Konform zur Norm

Automatisierte Fehleranalyse. Gerade kleinere und neu gegründete Unternehmen in der Automobilelektronik tun sich schwer, die Kosten und die Experten für den Zulassungsprozess aufzubringen. Hier hilft ein neues Verfahren, das automatisiert die Sicherheitsmetriken nach ISO 26262 bestimmt.

Automotive-ICs bilden das Rückgrat von Fahrerassistenzsystemen und vernetzten autonomen Fahrzeugen. Da ein Fehler gefährliche Folgen haben kann, müssen sie überaus zuverlässig und langlebig sein. Fehlfunktionen lassen sich aber nicht gänzlich vermeiden. Physikalische Phänomene wie die Elektromigration können Kurzschlüsse hervorrufen oder einen Stromkreis unterbrechen und den Chip dauerhaft beschädigen. Treffen außerdem Alphateilchen aus der kosmischen Strahlung auf eine Schaltung, verändern sie unter Umständen den Inhalt eines Speichers.

Heute sind Automotive-ICs um Einiges komplexer als noch vor einigen Jahren. Selbst in Mittelklassefahrzeugen findet man heute Features, die weit über das automatische Beschleunigen und Bremsen hinausgehen, beispielsweise automatische Lenkfunktionen im aktiven Spurhalteassistenten. Außerdem sind Transistoren kleiner geworden und die Schaltungen sehr viel stromsparender, wodurch eine geringere Energie ausreicht, um den Zustand eines IC zu verfälschen. Eine vermehrte Anfälligkeit ist die Folge.

Um Fehler zu vermeiden oder zumindest unter Kontrolle zu bringen, enthalten moderne Chips eine Vielzahl zusätzlicher Funktionen, die als Sicherheitsmechanismen (Safety Mechanisms, SMs) bezeichnet werden. Beim Schutz von Speichern kommen typischerweise ECC-Module (Error-Correcting Code) für SECDED (Single-Error Correction and Double-Error Detection) oder sogar DECTED (Double-Error Correction and Triple-Error Detection) zum Einsatz.

FAZIT

Kosten und Entwicklungsaufwand verringern. Die Berechnung der Sicherheitsmetriken nach ISO 26262 stützt sich selbst bei großen SoC oftmals auf aufwändige und fehleranfällige manuelle Analysen und auf rechen- und entwicklungsintensiven Fehlersimulationen. Renesas und OneSpin stellen in einem auf der DVCon Europe 2019 präsentierten Fachbeitrag ein alternatives, skalierbares Konzept für die Fehleranalyse von Automotive-Designs vor. Große SoCs lassen sich mit geringem Aufwand seitens des Anwenders in logische Abschnitte untergliedern. Die Fehlerklassifizierung ergibt vorläufige Schätzwerte für jeden Unterabschnitt. Reichen die konservativen Schätzungen nicht aus, um die Sicherheitsvorgaben einzuhalten, kann die Fehlerklassifizierung selektiv präzisiert werden. Dabei werden sichere, Rest- und latente Fehler identifiziert.

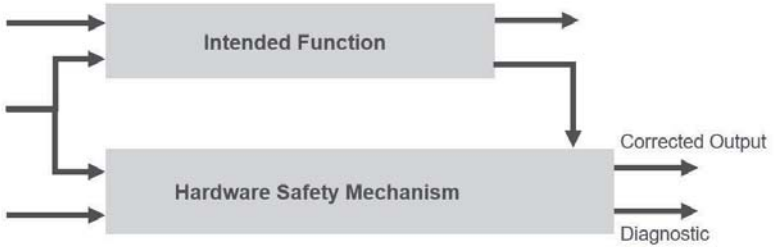
Sicherheit messbar machen

Die Functional-Safety-Norm ISO 26262 für elektronische Systeme in Kraftfahrzeugen definiert wichtige Metriken und Zielvorgaben für vier Sicherheitsstufen (Automotive Safety Integrity Levels, ASILs): ASIL A, ASIL B, ASIL C und ASIL D. Für die Steuerung der Rückleuchten muss ein IC einen weniger strikten Level erfüllen als für eine Lenkungssteuerung. Um eine Zulassung zu bekommen, müssen Entwickler SMs implementieren und Nachweise gemäß dem angestrebten ASIL vorlegen.

