Neuer Standard zur Entwicklung von Software für Automobile

Crash-Vorsorge

Bertram Janositz

Für die funktionale Sicherheit von Straßenfahrzeugen wird mit ISO 26262 demnächst eine neue weltweit gültige Norm eingeführt. Das hat weitreichende Folgen für die Optimierung von Entwicklungs- und Produktionsprozessen in der Automobilindustrie.

Wenn Raumsonden wegen technischer Mängel auf der Marsoberfläche zerschellen, ist viel Geld – sehr weit – aus dem Fenster geworfen worden. So etwas passiert vergleichbar in vielen Branchen. In der Automobilentwicklung geht es jedoch um mehr. Schwere Unfälle, Verletzungen, Todesfälle – solche Komplikationen möchten Autoentwickler vermeiden. Allein 2009 wurden in Europa 39 000 Verkehrstote gezählt. Die meisten Unfälle sind kein Problem der funktionalen Sicherheit. Da die Elektronik aber immer mehr Funktionen im Auto übernimmt, rücken diese Themen schnell in den Vordergrund.

In der Automobilindustrie scheinen sich die Rückrufe wegen Softwareproblemen herstellerübergreifend zu häufen. Ob Renault, Kia oder der einstige Qualitätschampion Toyota, keiner ist vor Softwareproblemen gefeit. Die deutschen Hersteller haben deshalb in den letzten Jahren ihr Qualitätsbewusstsein hinsichtlich der Software geschärft und umfangreiche Qualitätsprogramme umgesetzt, letztlich lassen sich bei steigender Komplexität Softwarefehler aber niemals ausschließen. Dramatisch wird es, wenn sicherheitskritische Systeme versagen und Menschenleben gefährden.

Zeitgemäßere Sicherheitsnorm

Die technischen Innovationen in der Automobilentwicklung der letzten Jahre, speziell für die Serienproduktion, ließen sich mit den bisherigen Sicherheitsnormen nicht mehr vollständig abdecken. Deshalb wurde basierend auf der IEC 61508 (siehe Glossar) eine weitere Norm entwickelt, die Mitte 2011 als ISO 26262 erscheinen soll.

Unter Sicherheit versteht man die Abwesenheit von Gefahr. Funktionale Sicherheit ist die Sicherheit der Funktionen eines Geräts. Wenn eine Hardware, etwa ein Navigationsgerät, bei einem Unfall in den Fahrerraum geschleudert wird, ist das ein Sicherheitsproblem. Löst jedoch das Navigationsgerät im Zusammenspiel mit einem Fahrassistenten durch eine Fehlfunktion eine kritische Situation aus, ist das ein Problem der funktionalen Sicherheit.

Bisher gilt für die Entwicklung elektronischer Geräte die IEC 61508. Speziell für die Entwicklung von Automobilelektronik ist die Norm schwer interpretierbar. Ende der 1970er-Jahre hatte ein Auto nicht mehr als eine Handvoll Steuergeräte. Heute ist die Elektronik längst zum Innovationstreiber in der Automobilentwicklung geworden. 70 und mehr vernetzte Steuergeräte sind keine Ausnahme mehr, und die Entwicklung schreitet stetig voran.

Die IEC 61508 definiert Sicherheit im Sinne von Betriebssicherheit (siehe Glossar) als „Freiheit von unvertretbaren Risiken“. Funktionale Sicherheit ist der Norm zufolge der Teil der Gesamtsicherheit, der von der korrekten Funktion des sicherheitsbezogenen Systems abhängt. Bleibt zu erwähnen, dass die Sicherheitsnormen in erster Linie auf die Vermeidung von Personenschäden ausgerichtet sind. Die Reduzierung von Vermögensschäden hat erst zweite Priorität.

