ASIL-konforme Safety-IPs

Um Entwickler dabei zu unterstützen, die Zertifizierung der SoC-Funktionssicherheit schneller zu erreichen, sollten IP-Lieferanten einen Best-Practice-Ansatz zum Erreichen funktionaler Sicherheit bereitstellen, um ISO-26262-konforme Prozessor-IP zu entwickeln. Ferner muss eine begleitende Dokumentation der Verfahren zur Verfügung gestellt werden, nach denen die ASIL-D-Anforderungen erfüllt werden können.

© Synopsys

Funktionale Sicherheit wurde angesichts der Tatsache, dass immer mehr SoCs in sicherheitskritischen Anwendungen eingesetzt werden, zu einem kritischen Gesichtspunkt in der Systemarchitektur und in Verifikationsmethoden. Funktionssicherheitsstandards, im Besonderen ISO 26262, assistieren Projektteams bei der Bewältigung dieser Herausforderung. Einsatzfertige Safety-IP, ASIL-bereite Dokumentation und moderne Verifikations-Tools sind ebenso verfügbar, um Designteams dabei zu unterstützen, Konformität mit den wesentlichen Standards sowie die SoC-Zertifizierung zu erreichen.

Während der Entwicklung von Prozessor-IPs haben Entwicklungsteams keine Kenntnis über das spätere Einsatzfeld der IP, sodass sie die IP unter Anwendung der Richtlinien für ein „Safety-Element-out-of-Context" (SEooC) entwerfen müssen. Wenn das Endsystem für die IP unbekannt ist, muss das Designteam bei der Ableitung der Sicherheitsziele zur Erfüllung von ISO 26262 Annahmen treffen und dokumentieren und dabei die wesentlichen Prozessorelemente berücksichtigen. Diese Annahmen werden zusammen mit dem Kunden validiert, wobei beide Sicherheitsmanager die Entwicklungsvereinbarung unterzeichnen.

Fehlermodelle

ISO 26262 klassifiziert Fehler entweder als Hardware- oder Software-Fehler. Es definiert einen Fehler als einen abnormen Zustand, welcher ein Fehlverhalten erzeugen kann, was zu verstehen ist als die Unfähigkeit, eine Funktion wie gefordert auszuführen. Fehler sollten überwacht und in einem "Failure-Modes-, Effects- und Diagnostic-Analysis"-(FMEDA)-Bericht dokumentiert werden, der für die Zertifizierung erforderlich ist.

Während Software-Fehler immer systematisch sind, können Hardware-Fehler systematischer oder zufälliger Natur sein. Systematische Fehler lassen sich durch Verarbeitungs- oder Entwurfsmaßnahmen vermeiden. Zufällige Fehler wie beispielsweise Unterbrechungen aufgrund von Oxidation sind hingegen nicht vorhersagbar.

Die Anforderungen an ISO-26262-konforme Prozessor-IPs umfassen sowohl den Entwurfs- als auch den Verifikationsprozess:

ISO-26262-konformer Entwurf

Das Entscheidende beim Entwurf für ISO-26262-Konformität ist, spezifische Funktionen zu integrieren, mit denen sich zufällige und systematische Fehler erkennen und korrigieren lassen. Hierzu gehören typischerweise ein geschickter Speicherschutz zur Erkennung und Korrektur von Fehlern in Instruktionen und Daten im Core, Timer zur Prüfung auf Timing-Probleme und Stuck-At-Fehler, sowie zusätzliche Funktionen zur Erkennung systematischer Fehler im

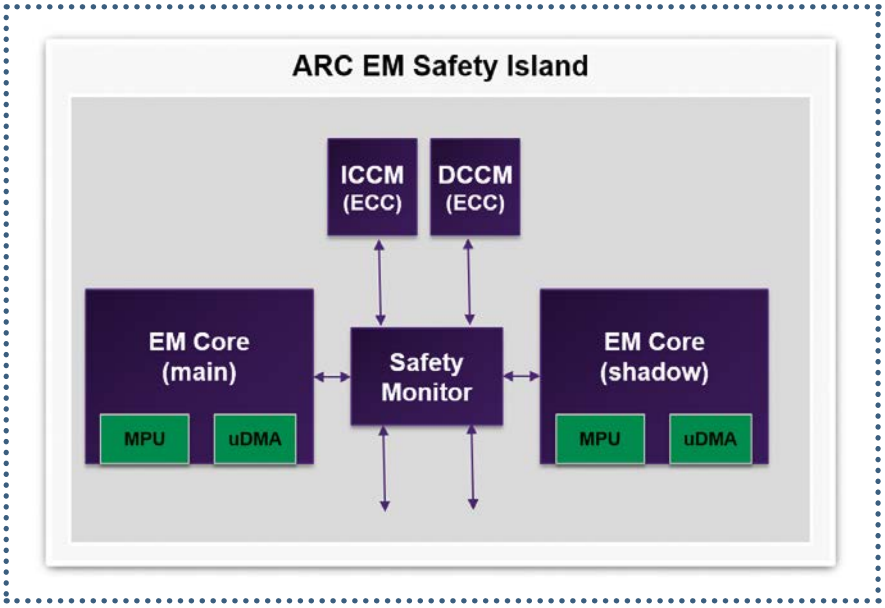

Bild 1: ARC-EM-Safety-Island – Examplarische Dual-Core-Lockstep-Prozessor-Lösung. (© Synopsys)