Die wichtigsten ISO-26262-Metriken sind SPFM (Single-Point Fault Metric), LFM (Latent Fault Metric) und PMHF (Probabilistic Metric for Random Hardware Failures). Da Single-Point- oder Restfehler gegen die Sicherheitsvorgaben verstoßen, müssen SMs ihre Zahl verringern, um den vorgegebenen SPFM-Wert zu erreichen. Latente Fehler, auch Multi-Point-Faults genannt, verletzen hingegen für sich allein nicht die Richtlinien, sie tun es aber eventuell, sobald ein zweiter Fehler auftritt. Ein fehlerhafter SM beispielsweise wirkt sich zunächst nicht auf die Funktion aus. Bleibt dadurch aber ein darauffolgender Fehler unentdeckt, kann dies zu einer gefährlichen Fehlfunktion führen. Es sei darauf hingewiesen, dass Fehler in SMs auch Restfehler sein können. Das hier dargestellte Szenario ist relativ unwahrscheinlich, andernfalls würde der SM die Sicherheitsmetriken verschlechtern anstatt verbessern.

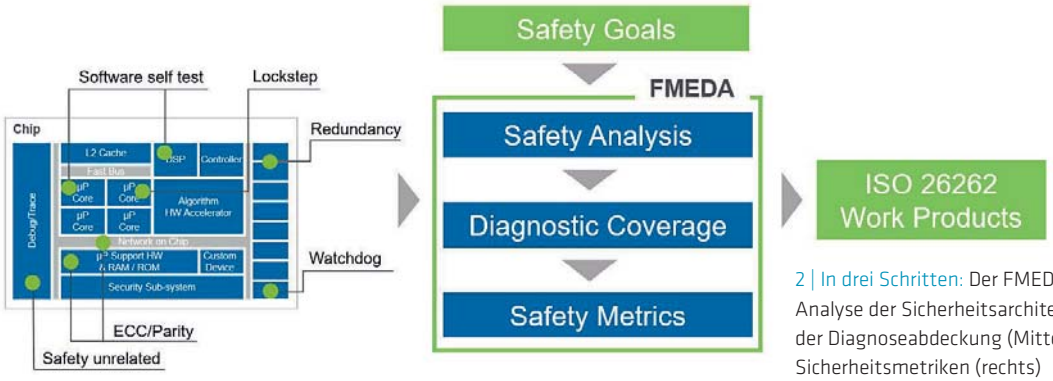
KONTAKT

OneSpin Solutions GmbH,
Nymphenburger Straße 20a,
80335 München,
Tel. 089 99013-0,
E-Mail info@onespin.com,
www.onespin.com



1 | Prüfen, melden, korrigieren: Sicherheitsmechanismen bewachen die Ein- und Ausgänge von Funktionsblöcken und generieren Diagnoseinformationen sowie korrigierte Signale

Bild: OneSpin Solutions



2 | In drei Schritten: Der FMEDA-Prozess besteht aus der Analyse der Sicherheitsarchitektur (links), der Bestimmung der Diagnoseabdeckung (Mitte) und der Berechnung der Sicherheitsmetriken (rechts)

FMEDA-Abläufe (Failure Modes, Effects and Diagnostic Analysis, siehe **Wissenskasten**) stützen sich im schlechtesten Fall auf eine fehlerträchtige und arbeitsaufwändige Analyse der Sicherheitsarchitektur. Oft bedienen sich Verifikations- und Sicherheitsingenieure einer umfangreichen Fehlersimulation, um die Sicherheitsmetriken zu bestimmen. Diese Methode weist jedoch drei entscheidende Mängel auf:

1. Sie kann nur Stimulus-abhängige Metriken liefern, was die Gültigkeit der Ergebnisse in Zweifel zieht – insbesondere im Fall von sogenannten Safety Elements out of Context (SEooCs),
2. Die Simulation erfordert erhebliche Rechenressourcen,
3. Es entsteht ein hoher Entwicklungsaufwand bei der Einstellung der Simulation, der Analyse von Resultaten und bei der Verbesserung der Stimulusqualität.

