Voraussetzung durch eine Norm wie die ISO 26262 vorgegeben wird. Bei der Adaption der ISO 26262 ergibt sich auf diese Weise eine besondere Herausforderung. Denn selbst wenn alle prozessualen Notwendigkeiten etabliert sind, steht und fällt die Entwicklung sicherheitskritischer Funktionen mit der Etablierung einer Sicherheitskultur.

Um eine erfolgreiche Einführung der ISO 26262 zu garantieren, ist eine frühzeitige Einbindung aller Projektbeteiligten enorm wichtig. Jedem Mitarbeiter muss klar und transparent kommuniziert werden, mit welchen Veränderungen gerechnet werden muss. Wichtig ist auch, dass bei allen Beteiligten ein Verständnis des Gesamtprozesses vorhan-

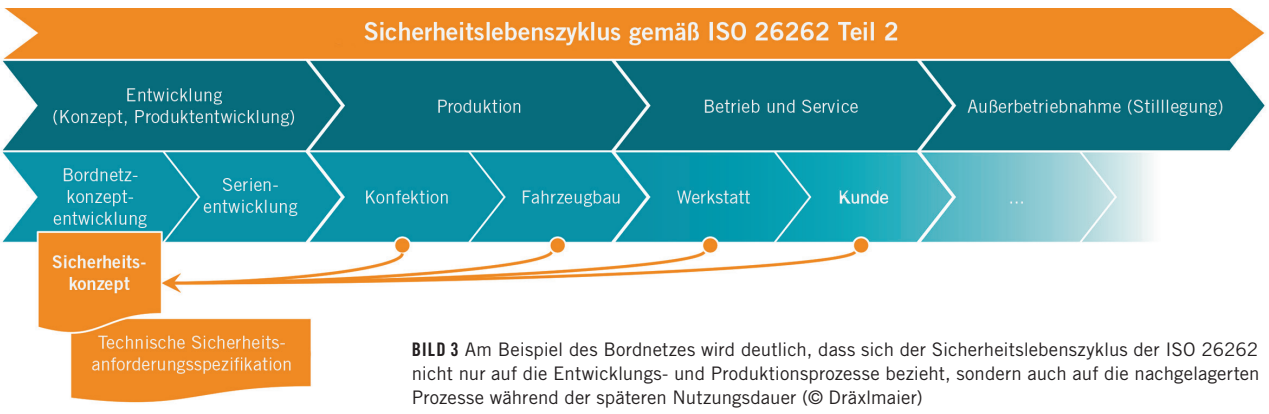


BILD 3 Am Beispiel des Bordnetzes wird deutlich, dass sich der Sicherheitslebenszyklus der ISO 26262 nicht nur auf die Entwicklungs- und Produktionsprozesse bezieht, sondern auch auf die nachgelagerten Prozesse während der späteren Nutzungsdauer (© Dräxlmaier)


smthybridpackaging
Nürnberg, 05.–07.06.2018
Jetzt kostenfreies Ticket sichern:
smthybridpackaging.de
mesago
Messe Frankfurt Group

den ist. Letztendlich muss sich im Sinne der Sicherheitskultur jeder Mitarbeiter mit seiner Rolle identifizieren. Damit kommt insbesondere dem Management eine große Aufgabe bei der Einführung der ISO 26262 zu.

POTENZIALE DER IMPLEMENTIERUNG

In der Umsetzung der ISO 26262 liegt aber auch ein großes Potenzial. So wird der relativ hohe Aufwand bei der Einführung eines Prozess-Systems schnell durch dessen spezifische Vorteile kompensiert. Besonders relevant: Die resultierenden Systeme können einen wesentlich höheren Qualitätsstand erreichen und verursachen deshalb weniger Folgekosten. Es bietet sich sogar an, die gewonnenen Erkenntnisse auf verwandte Prozesse im Unternehmensumfeld auszuweiten.

Projektbeteiligte werden schnell erkennen, dass die neu eingeführten Prozesse durch die beiden Faktoren Traceability und Consistency für eine größere Transparenz sorgen. Dies unterstützt die effiziente Gestaltung von Prozessen.