Mit der geplanten Veröffentlichung der ISO 26262 im nächsten Jahr wird dieser Entwicklung Rechnung getragen. Für Unternehmen, die Automobilelektronik programmieren, entsteht damit eine heikle Situation. Sie müssen bereits mit Veröffentlichung der Norm alle Anforderungen erfüllen, auch wenn sie mit der Entwicklung der Steuergeräte schon vor Jahren begonnen haben. Das Produkthaftungsgesetz gilt für alle an dem Produkt beteiligten Unternehmen und damit auch für die Autohersteller. Die Anforderungen werden in den Verträgen mit ihren Zulieferern eher „schwammig“ als „Stand der Technik“ umschrieben.

Glossar

Sicherheit: Der Begriff wird im deutschen Sprachgebrauch in zwei unterschiedlichen Bedeutungen verwendet, die klar zu unterscheiden sind. Zum einen ist die Angriffssicherheit zu nennen, die Schutz vor Angriffen von außen bietet. Sie schützt Menschen und technische Systeme, insbesondere IT-Systeme. Im Englischen spricht man von „Security". Funktionale Sicherheit ist zum anderen ein Teil der Betriebssicherheit, die umgekehrt Menschen und Umwelt vor den Gefahren eines technischen Systems, einer Anlage oder eines Geräts schützt. Im Englischen wird der Begriff „Safety" hierfür verwendet. Wenn nun die Sicherheit des Systems von der korrekten Funktionsweise seiner elektrischen oder elektronischen Bauteile oder der darin enthaltenen Software abhängt, ist das die funktionale Sicherheit, im Englischen als „Functional Safety" bezeichnet.

Sicherheitsnorm: Die IEC 61508 ist eine internationale Norm zur Entwicklung elektrischer, elektronischer und programmierbar elektronischer Systeme, die eine Sicherheitsfunktion ausführen. Sie wird von der International Electrotechnical Commission (IEC) herausgegeben (www.iec.ch/functional safety). Hiervon sind Normen für unterschiedliche Anwendungsbereiche abgeleitet wie die EN 50128 für Bahnanwendungen, die IEC 61513 für Kernkraftwerke, die DO187B für die Luftfahrt und auch die ISO 26262 für Pkw.

Betriebssicherheit: Die Sicherheitsnorm DIN EN 61508 definiert Sicherheit im Sinne von Betriebssicherheit als „Freiheit von unvertretbaren Risiken". Funktionale Sicherheit ist der Teil der Gesamtsicherheit, der von der korrekten Funktion des sicherheitsbezogenen Systems abhängt. Funktionale Sicherheit und Reifegradmodelle ergänzen sich.

Die ISO 26262 beschreibt die Anforderungen an den gesamten Produktlebenszyklus sicherheitsrelevanter elektrischer und elektronischer Systeme für Pkw. Für andere Straßenfahrzeuge wie Lkw oder Motorräder gilt nach wie vor die IEC 61508. Da die ISO 26262 aber auch eine Art „Best Practice" für die Entwicklung darstellt, steht einem Einsatz für andere Kraftfahrzeuge nichts im Wege. Das Geräte- und Produktsicherheitsgesetz schreibt aber nicht die Anwendung einer bestimmten Norm vor.

Anforderungen für sicheren Lifecycle

Insgesamt zehn Teile beschreiben die einzelnen Phasen des Sicherheitslebenszyklus der ISO 26262. Dadurch ist die Norm die Kombination eines Prozess- und eines Lebenszyklusmodells mit Anforderungen an die Hardware- und Softwarearchitektur. Die Anforderungen des Lebenszyklusmodells berühren etwa auch Themen wie die Sicherheit in der Prüf- und Wartungsphase des Automobils. Es gibt beispielsweise in fast allen Autos Airbags, deren Treibsätze unter das Sprengstoffgesetz fallen. Die ISO 26262 schreibt vor, dass sie am Ende ihres Lebenszyklus sicher zu entsorgen sind.

Die zukünftige ISO 26262 fordert explizit die Einführung eines Sicherheitsprozesses und stellt Anforderungen an die Entwicklungsprozesse. Dabei geht es nicht nur um die reine Entwicklungstätigkeit, vielmehr werden auch klare Anforderungen an die Organisation gestellt.

