Normen

ISO 26262: Das Wichtigste zur zweiten Auflage und zu SOTIF

29.10.2019 | Autor / Redakteur: Joseph Dailey, Jürgen Schlöffel / Sven Prawitz

Im ISO-26262-Standard fehlen bisher Details zur Entwicklung von automatisierten Fahrzeugen. Diese behandelt nun der neue Standard SOTIF (Safety of the Intended Functionality). Jürgen Schlöffel und Joseph Dailey von Mentor Graphics fassen die Neuerungen zusammen.

Automatisierte Fahrzeuge müssen sicher sein. Für die Entwicklung der Funktionen gibt es den ISO-Standard 26262, der nun erweitert wird.
(Bild: Daimler)

Die Norm ISO 26262 behandelt viele Aspekte der funktionalen Sicherheit für Pkw mit einem maximalen Gesamtgewicht von 3,5 Tonnen. Die Aktualisierung dieses Standards beinhaltet viele Upgrades und hebt die Gewichtsbeschränkung auf. Dadurch kann die ISO-Norm auf andere Straßenfahrzeuge wie schwerere Pkw, Lkw, Busse und Motorräder ausgedehnt werden. Diese zweite Auflage enthält insbesondere auch Richtlinien zur Anwendung von ISO 26262 auf Halbleiter.

Im ISO-26262-Standard fehlen noch Details zur Entwicklung von automatisierten

Fahrzeugen. Diese fehlende Funktionalität behandelt nun der neueste, auf den ISO 26262:2018 folgende Standard, ISO/PAS 21448, der allgemein als SOTIF (Safety of the Intended Functionality) bezeichnet wird. **Funktionale Sicherheit und SOTIF betreffen alle Teile der automobilen Lieferkette.** Die Design-Automation-Software muss beispielsweise die Qualität und Zuverlässigkeit der Komponenten im automobilen Umfeld berücksichtigen. ISO 26262 definiert die funktionalen Anforderungen an die Risikobewertung und das Vertrauen in den Einsatz solcher Software-Tools.

Was ist neu in der ISO 26262?

All dies ist in Abschnitt 11 der ISO 26262, Teil 8, beschrieben. Dieser verlangt für alle verwendeten Software-Werkzeuge, die für die Entwicklung, Fertigung und den Betrieb von E/E-Systemen im Fahrzeug verwendet werden, eine Qualifizierung dieser Werkzeuge. Dies wird bereits in der aktuellen Ausgabe des Standards beschrieben und gefordert.

Für Software-Tool-Anbieter gibt es einige wichtige Änderungen:

- Bei den PMHF- (Probabilistic Metric for Hardware Failure) Gleichungen und der Verifikation der Sicherheitsanalysen gab es Aktualisierungen.
- Das Vertrauen in die Verwendung von Softwarewerkzeugen beinhaltet die Validierung der Hersteller
- Neuer Abschnitt 11; Richtlinien zur Anwendung des ISO-26262-Standards auf Halbleiter

Der ISO-26262-Standard enthält bereits eine Reihe von Mindestanforderungen, um die funktionale Sicherheit zu erfüllen, er kann aber nicht alle Sicherheitsaspekte eines Produkts abdecken. **Der Systemlieferant muss sicherstellen, dass das Produkt die höchsten Sicherheits-, Zuverlässigkeits- und Leistungskriterien erfüllt.** Die Gewährleistung, dass die Softwarewerkzeuge die Sicherheitsbestimmungen einhalten, ist Teil dieses Prozesses. Aus der ISO-26262-Perspektive müssen Softwarewerkzeuge für die Entwicklung von Automobilsystemkomponenten qualifiziert sein, damit sie ihre Aufgabe in einer funktional sicheren Designumgebung erfüllen können. Der Nachweis erfolgt durch einen zertifizierten Qualifizierungsbericht.

Tool-Confidence-Level (TCL) definiert

Alle Anforderungen an die Klassifizierung und Qualifizierung von Softwarewerkzeugen sind in Teil 8 des ISO-26262-Standards beschrieben und festgelegt. Er definiert so genannte Tool-Confidence-Level (TCL1-3), die eine Klassifizierung der Vertrauensanforderungen ermöglichen. **TCL ist ein Maß für die Möglichkeit, dass die Software für einen Fehler in einer Komponente verantwortlich ist,** und für die Fähigkeit der Software, dieses Problem zu erkennen. TCL1 ist der höchste, TCL3 der niedrigste Level.

