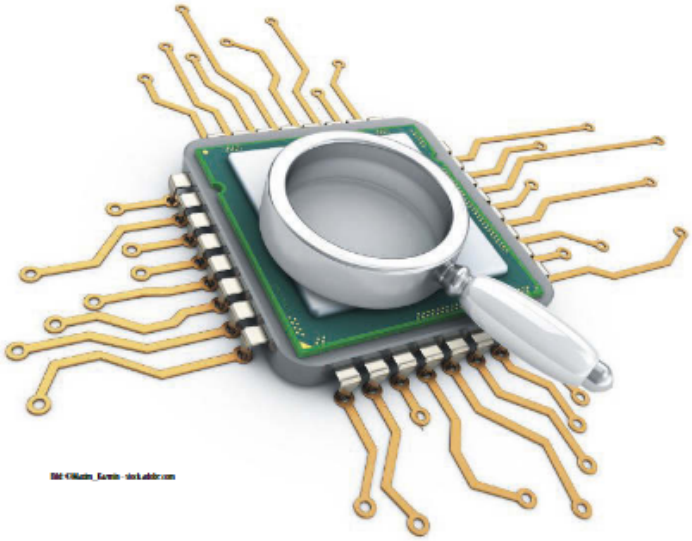
Safety, Security und Trust

Sicherstellung der Integrität von RISC-V-Prozessorkernen mit unabhängiger Verifikationslösung

Die Offenheit der RISC-V-Instruction-Set-Architektur und ihre mittlerweile weite Adaption machen eine gründliche Überprüfung der RISC-V-Kerne erforderlich. Im Beitrag beschreibt elektronik industrie eine Lösung zur Sicherstellung der Integrität von RISC-V-Implementierungen, die in Form von Apps ihre Anwendung für den Nutzer so einfach wie möglich gestaltet.

Autoren: Sven Beyer, Tom Anderson



Eines der am meisten diskutierten Themen in der Halbleiterindustrie ist heutzutage die RISC-V-Instruction-Set-Architecture (ISA). Auf vielen Konferenzen und in Fachartikeln wurde über RISC-V diskutiert und es ist noch lange kein Ende abzusehen. Auch wenn sich die RISC-V-Architektur noch in der Entwicklung befindet, leitet sie möglicherweise eine revolutionäre Änderung in der Intellectual Property (IP) und Halbleiterindustrie ein. Sie wird von der RISC-V-Foundation definiert als „freie und offene ISA, die durch die Zusammenarbeit mit offenem Standard eine neue Ära der Prozessorinnovation ermöglicht". Dadurch fordert sie etablierte Prozessorfamilien direkt heraus. Jeder kann RISC-V-Prozessorkerne entwickeln oder in System-on-Chip-Designs (SoC) integrieren. Die Stiftung unterstützt, standardisiert und entwickelt die RISC-V-ISA, ohne dass eine Lizenz erforderlich ist oder Lizenzgebühren erhoben werden.

Gründliche Überprüfung notwendig

RISC-V wurde ursprünglich in der EECS-Abteilung der University of California in Berkeley entwickelt. Die ISA wurde mit zahlreichen Konfigurationen und optionalen Erweiterungen wie der Unterstützung von IEEE 754-2008 Floating-Point und benutzerdefinierten Anweisungen entwickelt. Sie ist nicht auf bestimmte Technologien oder Mikroarchitekturen ausgerichtet, sodass eine Vielzahl von Implementierungen möglich ist. Tatsächlich sind jetzt mehrere Prozessorkerne und sogar ganze SoC-Projekte auf Open-Source-Sites verfügbar. Diese Offenheit und die weite Adaption machen eine gründliche Überprüfung der RISC-V-Kerne erforderlich. Bei traditionellen Prozessorfamilien gibt es nur ein oder zwei Anbieter, die bereits seit vielen Jahren Core und Chips anbieten. Von den Zulieferern wird erwartet, dass sie ihre Produkte überprüfen. Es ist daher ungewöhnlich, dass SoC-Designer die von ihnen lizenzierten Kerne erneut überprüfen wollen.

