

FPGA Code Protection



FCP damit niemand unbefugt an Ihre Daten kommt....

Schützen Sie Ihr Produkt gegen illegales Kopieren!

- FPGA
- Microcontroller
- Gesamtsysteme

1. Allgemeines

Datensicherheit ist im Informationszeitalter wichtiger denn je und FPGAs finden ihren Weg in immer mehr Produkte. Durch den stetig steigenden Marktanteil, werden Sicherheitslösungen für diesen Bereich nach und nach zu einem drängenden Problem. Die FCP bietet jetzt eine Lösung, um geistiges Eigentum (IP) in FPGAs für die Zukunft zu schützen.

FPGAs auf der Basis von SRAM sind flüchtig und verlieren darum ihre Konfiguration nach dem Ausschalten. Bei solchen Bausteinen muss die Konfiguration in einem externen Speicher abgelegt werden. Nach dem Einschalten des Gerätes werden diese Konfigurationsdaten über eine physikalische Verbindung vom Speicher zum FPGA übertragen. An dieser Stelle besteht eine große Sicherheitslücke. IP-Diebe können die Daten abfangen und ihre eigenen Systeme damit programmieren. Innerhalb von wenigen Augenblicken kann so die gesamte Entwicklungsleistung für ein FPGA - basiertes Produkt verloren sein.

Gleichmann Electronics Research bietet für dieses aktuelle Problem eine technisch ausgefeilte Lösung an.

Herzstück der FPGA Code Protection ist ein CPLD das eine ständige Sicherheitsüberwachung des zu schützenden Designs während des Betriebes macht.

Der Security Core für das FPGA wird dem Kunden in Form einer Blackbox zur Verfügung gestellt und kann einfach instantiiert werden.

(mehr dazu auf der nächsten Seite)

Die FCP bietet allerdings noch einen weiteren großen Vorteil. Es können zusätzlich Schaltungsteile untergebracht werden, sodass dieser Baustein kostenneutral eingesetzt werden kann. So übernimmt die FCP z.B. auch die Konfiguration des FPGAs wodurch man teure Configuration Devices spart.

2. Funktionsbeschreibung

Um einen IP-Core zu schützen geht man bei der FPGA Code Protection nicht den Weg die Konfigurationsdatei zu verschlüsseln, sondern man macht eine ständige Sicherheitsüberwachung des Designs während des Betriebes (vgl. Bild 1). Mit Hilfe eines CPLDs werden so genannte Handshaking-Token generiert und zu den beteiligten Bausteinen gesendet.

Sind die richtigen Token vorhanden, dann wird der Systemtakt für das User Design und somit die Funktion freigegeben. Werden die falschen Daten übermittelt, dann wird das ganze System zum Stillstand gebracht, indem man dem User Design einfach den Systemtakt abschaltet.

Die Kombination eines ausgeklügelten Echtzufallszahlengenerators mit bewährten Verschlüsselungsalgorithmen versperrt jeden derzeit bekannten Weg das Sicherheitssystem zu brechen.

Die Technologieunabhängigkeit der vorliegenden Entwicklung erlaubt einen praktisch beliebigen Austausch des CPLDs und der FPGAs als physikalischer Träger der Sicherheitslösung. Hierdurch ist die technische Nachhaltigkeit gewährleistet.

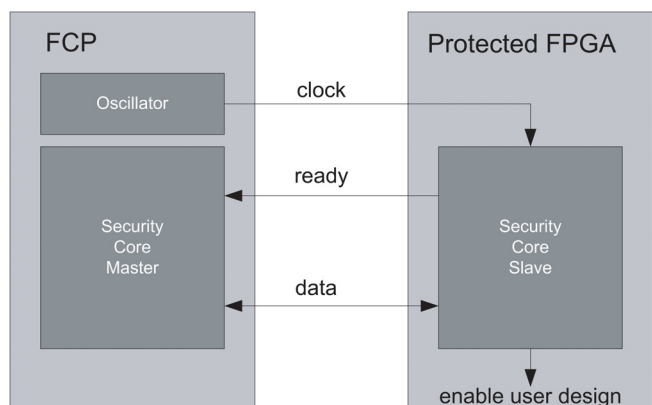


Bild 1: Security System

Die FCP steht als CPLD im 100 Pin TQFP zur Verfügung. Der Security Core, der dem Kunden in Form einer Blackbox zur geliefert wird, ist abhängig von der Zieltechnologie. Gleichmann Electronics Research bietet diese Blackbox für Altera, Xilinx und Lattice Bausteine an.

Zusätzlich kann man mit dem FPGA Entwicklungssystem Hpe_mini LEC (MSC) die Funktionalität direkt ausprobieren. Dieses System ist bereits mit FCP ausgestattet.

3. Applikationsbeispiele

In diesem Abschnitt werden einige Konzepte für den Einsatz der Sicherheitslösung vorgestellt.

3.1 Schutz eines FPGA:

In dieser Variante wird, wie vorher beschrieben, das FPGA durch die FCP geschützt. Zwar kann der Datenstrom des FPGA beim Konfigurieren aufgezeichnet werden, doch ohne die zugehörige FCP funktioniert das Design nicht.

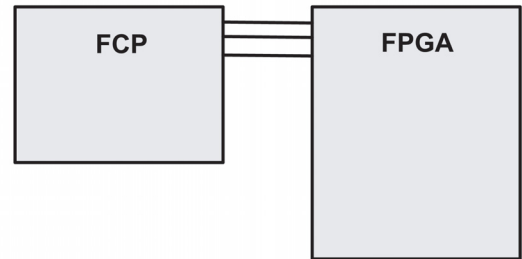


Bild 2: Standardanwendung

3.2 Schutz- und Konfigurationssystem für SRAM-basierte FPGAs:

In dieser Variante wird der FPGA nicht nur geschützt sondern mit Hilfe der FCP auch konfiguriert. Dabei werden die Daten in einem parallelen oder kostengünstigen, seriellen Flash abgelegt und die FCP wirkt als Controller.