Für ein Softwarewerkzeug, das für die Entwicklung eines Automobilsystems eingesetzt wird, heißt es in einem Abschnitt des ISO 26262, dass: „das Risiko systematischer Fehler im entwickelten Produkt aufgrund von Fehlfunktionen des Softwarewerkzeugs, die zu fehlerhaften Ergebnissen führen, minimiert wird. Und dass der Entwicklungsprozess im Hinblick auf die Einhaltung des ISO-26262-Standards angemessen ist, wenn sich die vom ISO 26262 geforderten Aktivitäten oder Aufgaben auf die korrekte Funktion des verwendeten Softwaretools stützen."

Qualifizierungsmethode je nach ASIL

ISO 26262:2018 beschreibt vier Qualifizierungsmethoden zum Erreichen eines bestimmten Vertrauensniveaus. **Es sind jedoch nicht alle Methoden erforderlich:** Basierend auf dem angestrebten ASIL (Automotive Safety Integration Level) werden verschiedene Methoden empfohlen. Wenn die Komponente beispielsweise auf ASIL-A oder ASIL-B abzielt, sind die Methoden 1a und 1b „sehr empfehlenswert" (++) und die Methoden 1c und 1d „empfehlenswert" (+).

Die vier Methoden sind nur ein Teil des Prozesses zur Qualifizierung der verwendeten Software-Tools. Der Qualifizierungsbericht für Softwarewerkzeuge ist eine Zusammenfassung des Klassifizierungs- und Validierungsprozesses, der Ergebnisse, Empfehlungen, projektspezifischen Prozessmaßnahmen und detaillierter Informationen über den Einsatz der Werkzeuge. Die als TCL1 klassifizierten Softwareentwicklungswerkzeuge eignen sich für den Einsatz in ASIL-D-Komponenten.

Neue Anforderungen für Tier-2-Halbleiterlieferanten

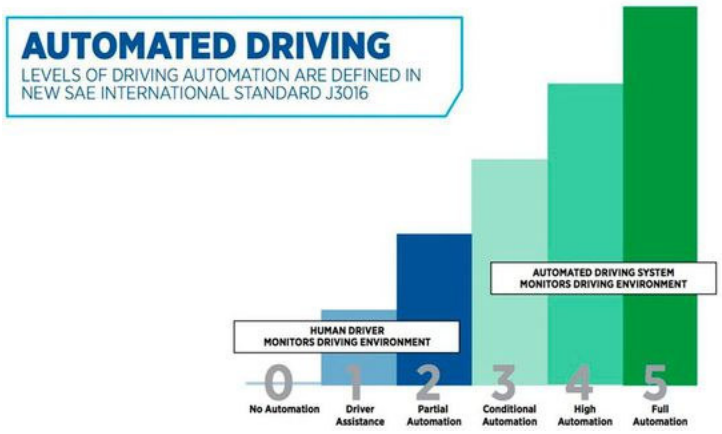
Die Tier-2-Halbleiterzulieferer für Automobilanwendungen werden mit vielen hohen Anforderungen ihrer OEMs und Tier-1-Unternehmen konfrontiert. Sie müssen den Nachweis erbringen, dass die Entwicklung integrierter Schaltungen und Systeme nach

geeigneten Design-, Verifikations- und Validierungsabläufen unter Verwendung qualifizierter Softwarewerkzeuge erfolgt. Der ISO-26262-Standard unterstützt dies durch die Beschreibung der Anforderungen an die Werkzeugqualifizierung.

Die 2018-Ausgabe wird ein neues Kapitel (Kapitel 11) mit Richtlinien zur Anwendung des ISO 26262 Standards auf Halbleiter enthalten. Das Kapitel enthält allgemeine Beschreibungen über Halbleiterbauelemente und deren Entwicklung sowie möglicher Partitionierungen. **Es geht dann auf einige wichtige Punkte im Zusammenhang mit ISO 26262 ein,** einschließlich den Abschnitten über Hardwaremängel, Fehler und Fehlermodi. Zudem befasst es sich mit geistigem Eigentum (Intellectual Property, IP), insbesondere mit ISO-26262-bezogener IP mit einer oder mehreren zugewiesenen Sicherheitsanforderungen.

SOTIF: Richtlinien für Automatisiertes Fahren

Im Jahr 2014 stellte die SAE International mit dem SAE-Standard J3016 eine gemeinsame Terminologie für automatisiertes Fahren <https://www.automobil-industrie.vogel.de/autonomes-fahren-definition-level-grundlagen-a-786184/> zur Verfügung. Der Standard beschreibt sechs Level des automatisierten Fahrens.