Im Gegensatz dazu gibt es bereits mehrere Parteien, die RISC-V-Kerne anbieten und diese Zahl wird in den nächsten Jahren erheblich zunehmen. Es gibt kein zentrales Team, das diese Kerne entwirft und überprüft. Für eine weitere Ausdehnung des RISC-V-Ökosystems benötigen die Kernanbieter eine unabhängige Verifikationslösung, um sicherzustellen, dass ihre Designs miteinander kompatibel sind und den ISA-Spezifikationen entsprechen.

Mehr als ein Funktionalitäts-Test

Um gegen die etablierten Prozessorfamilien mit ihrer jahrelangen umfassenden Validierung und Implementierung von Silizium erfolgreich zu bestehen, ist eine gründliche Verifikation unerlässlich. Ebenso müssen SoC-Entwickler sicherstellen, dass die von ihnen lizenzierten Kerne vollständig verifiziert und ISA-kompatibel sind. Die RISC-V-Foundation bietet zwar eine gewisse Compliance-Unterstützung, die aber nur eine Teillösung darstellt.

Die Sicherstellung der Integrität einer RISC-V-Implementierung geht weit über die Überprüfung der Funktionalität hinaus. Sowohl die Hauptanbieter als auch die Integratoren sehen sich Herausforderungen in Bezug auf Safety, Security und Trust gegenüber. Die Entwicklung vieler RISC-V-Kerne geschieht für Produkte mit

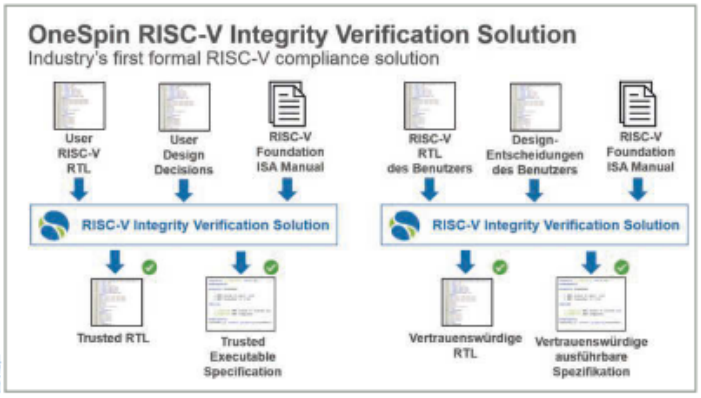


Bild: OneSpin

Die RISC-V Integrity Verification Solution stellt sicher, dass RISC-V-Cores Safety-, Security- und Trust-Anforderungen einhalten.

hohen Anforderungen an die funktionale Safety. Die Entwürfe müssen eine Safety-Logik enthalten, um zufällige Fehler im Feld zu behandeln, einschließlich Alpha-Teilchen, die Speicherbits umschalten. Normen, wie die ISO 26262 für die Automobilindustrie, erfordern die Überprüfung der Safety-Logik und die Berechnung der Ausfallwahrscheinlichkeit. Kernintegratoren werden darauf bestehen, dass ihre Lieferanten die strengen Anforderungen dieser Standards erfüllen, was auch dazu beiträgt, ihre SoCs und Endprodukte für Safety zu zertifizieren.

Darüber hinaus kommen viele RISC-V-Cores in Anwendungen zum Einsatz, die vor bösartigen Angriffen zu schützen sind. Core- und SoC-Designs müssen auf Sicherheitslücken analysiert werden, die es Angreifern ermöglichen könnten, die Kontrolle über das System zu übernehmen. Die Ausnutzung von Sicherheitslücken für autonome Fahrzeuge, Kernkraftwerke und Luft- und Raumfahrt könnte schwerwiegende Folgen haben. Angreifer können durch Hardware-Trojaner oder andere schädliche Logik Unterstützung finden, die von Mitarbeitern oder Tools im Entwurf von RTL bis Silizium in den Core (oder SoC) eingefügt werden. Der Prozess der Integritätssicherung muss solche Verletzungen von Trust absolut zuverlässig aufdecken.