Erfahrungsgemäß lassen sich viele Anforderungen der Norm durch einen ausgereiften Entwicklungsprozess abdecken. Da es aber immer noch viele Organisationen gibt, die zwar Automobilelektronik entwickeln, sich jedoch im Bereich Prozesse schwertun, ist ein integrierter Ansatz zu empfehlen. „Unreife" Organisationen werden Probleme haben, die Anforderungen der ISO 26262 umzusetzen, da die Basis, also reife Entwicklungsprozesse, nicht gegeben ist. Den Mehraufwand zur Einführung der Norm schätzen Experten auf 10 bis 50 Prozent des gesamten Entwicklungsaufwands. Der Mehraufwand, um einen Entwicklungsprozess nachträglich nach der ISO 26262 zu qualifizieren, wird wahrscheinlich die 50-Prozent-Marke noch übertreffen. Dabei ist festzuhalten, dass eine Norm nur das absolut notwendige Vorgehen abdecken kann. Ihre Vorschriften stellen lediglich die Minimalanforderungen an den Prozess und die Organisation dar.

Auf der sicheren Seite

Bei Unfällen mit Personenschaden, die womöglich auf eine Fehlfunktion zurückgehen, wird fast immer ein Gutachter hinzugezogen. Er prüft nicht etwa die Details des Entwicklungsprozesses, sondern betrachtet nur, welche Faktoren die funktionale Sicherheit gewährleisten sollen. Dabei verlässt sich der Gutachter hauptsächlich auf die vorhandenen Normen. Sollten sie bei der Entwicklung nicht oder nur teilweise eingehalten worden sein, besteht der Tatbestand der Fahrlässigkeit. Das bedeutet nicht nur für die Firma, sondern auch für die einzelnen Beteiligten empfindliche zivil- und strafrechtliche Folgen. Das gilt für Entwickler genauso wie für den Projektmanager und den Geschäftsführer.

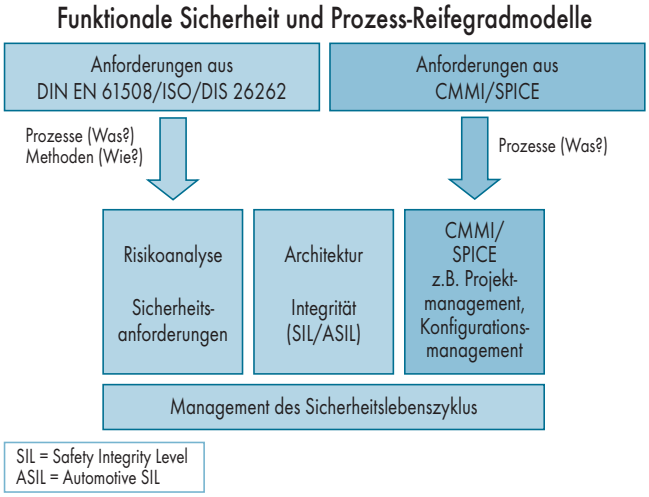
Selbst Managerhaftpflichtversicherungen schützen nicht, da ein fehlendes Umsetzen der Sicherheitsnormen als Vorsatz oder grobe Fahrlässigkeit gewertet wird. Es wäre sogar möglich, dass sich der Richter in einem Gerichtsverfahren auf die vorhandene DIS-Version (Draft International Standard) bezieht. Die rechtliche Klärung durch einen Präzedenzfall oder ein Gerichtsurteil, ob bereits eine DIS-Version Verpflichtungen für die Organisation enthalten kann, steht noch aus.

Da die ISO 26262 bereits seit Sommer 2009 als Draft-Ausgabe vorliegt, ist es für alle Firmen, die Automobilelektronik entwickeln, höchste Zeit, sich mit dem Thema zu befassen. Die aktuelle Version enthält fast alle kommenden Anforderungen und bietet eine solide Grundlage für die Einführung der neuen Norm. Zur Erinnerung: Sie gilt für alle ab ihrer Veröffentlichung verkauften Produkte. Das kann bedeuten, dass bereits entwickelte und immer noch verkaufte Produkte an die neuen Anforderungen anzupassen sind.