Die Fehlerklassifizierung auf der Basis formaler Methoden ist hingegen rigoroser und kommt ohne Stimuli aus, kann allerdings mit Komplexitätsproblemen behaftet sein, die ihre Praxistauglichkeit einschränken.

Sicherheitsbewusste Hardwarepartitionierung

In einem von Renesas Electronics und OneSpin Solutions gemeinsam auf der DVCon Europe 2019 präsentierten Fachbeitrag mit dem Titel ‚ISO 26262: Fault Analysis in Safety Mechanisms' stellen die Autoren einen automatisierten, effizienten und skalierbaren FMEDA-Prozess für digitale Schaltungen vor. Demonstriert wird dieser Prozess an zwei ECC-geschützten FIFO-Modulen, wie sie häufig in FPGA- und ASIC-Systemen vorkommen.

Im ersten Schritt der Sicherheitsanalyse automatisiert die FCA-App (Fault Contribution Analysis) den sicherheitsorientierten Hardware-Partitionierungsprozess. Die Ausfallarten werden jeweils Unterabschnitten des Designs zugeordnet, die etwa durch geschützte oder Diagnoseausgänge von SMs abgegrenzt werden (**Bild 1**). Die Unterabschnitte lassen sich in zwei Kategorien einteilen: aktiv, wenn die Fehler zu den Ausgängen der beabsichtigten Funktion (Beobachtungspunkte) durchschlagen können oder passiv, wenn die Fehler nur bis zu den Diagnoseausgängen des SM (Diagnosepunkte) gelangen können. Aus den Unterabschnitten leitet man die Fehlerlisten und Attribute, zum Beispiel die geschätzte Halbleiterfläche, ab und nutzt diese anschließend für die Fehleranalyse und nachfolgende Schritte. Hervorzuheben ist, dass sich diese Methode der Sicherheitsanalyse anders als bei der Fehlersimulation und der herkömmlichen formalen Technik auf große und komplexe Bauelemente skalieren lässt.

Die Hardwarepartitionierung ergibt umgehend konservative Schätzwerte für die Sicherheitsmetriken. Für bestimmte Unterabschnitte können auch die Fehlersimulation oder die formale Analyse eingesetzt werden, sofern die geschätzten Ergebnisse nicht dem angestrebten ASIL entsprechen. Die FPA-App (Fault Propagation Analysis) und die FDA-App (Fault Detection Analysis) automatisieren diesen zusätzlichen Schritt, was letztendlich die Einschränkungen der geschätzten Metriken reduziert. Die FPA-App identifiziert sichere Fehler, die das Sicherheitsziel nicht gefährden, da sie nicht bis an sicherheitskritische Ausgänge durchschlagen. Die FDA-App zeigt Fehler auf, die ein SM in jedem Fall erkennen und anzeigen muss.

Die Ergebnisse der Fehleranalyse für die Unterabschnitte lassen sich schließlich kombinieren, um Sicherheitsmetriken für das gesamte SoC zu erhalten. Auch dieser Schritt läuft automatisch ab, nämlich mit der HMC-App (Hardware Metrics Computation). mey

Autoren
Jörg Grosse ist Product Manager für Functional Safety und Sergio Marchese ist Technical Marketing Manager, beide bei OneSpin Solutions.

Online-Service
Weitere Infos zur FMEDA-Lösung von OneSpin

www.elektronik-informationen.de/90072

WISSENSWERT

Ablauf der Fehleranalyse. Als FMEDA (Failure Modes, Effects and Diagnostic Analysis) bezeichnet man einen etablierten, systematischen Prozess, der eine quantitative Analyse der Ausfallarten und Diagnosefähigkeiten eines IC ermöglicht (**Bild 2**). Schon bei ASIL B stellt dies eine zeitraubende und teure Aufgabe dar. Der FMEDA-Prozess gliedert sich in drei Schritte:

1. Safety-Architektur des IC validieren und Hardwarefunktionen sowie Fehler entsprechend den Ausfallarten partitionieren,
2. Diagnoseabdeckung bestimmen– sie beschreibt die Fähigkeit der Sicherheitsmechanismen, Verletzungen der Sicherheitsvorgaben zu verhindern,
3. Sicherheitsmetriken berechnen.

Bild: OneSpin Solutions