Sicherheitslücken im Design aufdecken

All diese Herausforderungen führen zu einer unumgänglichen Schlussfolgerung: RISC-V-Kerne bedürfen einer umfassenden Überprüfung, wobei formale Techniken eine Schlüsselrolle spielen. Formale Tools können garantieren, dass ein Kerndesign die ISA genau implementiert, dabei keine erforderlichen Funktionen fehlen und kein vorsätzliches oder unbeabsichtigtes Verhalten eingefügt wird, das gegen die ISA verstößt. Dazu gehören das Screening des Designs auf Sicherheitslücken und das Erkennen von Hardware-Trojanern. Nur formale Werkzeuge können nicht nur beweisen, dass das Design das tut, was es tun soll, sondern auch, dass es nichts tut, was er nicht tun soll. Formale Anwendungen (Apps) können auch das Kerndesign für die funktionale Safety analysieren und die von Safety-Standards geforderten Fehler- und Fehlermetriken berechnen. Viele dieser Apps laufen auch auf Full-Chip-Ebene und gewährleisten so die Integrität von SoCs, die RISC-V-Cores integrieren.

Für das Wachstum des RISC-V-Ökosystems ist es am besten, wenn die Konformitäts- und Integritätsüberprüfung durch Tools und IP von Drittanbietern durchgeführt werden kann. Auf diese Weise können mehrere Kernanbieter mit derselben Lösung überprüfen, was sie zu einem De-facto-Industriestandard macht. SoC-Anbieter, die Open-Source-Cores lizenzieren, können dieselben Tools und IPs verwenden, um potenzielle Cores zu überprüfen und die Einhaltung von Safety-Standards sowie die Einhaltung von Security- und Trust-Anforderungen zu überprüfen. Vor diesem Hintergrund hat Onespin kürzlich die RISC-V Integrity Verification Solution eingeführt.

RISC-V Integrity Verification Solution

Diese Lösung formalisiert die RISC-V-ISA in einer Reihe von System-Verilog-Assertions (SVA). Assertions definieren die Ergebnisse für jeden Befehl und die Exceptions und umfassen die Ausführung von der Befehlsdekodierung an in einer beliebigen RISC-V-Implementierung.

Dieser Ansatz ermöglicht einen 100-prozentigen formalen Nachweis für die Implementierung aller Instruktionen und Exceptions gemäß der ISA-Spezifikation und gewährleistet zuverlässig, dass ein Kern vollständig kompatibel ist. Der Benutzer stellt Informationen zur Implementierung des RISC-V-Kerns bereit, zum Beispiel die Anzahl der Pipelinestufen, um die SVA auf die Implementierung abzubilden. Die Lösung erkennt auch zusätzliche Funktionalitäten, die über die ISA-Spezifikation hinausgehen und überprüft formal, dass der Kern keine Hardwaretrojaner oder andere unbeabsichtigten Funktionen enthält.

Die RISC-V Integrity Verification-Lösung wird in Form einer Reihe von Apps bereitgestellt, um die Verwendung so einfach wie möglich zu gestalten. Sie ist flexibel genug, um vom Benutzer hinzugefügte benutzerdefinierte Erweiterungen gemäß RISC-V zu überprüfen und gleichzeitig sicherzustellen, dass die Compliance nicht beeinträchtigt wird. Sie wurde bereits verwendet, um Open-Source-Implementierungen von RISC-V-Core und SoC zu überprüfen. Dabei wurden sowohl interessante Designfehler als auch unerwartete Funktionen gefunden. Diese Ergebnisse sind für die RISC-V-Community von Nutzen und validieren die Onespin-Lösung als effektive Möglichkeit, die Integrität von Prozessor- und SoC-Designs zu gewährleisten. *(ma)* ■

Autoren

Sven Beyer
Product Manager Design Verification bei Onespin Solutions

Tom Anderson
Technical Marketing Consultant bei Onespin Solutions