Als ersten Schritt sollten Organisationen einen Manager für funktionale Sicherheit ernennen. Da die fachlichen Anforderungen an die neue Position anspruchsvoll sind, wäre auf Qualifikation und Erfahrung besonderer Wert zu legen. Der Manager für funktionale Sicherheit muss unabhängig von den Entwicklungs- und Produktionsabteilungen die Einführung der Norm vorantreiben und für die Organisation einen Plan erstellen, mit dem sich deren Anforderungen in den Projekten umsetzen lassen. Die Weiterbildung und Sensibilisierung der Mitarbeiter spielt dabei eine entscheidende Rolle, da die Norm die Organisation und nicht einzelne Mitarbeiter betrifft.

Der nächste Schritt wäre das Erstellen eines firmenspezifischen Funktionssicherheitsprozesses, den man kontinuierlich anpassen und verbessern muss. Die ersten Aktivitäten zur Absicherung der Projekte nach ISO 26262 müssen bereits vor der Entwicklung während der Angebotsphase erfolgen, zum Beispiel die Schätzung der Aufwände für sicherheitsrelevante Funktionen.

Daraufhin wären sowohl auf Organisationsebene als auch in den einzelnen Projek-



Funktionale Sicherheit und Reifegradmodelle ergänzen sich.

ten Verantwortliche für funktionale Sicherheit zu benennen. In der Praxis erstellen die Projektbeteiligten in aller Regel einen Sicherheitsplan (Safety Plan), der das zentrale Dokument zum Management der funktionalen Sicherheit ist und die projektspezifischen Regelungen enthält, wie sich die funktionale Sicherheit erreichen lässt. Als Planungs- und Steuerungsinstrument dient er als zentrale Informationsdrehscheibe für alle Beteiligten. Der Sicherheitsplan ist meist eine Textdatei und enthält Verweise auf Dokumente zu spezifischen Planungsaspekten. Er soll gewährleisten, dass das gesamte Entwicklungssystem und das entwickelte Produkt die Anforderungen erfüllen.

Im Rahmen eines Projekts werden die Risiken durch eine Gefährdungs- und Risikoanalyse mit Automotive Safety Integrity Level (ASIL) eingestuft. Die Risiken nach IEC 61508 können aber höher ausfallen (Kernkraftwerk, Airbus A380) als bei einem Auto. Dadurch sind die in der ISO 26262 genannten ASIL feiner abgestuft als die SIL der IEC 61508.

Fazit

Im Mittelstand ist ein deutlicher Nachholbedarf in Sachen ISO 26262 festzustellen. Unwissenheit und Unsicherheit bei der Interpretation der Sicherheitsnormen sind weit verbreitet. Voraussetzungen für die effektive Umsetzung der Anforderungen sind angepasste Prozesse und qualifiziertes Personal. Die Schaffung der Voraussetzungen erfordert vom Hersteller und seinen Lieferanten Vorbereitungen, die rechtzeitig vor dem Start eines Entwicklungsprojekts mit sicherheitsbezogenen Anteilen zu planen sind. Notwendige Prozessanpassungen und die Einführung spezifischer Methoden und Verfahren sollten im Rahmen eines Programms zur Prozessverbesserung nach CMMI oder SPICE erfolgen. Funktionale Sicherheit und Reifegradmodelle haben einen hohen Überdeckungsgrad und ergänzen sich ideal (siehe Abbildung). (ane)

BERTRAM JANOSITZ

ist Mitarbeiter der KUGLER MAAG CIE GmbH und beschäftigt sich seit vielen Jahren mit den Themen Prozessverbesserung nach CMMI und Automotive SPICE sowie funktionaler Sicherheit.