Die sechs SAE-Level für autonomes Fahren.
(Bild: SAE International)

Der ISO-26262-Standard ist nach wie vor die Grundlage für ein sicheres System, sichere Hardware und sichere Software, die im Fehlerfall einen unabhängigen und sicheren Betrieb ermöglichen. ISO 26262 führt modernste Prozesse und Architekturen ein und legt klare Regeln fest, die ein E/E-System sicher machen.

Der SOTIF-Standard befindet sich noch in der Entwicklung. Er enthält Richtlinien für automatisierte Fahrzeuge gemäß Level 0, 1 und 2. Selbst bei diesen Level der Autonomie müssen die weltweiten Experten für autonomes Fahren um die Definition kämpfen, wie sie ein System sicher machen. Wenn gewährleistet werden soll, dass ein automatisiertes Fahrzeug während des normalen Betriebs sicher funktioniert und handelt, gibt der SOTIF-Standard die Richtlinien vor.

Was der SOTIF-Standard beschreibt:

- Konzepte für eine autonome Architektur,
- wie SOTIF-Risiken bewertet werden, die sich von denen des ISO 26262 unterscheiden,
- wie Szenarien und auslösende Ereignisse identifiziert und bewertet werden,
- wie SOTIF-bezogene Risiken reduziert, verifiziert und validiert werden und
- welche Kriterien für die Freigabe eines autonomen Fahrzeugs erforderlich sind.

Die bezieht sich auf die Methodik für automatisiertes Fahren, aber jetzt kommt die Implementierung. Die Verifikation und Validierung automatisierter Fahrzeuge muss von der Simulation bis zum Gesamtfahrzeug viele Tests bestehen. Dazu zählen Faktoren, die die gesamte 4-D-Umgebung umfassen, einschließlich Wetter, Straßenzustand, umgebende Landschaft, Objekttextur und mögliche missbräuchliche Anwendung durch den Fahrer.

SOTIF bietet viele Methoden und Richtlinien zur Einbeziehung von Umweltszenarien für die Vorabanalyse des Konzepts und die endgültige Validierung. Das SOTIF-Komitee möchte den Anwender durch die Dokumentation der verschiedenen Szenarien, der Sicherheitsanalyse dieser Szenarien, der Überprüfung der Sicherheitssituationen und der auslösenden Ereignisse sowie der Validierung des Fahrzeugs für die Umwelt mit angewandten sicheren Systemen führen. Diese Faktoren sind ausschlaggebend, um dem kommenden Standard für automatisiertes Fahren zu entsprechen.

Vertrauen in Simulation und Testing wichtiger denn je

Diese Konzepte, Evaluierungen und Tests gehen weit über die bisherige Entwicklung hinaus. Vor diesem Hintergrund ist das Vertrauen in Testplattformen, Softwarewerkzeuge, die Simulation digitaler Zwillinge oder Hardware in the Loop wichtiger denn je. Bei der Entwicklung eines Systems zum autonomen Fahren müssen die Tier-1- und Tier-2-Automobil-IC-Zulieferer darauf vertrauen können, dass sie die beste Software für die Entwicklung verwenden.

Über die Autoren

Jürgen Schlöffel ist Program Manager im Bereich EDA und DFT bei Mentor Graphics Development in Hamburg. Sein derzeitiges Aufgabengebiet umfasst fortschrittliche Test-Techniken für integrierte Schaltungen, Designautomatisierung für DSM-Technologien und Automotive Test. Jürgen Schlöffel hat ein Diplom in Physik der Universität Göttingen. Bevor er 2008 als Engineering & Governmental Relations Manager zu Mentor Graphics kam, war er mehr als 20 Jahre lang in verschiedenen F&E-Positionen bei NXP und Philips Semiconductors tätig.

Joe Dailey ist Global Functional Safety Manager bei Mentor und hat über 25 Jahre Berufserfahrung. Er hat das Mentor-Safe-Programm ins Leben gerufen. Dieses konzentriert sich auf spezifische Aktivitäten im Bereich der funktionalen Sicherheit, darunter unterstützende Prozesse, Sicherheitsarchitekturen, Sicherheitsanalysen und Schulungen. Joe Dailey hat einen Master-Abschluss in Betriebswirtschaft der Arizona State University und einen Bachelor of Engineering in Elektrotechnik der Youngstown State University.