Core. Chip-Architekturen können Komponenten, die kritische Funktionen haben, auch in redundanter Ausführung enthalten, um ein zusätzliches Maß an Sicherheit zu erzielen. Im Hinblick auf die ASIL-D-Zertifizierung beispielsweise werden Prozessoren üblicherweise in einem Lockstep-Modus mit einem Safety-Monitor betrieben, um zu verifizieren, dass sich Fehler nicht bis auf die Systemebene ausbreiten.

ISO-26262-konforme Verifikation

Verifikation ist ein wesentlicher Schritt, um Prozessor-IP für ISO-26262-Konformität vorzubereiten. Sicherheitskritische Systeme erfordern zur Verifikation mehr Zeit und Expertise als Consumer-IP, weil Verifikationsingenieure sowohl die Fehlertoleranz des Designs durch Injektion zufälliger Fehler prüfen als auch dessen Funktionalität validieren müssen.

Das Verifikationsteam muss sowohl die funktionale als auch die Code-Abdeckung ermitteln, um die sicherheitssteigernden Funktionen zu verifizieren. Dies erfordert den Einsatz von Tools zur funktionalen Qualifizierung innerhalb des Verifikationsflows sowie die Verwendung einer Testbench, die zufällige Fehler implementieren kann. Die Nutzung von Stuck-At-Fault-Tests kann die Bestimmung des Fehlerbildes und der diagnostischen Abdeckung unterstützen. Diese Information geht in den FMEDA-Bericht ein, welcher nötig ist, um die ASIL-A- bis ASIL-D-Zertifizierung zu erhalten.

Entwicklung einer Sicherheitskultur

Die Etablierung sicherheitsorientierter Entwurfs- und Verifikationsflows ist von grundlegender Bedeutung für die ISO-26262-Konformität, aber der Standard formuliert auch gewisse Erwartungen an eine Sicherheitskultur innerhalb der Organisation. Beispielsweise sollte ein Unternehmen funktionale Sicherheit als ein Unternehmensziel definieren und firmenspezifische Strategien und Prozesse etablieren, zum Beispiel wie es beabsichtigt, die gegenwärtigen Praktiken kontinuierlich zu verbessern.

Beispiel: DesignWare-ARC-EM-Prozessor-IP

Die DesignWare-ARC-EM-Safety-Islands sind das Resultat von Synopsys' Plan, höchst effiziente IPs für den Einsatz in ISO-26262-sicherheitskonformen Automotive-Anwendungen bereitzustellen. Die Lösung kombiniert leistungseffiziente und kompakte, im Lockstep-Modus laufende Prozessoren mit integrierten Hardware-Sicherheitsfunktionen mit einem integrierten selbsttestenden Safety-Monitor. Die EM-Safety-Islands sind ASIL-D-zertifiziert und beinhalten umfassende Verifikation und Dokumentation, um die SoC-ISO- »

26262-Zertifizierung zu vereinfachen und zu beschleunigen.

Synopsys hat auch eine mit Automotive-Sicherheitsanforderungen konforme Organisationsstruktur, wozu auch die Benennung von Projekt-Sicherheitsmanagern gehört, und verwendet seine eigene, sicherheitsorientierte Verifikationsmethodik einschließlich des Certitude-Systems zur funktionalen Qualifizierung.

Die EM-Prozessoren innerhalb der Safety-Islands basieren auf der ARCv2-Befehlssatzarchitektur und sind auf Automotive-Sicherheitsanwendungen ausgerichtet. Entwickler können den Core konfigurieren, um jene Instanzen zu implementieren, welche die optimale Kombination aus Rechenleistung, Chipfläche, Leistungsaufnahme und Codedichte für ihre spezifische Anwendung bieten. Die erweiterbare ARC-Architektur ermöglicht die Integration eigener Instruktionen oder Hardware-Beschleunigern, um die Rechenleistung und die Leistungsaufnahme weiter zu verbessern.

Das ARC-MetaWare-Development-Toolkit für Safety und die Safety-Dokumentation ermöglichen Entwicklern sicherheitskritischer Systeme, die Anforderungen des ISO-26262-Standards zu erfüllen. Das Toolkit beinhaltet einen ASIL-D-zertifizierten Compiler und ist eine Lösung für die Entwicklung, das Debugging und die Optimierung eingebetteter Software für ARC-Prozessoren. Die begleitenden Unterlagen, darunter ein Handbuch und eine Anleitung, vereinfachen die Vorbereitung der Dokumente für den ISO-26262-Konformitätstest.

