



© Siemens Digital Industries Software

Test, Zuverlässigkeit und Sicherheit für Automobil-ICs realisieren

# Zukunftssicheres Konzept: Safety Island

Um die Herausforderungen zu bewältigen, die durch Entwicklung und Einsatz von Elektronik im Fahrzeug entstehen, müssen nicht nur Lösungen auf dem Chip für Test und Zuverlässigkeit gefunden werden, sondern auch für die Implementierung von Sicherheits-IP-Blöcken und die Auswertung von Chip-Daten.

Lee Harrison

Der alte Ausspruch „May you live in interesting Times“ bedeutet zugleich Segen und Fluch – und die Hersteller von Halbleitern im Automotive-Bereich leben wahrlich in interessanten Zeiten. In diesem Fall jedoch stellt die Komplexität, also der Fluch, gleichermaßen ein Segen, nämlich einen Wettbewerbsvorteil dar, so lange man Herausforderungen wie Test, Zuverlässigkeit und Datensicherheit meistern kann. Tessent als Teil der Siemens Digital Industries Software bietet eine Lösung, um die neuen Anforderungen an ICs im Automobil-Bereich zu bewältigen: Tessent Safety Island.

## Herausforderungen an ICs im Automobilsektor

System-on-Chips (SoCs) für den Automotive-Bereich sind größer und komplexer als jemals zuvor und müssen konform zu Industrie-Standards wie der

ISO 26262 sein, was Auswirkungen auf die Hardware- und Software-Entwicklung hat. Um die funktionale Sicherheit im SoC und im System sicherzustellen, ist es wichtig, das richtige Maß an Übereinstimmung mit dem Standard zu verwirklichen. Diese Stufen werden als

Automotive Safety Integrity Level (ASIL) bezeichnet und reichen von A bis D. Wenn ein System für ASIL-Stufe D entwickelt wird, ist es möglich, dass unterschiedliche Blöcke auf dem IC auch unterschiedliche ASIL-Einstufungen besitzen. Daher ist es erforderlich,

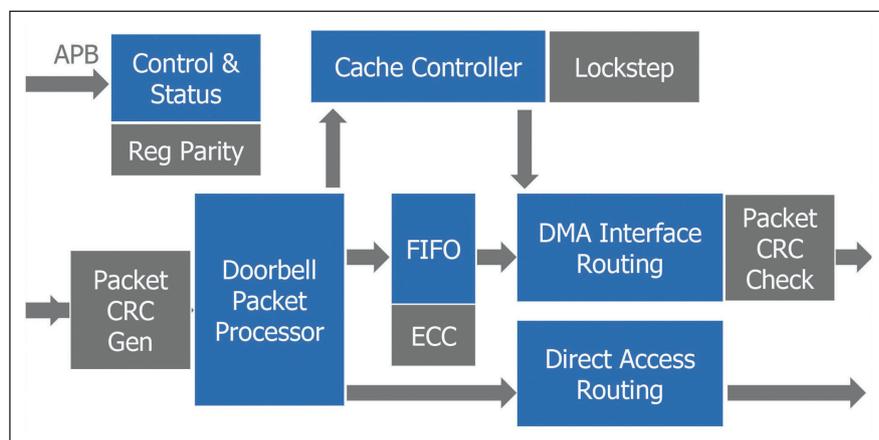


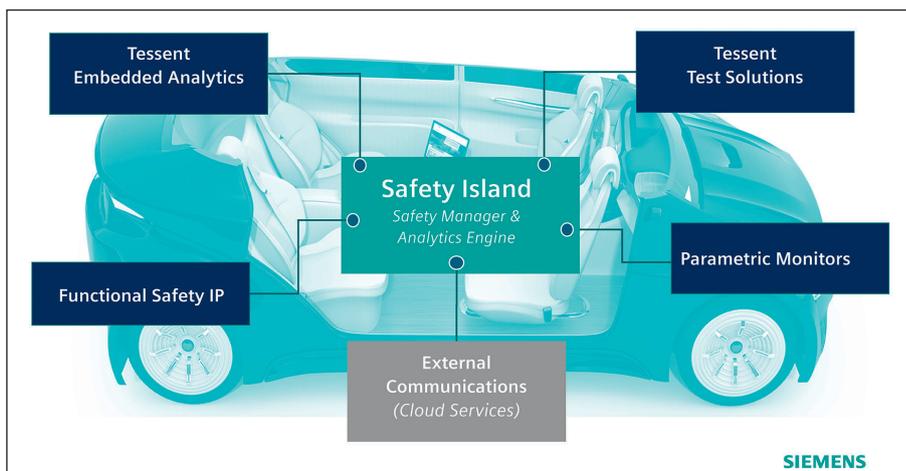
Bild 1: Typische Verteilung der funktionalen Sicherheit innerhalb eines Automobil-SoCs.

© Siemens Digital Industries Software

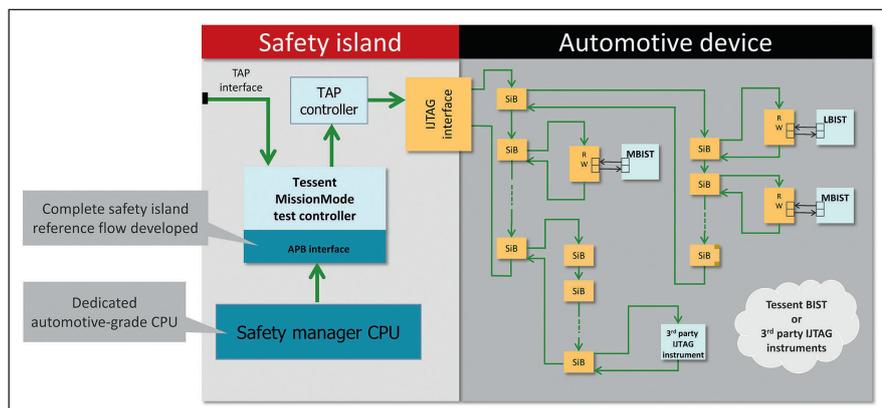
ein modulares Konzept für die Integration von Blöcken mit verschiedenen ASIL-Einstufungen zu verwirklichen.