Da der Preis der Configuration Devices bei den FPGA Herstellern teilweise sehr hoch ist, kann man hier durch Einsparungen, mit Hilfe kostengünstiger Flash-Speicher, die Kosten für die FCP neutralisieren.

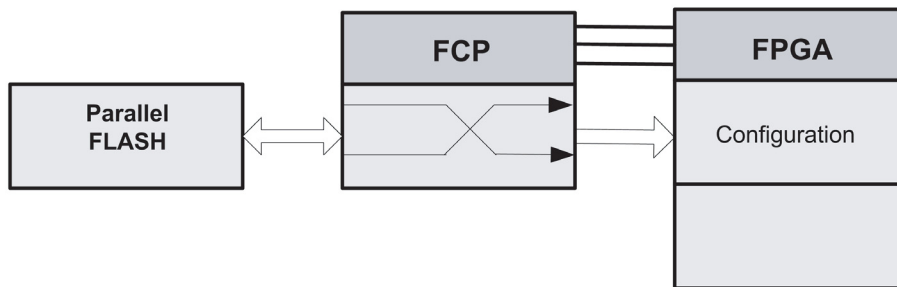


Bild 3: Schutz und Konfiguration

3.3 Schutz- und Konfigurationssystem + externer Programmspeicher:

Wie man in diesem Beispiel sehen kann, lässt sich dieses System nicht nur für die Sicherheit und die Konfiguration verwenden, sondern bietet z.B. auch die Möglichkeit das Flash zusätzlich als Programmspeicher für die CPU einzusetzen.

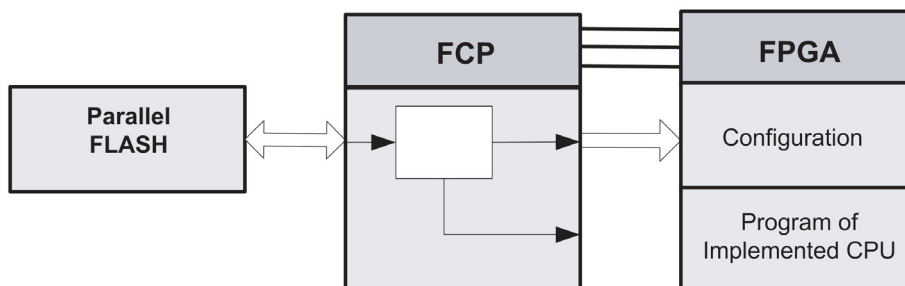


Bild 4: Erweiterte Anwendung

3.4 Schutz eines Mikrocontrollers-Systems:

Systeme mit Mikrocontroller, die den gesamten Programmcode im internen Flash haben, sind je nach Hersteller relativ sicher. Was passiert allerdings bei einem Programm Update, wenn sich das System schon beim Kunden befindet? Hier besteht die gleiche Sicherheitslücke wie bei FPGAs, da der Code über eine physikalische Schnittstelle übertragen werden muss.

So ein System kann man ebenfalls mit Hilfe der FPGA Code Protection schützen. Voraussetzung dabei ist, dass Funktionalität vom Mikrocontroller auf den FPGA ausgelagert wird. (Bild 4 zeigt die ausgelagerte Decryption von Daten) Somit kann der FPGA über die FCP und damit das gesamte Design geschützt werden.

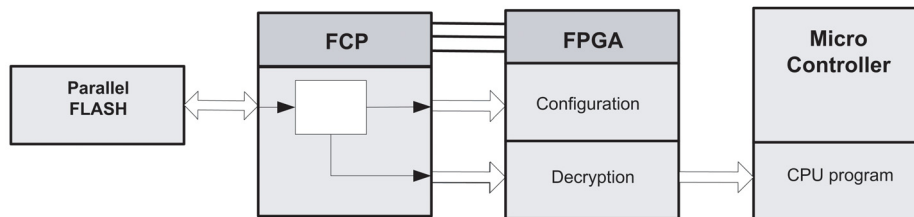


Bild 4: Schutz eines Mikrocontroller-Systems

Es gibt noch viele weitere Möglichkeiten wo die FPGA Code Protection einsetzbar ist. Gleichmann Electronics Research unterstützt Sie natürlich gerne bei der Entwicklung und Implementierung ihrer eigenen speziellen Lösung.

Für weitere Fragen stehen wir Ihnen natürlich ebenfalls gerne zur Verfügung.

Gleichmann Electronics Research (Austria) GmbH
(Austria) GmbH & Co KG

Softwarepark – IT Center – Top 2/4
Hauptstraße 119
4232 Hagenberg | Austria

GE Research

per Tel.: +43 7236 3343 499
per Mail: sales@ger-fae.com

www.ger-fae.at



Copyright Notice (2006)

This document is copyrighted, 2005, by Gleichmann Electronics Research (Austria) GmbH & Co KG. All rights are reserved. Gleichmann Electronics Research (Austria) GmbH & Co KG reserves the right to make improvements to the products described in this manual at any time without notice. No part of this manual may be reproduced, copied, translated or transmitted in any form or by any means without the prior written permission of Gleichmann Electronics Research (Austria) GmbH & Co KG. Information provided in this manual is intended to be accurate and reliable. However, Gleichmann Electronics Research (Austria) GmbH & Co KG assumes no responsibility for its use, nor for any infringements upon the rights of third parties which may result from its use.