Es kann daher festgehalten werden: Auch wenn mit der Erstimplementierung der ISO 26262 durchaus ein Mehraufwand entsteht, so kann im Gegenzug der Aufwand, der mit dem Transformationsprozess zwangsläufig einhergeht, zum Großteil kompensiert werden. Dies gelingt insbesondere dadurch, dass alle Prozesse davon profitieren können – nicht nur solche, die sicherheitsrelevante Systeme betreffen.

Diese Potenziale können umso schneller gehoben werden, je enger die betroffenen Organisationen in allen Phasen zusammenarbeiten – von der Prozessanalyse über die Konzeption und Implementierung bis hin zur Nutzung.

Insbesondere im Hinblick auf die Entwicklungen im Automobilmarkt, welche durch das Thema hoch- und vollautomatisiertes Fahren entstehen, wird es interessant sein zu beobachten, wie die verschiedenen Unternehmen mit dieser Herausforderung umgehen.

BEISPIEL BORDNETZENTWICKLUNG

Aus den skizzierten Vorgängen zur Gewährleistung der funktionalen Sicherheit von Fahrzeugen ergeben sich sehr spezielle Anforderungen an den Leitungssatz als vernetzendes Element zwischen einer Vielzahl von Komponenten und Teilsystemen. Er ist im wahrsten Sinne des Wortes das physische Abbild aller prozessualen Schnittstellen in der Fahrzeugentwicklung und -produktion. Ändern sich Anforderungen an einer Stelle, hat dies schon heute Auswirkungen auf andere Komponenten im Bordnetz – allerdings müssen diese bei Anwendung der ISO 26262 nun in einem durchgängigen Änderungsmanagement dokumentiert werden. Da es zugleich notwendig ist, bei einer Änderung alle nachgelagerten Prozesse zu berücksichtigen, müssen die Anforderungen der spezifischen Fahrzeugarchitektur vollständig bekannt sein.

Gerade hier greifen die in der ISO 26262 festgehaltenen Forderungen nach Traceability und Consistency, denn nur so können die in komplexen Fahrzeugprojekten auftretenden Änderungen zuverlässig abgearbeitet werden. Dabei müssen die folgenden Fragen stets im Fokus stehen: „Was ist zu testen?“, „Wie muss getestet werden?“, „Welches Produktionsverfahren ist zu wählen?“ und „Ist die durchgängige ISO 26262-Konformität sichergestellt?“. Ziel muss es stets sein, Änderungen nahtlos in das Gesamtfahrzeugkonzept einzufügen. Der Arbeitskreis „ASIL-Metrik im Bordnetz“, der vom Cluster Automobil bei der Bayern Innovativ betrieben wird, beschäftigt sich seit dem Frühjahr 2015 mit der gesamthaften Thematik. Der Arbeitskreis setzt sich derzeit aus circa 20 Firmen der Automobilbranche zusammen, zu denen auch die Dräxlmaier Group zählt.

Die Zielsetzung des Arbeitskreises ist es, eine Gesamtsystembetrachtung des Bordnetzes sowie der jeweiligen Komponenten durchzuführen und daraus verbindliche Metriken zur FIT-Raten-Betrachtung sowie Handlungsempfehlungen abzuleiten. Der thematische Schwerpunkt liegt dabei auf der Betrachtung zufälliger Hardwarefehler. Voraussetzung für die Definition der FIT-Raten ist jedoch, dass die Fertigungsprozesse fehlerfrei funktionieren.