In einem SoC mit IP-Blöcken unterschiedlicher Zuverlässigkeits-Stufen muss es eine Möglichkeit geben, die Bereiche für systeminterne Tests zu isolieren. **Bild 1** zeigt eine mögliche Verteilung von IP-Blöcken für die funktionale Sicherheit auf einem Automobil-SoC.

Gemeinsame Ressourcen, beispielsweise Speicher, müssen soweit wie möglich unabhängig sein zwischen den Bereichen, so dass Fehler in einem Be-



**Bild 3: Erweiterte Anschlussmöglichkeiten vom Safety Island** © Siemens Digital Industries Software



**Bild 2: Grundlegende Architektur vom Safety Island** © Siemens Digital Industries Software

reich keine Auswirkungen auf andere haben und somit nicht die ASIL-Gesamteinstufung reduzieren. Es bedarf einiger Anstrengungen, um Komponenten für Testzwecke und der funktionalen Sicherheit voneinander unabhängig zu machen. Aber wer trägt die Verantwortung? Welche Mechanismen werden die Fehler-Überwachung übernehmen, den Test organisieren und Probleme an das übergeordnete System weiterleiten? Das ist die Aufgabe vom Tessent Safety Island (**Bild 2**). Es stellt einen Mechanismus dar, durch den der Chip auf IP-Blöcke verschiedener ASIL-Einstufungen im SoC zugreifen, sie steuern und überwachen kann und Fehler an das externe System meldet. Beispielsweise einen Alarm auslösen, der dem Fahrer signalisiert, die Kontrolle zu übernehmen, sobald eine ADAS-Komponente versagt. Das Safety Island lässt sich konfigurieren und für zukünftige Anforderungen und Einsatzbereiche erweitern.

Die Zusammenführung sämtlicher systeminterner Teststrukturen für die funktionale Sicherheit ist denkbar einfach bei Verwendung des Tessent MissionMode Controllers, der einen

zentralen Zugriffspunkt für die Kontrolle darstellt. Der Controller ist dabei lediglich der Mechanismus, der die Konfiguration und Ablaufsteuerung der unterschiedlichen Tests ermöglicht und deren Ergebnisse abrufen. Durch die Kombination mit einer CPU für Sicherheitsaufgaben kann er zu einem eigenen Safety Island werden, verbunden durch eine AMBA APB-Schnittstelle als Teil des IPs.

**Verwendung über den Test hinaus**

Der durch spezifische Sicherheitsmechanismen gesteuerte Test im Automobil-Bereich, zum Beispiel BIST, ist nur ein Teil der Anforderungen an ICs aus dem Automobil-Sektor. Sobald ein Safety Island implementiert wurde, kann dessen Nutzung erweitert werden. Durch die IJTAG-Schnittstelle und zusätzliche Bus-Verbindungen ist es möglich, auch eine Reihe anderer IP-Blöcke anzubinden, die für die Verbesserung der funktionalen Sicherheit des ICs verwendet werden können. **Bild 3** veranschaulicht die erweiterten Anschlussmöglichkeiten des Safety Island. Die Überwachung und Ansteuerung

von BIST-Strukturen zum Test auf strukturelle Defekte kann einfacherweise über die IJTAG-Infrastruktur erfolgen, die zusammen mit den BIST-IP-Blöcken auf dem Chip implementiert wird. Die Aufgaben der funktionalen Sicherheit lassen sich durch den Einsatz von Embedded Analytics IP erweitern, das die Überwachung und Datenerhebung innerhalb der SoC-Strukturen ermöglicht. Die Embedded Analytics IP kann einen weiten Bereich der Aktivitäten auf dem Chip adressieren, darunter sogar Anforderungen durch die ISO 21434. IP-Blöcke für die funktionale Sicherheit können mit dem Safety Island verbunden, darüber angesteuert und überwacht werden. Die Überwachung von Parametern deckt Probleme auf, die durch Variation von Spannung, Temperatur und Prozessfaktoren entstehen und Einfluss auf Performance und/oder Zuverlässigkeit des Chips haben können. Die Daten, die über das Tessent Safety Island gesammelt werden, müssen offline analysiert werden. Deshalb ist es wichtig, über eine Auswahl an externen Anschlussmöglichkeiten zu verfügen. Das Safety Island ermöglicht eine Vorverarbeitung der Daten, um die effektive Nutzung von Bandbreite und Speicherbedarf sicherzustellen.

Siemens EDA bietet die Komponenten, um eine komplette und zukunftssichere Lösung für ein Safety Island zu erstellen, das on-chip IP-Blöcke für Test und funktionale Sicherheit ansteuert und Datenströme überwacht. ■ (eck)

[www.resources.sw.siemens.com](http://www.resources.sw.siemens.com)



**Lee Harrison** ist Manager für Automotive IC Test Solutions innerhalb der Tessent Gruppe von Siemens Digital Industries Software. © Siemens