Die ARC-EM-Safety-Islands implementieren Sicherheitsfunktionen, die für die Einhaltung des ISO-26262-Standards essenziell sind. Der Standard verlangt ein Höchstmaß an Sicherheitsintegrität.

Fehlererkennung

Die ARC-EM-Prozessoren unterstützen zwei Fehlerbehandlungstechniken: Fehlerkorrigierenden Code (ECC) und Paritätsprüfung.

ECC wird eingesetzt zur Erkennung und Korrektur von Fehlern in Speichern, die durch Single-Event-Upsets (SEUs) wie beispielsweise einem Aufprall von Neutronen oder Alpha-Teilchen verursacht werden. Die ECC-Hardware unterstützt die Einzelfehlerkorrektur und Zweifachfehlererkennung für die eng gekoppelten Speicher und Caches. Sie erkennt Einzelbit-Fehler im Instruktionscode und korrigiert Datenzugriffe. Zweifachfehler werden als nicht korrigierbar angesehen und führen zu Exceptions. Die Parity-Hardware bietet Einzelfehlererkennung bei Speichern, wobei gerade und ungerade Parität unterstützt wird. Werden Fehler im Instruktionscode und bei Datenzugriffen erkannt, so findet keine Korrektur statt, jedoch werden stets Exceptions ausgelöst.

Watchdog-Timer

Der Watchdog-Timer dient zur Überwachung und Erkennung von Hard- und Software-Deadlock-Zuständen. Im Falle eines Deadlocks kann entweder ein System-Timeout/-Reset oder ein Interrupt ausgelöst werden, um einen Wiederherstellungsprozess anzustoßen.

Lockstep-Interface und Safety-Monitor

Das Lockstep-Interface dient zur Implementierung der Dual-Core-Lockstep-Architektur. Das Interface macht relevante Signale sichtbar, die den internen Prozessorzustand repräsentieren. In einer Lockstep-Architektur werden zwei identische Prozessoren instanziiert. Die beiden Prozessoren werden beim Systemstart in den gleichen Zustand gebracht und an ihren externen Schnittstellen mit den gleichen Eingangswerten versorgt. Während des Normalbetriebs wird erwartet, dass sich die beiden Prozessoren stets im gleichen Zustand befinden. Ein Safety-Monitor verbindet die zwei Prozessor-Cores in einem effektiven Lockstep, vergleicht die Ausgangswerte beider Prozessoren und meldet einen Fehler im Falle unterschiedlicher Ausgangswerte. Das Fehlersignal kann genutzt werden, um den Mikroprozessor zurückzusetzen oder zu unterbrechen, oder aber um das externe Subsystem über die Fehlersituation zu informieren. Der Safety-Monitor besitzt auch die Fähigkeit zur Time-Diversity. Hierbei verzögern Lockstep-Flip-Flops die Ein- und Ausgangsdaten beider Prozessoren um n Taktzyklen. Dies ist hilfreich, um die potenziellen Auswirkungen zu reduzieren, wenn ein Störimpuls beide Cores gleichzeitig treffen sollte. Die Time-Diversity-Buffer beinhalten ferner eine Paritätsprüfung, um Single-Point-Failures zu verringern.

Fazit

Um die Markteinführung ISO-26262-zertifizierter IP und SoCs zu beschleunigen, müssen Projektteams die Anforderungen so früh wie möglich im Entwurfsprozess berücksichtigen, idealerweise bereits während der Architektur-Definition. Die Sicherheitsfunktionalität sollte im Hinblick auf den anvisierten Markt und die Erfordernisse des ASIL-Levels identifiziert werden. Letztlich ergeben sich daraus die benötigten Hardwarefunktionen der IP bzw. des SoC. Der Sicherheitsplanungsprozess sollte die angewandten Verifikationsmethoden berücksichtigen, um den angestrebten ASIL-Signoff zu erreichen, zum Beispiel Failure-Mode und Diagnostic-Coverage. Der Einsatz eines robusten Qualifizierungstools zur Fehlerermittlung im RTL-Code und die Realisierung eines Fehlerinjektionsflows für die Verifikation sind entscheidend zum Erreichen der ASIL- und ISO-26262-Hardware-Zertifizierung.

Zu guter Letzt, und dies ist am wichtigsten, ist es notwendig, dass das Projektteam und das gesamte Unternehmen eine Kultur der funktionalen Sicherheit pflegt. Sicherheit muss zu einem Schlüsselaspekt in jedem sicherheitskritischen Entwurfs- und Verifikationsprojekt werden. ■ (oe)

» **www.synopsys.com**

» **www.hanser-automotive.de/3767813**

Hier finden Sie die Download-Version des Beitrags.

Angela Raucher ist Product-Line-Manager für ARC-EM-Prozessoren bei Synopsys.

Fergus Casey ist Senior-R&D-Manager für ARC-Prozessoren bei Synopsys.