In den Untersuchungen wurde schnell klar, dass aufgrund der Komplexität eines Bordnetzes unmöglich alle Komponenten betrachtet und untersucht werden können. Hinzu kommt, dass gemäß der ISO 26262 möglichst eine Komplexitätsreduzierung anzustreben ist. Um diesen Anforderungen zu entsprechen, wurden passende Design Rules entwickelt. Ein wesentlicher Aspekt ist dabei die automatisierte Fertigung von Komponenten, da durch sie potenzielle Fehlerquellen aus der manuellen Fertigung ausgeschlossen werden können. Hierbei ist zu beachten, dass die ISO 26262 grundsätzlichkeinebestimmtentechnologischenUmsetzungen fordert. Eine automatisierte Fertigung kann jedoch als zielführend angesehen werden, da sie bessere Möglichkeiten der Prozessüberwachung bietet und so den Forderungen der ISO 26262 nach Rückverfolgbarkeit und Konsistenz zuträglich ist. Um einen Leitungssatz automatisiert fertigen zu können, ist es von Vorteil, wenn dieser nur Punkt-zu-Punkt-Verbindungen aufweist. Dies kommt zugleich dem Ziel der Komplexitätsreduzierung entgegen. Einfache elektrisch-elektronische Architekturen, die möglichst ohne Trennstellen oder anderweitige Verbinder auskommen, sind also zielführend.

Gerade Verbinder stellen für die funktionale Sicherheit von Bordnetzen eine Herausforderung dar: So kann es beispielsweise bei Ultraschallschweißprozessen durch Schwingungsübertragungen über die Leitung zu Brüchen an den Kontakten kommen. Im Hinblick auf die Forderungen der ISO 26262 entsteht so ein viel zu hoher Absicherungsaufwand. Der Arbeitskreis „ASIL-Metrik im Bordnetz“ empfiehlt daher, bei funktionssicherheitsrelevanten elektrischen Funktionen auf ultraschallgeschweißte Verbinder zu verzichten. Darüber hinaus sollten die für die funktionale Sicherheit relevanten Teile des Bordnetzes vom restlichen Leitungssatz getrennt werden.

Wesentlich für die Gewährleistung der funktionalen Sicherheit ist also die Wahl einer möglichst einfachen Bordnetzarchitektur, denn: Je weniger Komplexität der Leitungssatz aufweist, desto weniger Elemente müssen entsprechend der ISO 26262 abgesichert werden.

In der topologischen Betrachtung sollten zudem möglichst crashgeschützte und vibrationsarme Bauräume genutzt werden. Sind für sicherheitsrelevante Funktionen redundante Auslegungen notwendig, so empfiehlt es sich, für die jeweiligen Komponenten und Leitungen unterschiedliche Topologiesegmente zu verwenden.

EIN UMDENKEN IST ERFORDERLICH

Geregelte Prozesse sowie eine passende sicherheitsbezogene Denkweise aller Betroffenen sind unter dem Strich der Schlüssel für funktional sichere Produkte. Die entsprechende technische Auslegung von Komponenten basiert letztendlich darauf, dass Menschen im Rahmen der Prozesse der ISO 26262 die richtigen Maßnahmen ergreifen, um das Produkt im Sicherheitslebenszyklus reifen zu lassen und zu betreiben.

Die Umsetzung der ISO 26262 stellt somit im Kern eine Herausforderung im Bereich der Organisation dar. Im Automobilsektor ist davon insbesondere die übergreifende Projektorganisation betroffen, da sich alle Beteiligten – OEM und Zulieferer – intensiver als bisher abstimmen müssen. Die Entwicklung funktional sicherer Systeme ist darüber hinaus zunehmend eine interdisziplinäre Tätigkeit, in der jeder sein Wissen und vor allem seine Erfahrung einbringen muss. Die Aufgabe der Gesamtsystemverantwortlichen auf den jeweiligen Ebenen der Lieferkette ist es, bei allen Beteiligten ein Bewusstsein für die neuen Prozesse der ISO 26262 zu etablieren, sie untereinander zu vernetzen und Verantwortlichkeiten klar zu definieren.

Der Exkurs in die Bordnetzentwicklung zeigt beispielhaft die Herausforderungen auf, welche die Anwendung der ISO 26262 bei der Fertigung komplexer Bauteile mit sich bringt. Besonders erfolgreich wird derjenige sein, der es schafft, die Adaption der neuen Norm zeitnah umzusetzen. Dabei wird nicht zuletzt der Know-how-Transfer aus anderen Bereichen eine große Rolle spielen.