

Zusammenhang von Bitstrom und der realen Implementation (Zynq UltraScale+ MPSoC-FPGA)

HTV Halbleiter-Test & Vertriebs-GmbH, Bensheim, Deutschland



Kurzfassung

FPGAs (Field Programmable Gate Arrays) sind integrierte Schaltkreise der Digitaltechnik und kommen in vielen Gebieten der digitalen Elektronik zum Einsatz. Die hohe Flexibilität erreichen FPGAs durch ihre änderbare Konfiguration, die durch den sogenannten Bitstrom in den FPGA geladen wird. Durch hochenergetische kosmische Strahlung kann es vorkommen, dass der Zustand eines Bit geändert und die Funktion eines Designs gestört wird. HTV untersuchte im Kundenauftrag, welche Bitfehler in der Konfiguration eines FPGAs tatsächlich einen signifikanten Effekt im Design aufweisen.

1 Bitstrom und Frameadresse

Bei FPGAs der Firma Xilinx unterteilt sich die gesamte Konfiguration in kleine Abschnitte, den sogenannten Frames. Diese besitzen eine physikalische Frameadresse (PFA) mit der sie angesprochen werden können (vgl. Abbildung 1). Jedes Frame besteht bei einem ZU9EG (Zynq UltraScale+ MPSoC) aus 93 Wörtern mit jeweils 32 Bits bzw. 2976 Bits in Summe.

Der Bensheimer Elektronikspezialist HTV entwickelte nun ein Verfahren, mit dem es möglich ist, zu allen Ressource-Spalten der programmierbaren Logik die jeweils zugehörigen physikalischen Adressen zu ermitteln und den Inhalt der Frame auszulesen. Im Bitstrom gesetzte Bits können so einem physikalischen Bereich auf dem FPGA-Chip zugeordnet werden. Dies ermöglicht es zu testen, welchen Effekt diese Bits in einem Design aufweisen und Vorhersagen dazu zu treffen.

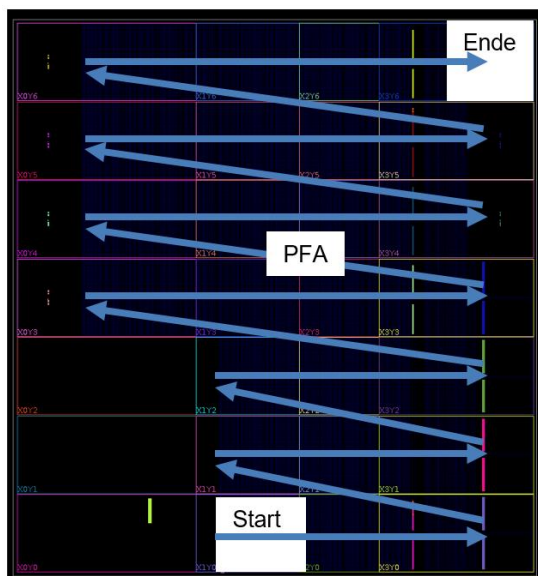


Abbildung 1: Verlauf der physikalischen Frameadressen.

2 Konfiguration des Designs

Logische Funktionen werden auf FPGAs in den sogenannten Slice-Blöcken realisiert. Ein Frame enthält beim ZU9EG insgesamt 60 solcher Slices. Die Slices enthalten die logischen Grundelemente wie z. B. LUT, FF und MUX (vgl. Abbildung 2).

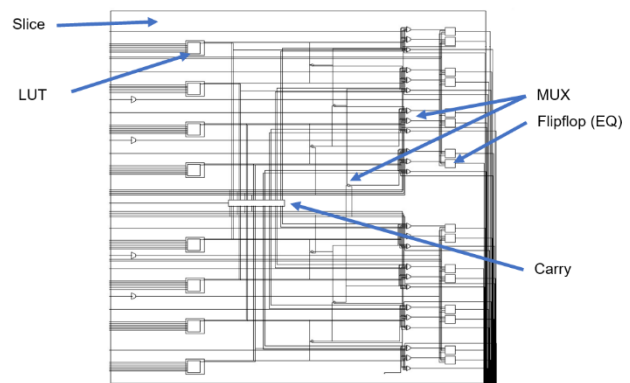


Abbildung 2: Elemente eines Slice-Blocks.

Für die Demonstration wird in der Slice X36Y0 das Flipflop mit dem Ausgang EQ konfiguriert und im nächsten Abschnitt versucht dessen Zustand zu beeinflussen (vgl. Abbildung 3).

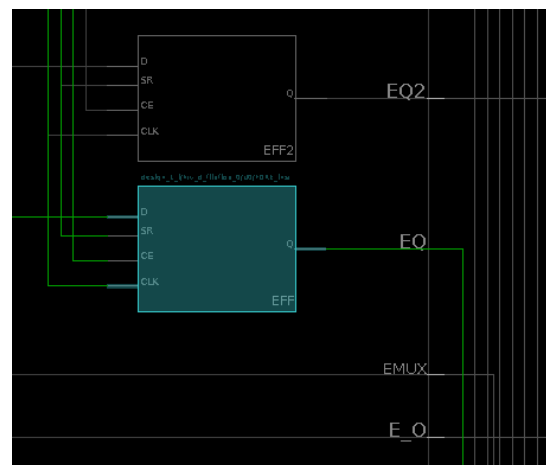


Abbildung 3: Konfiguriertes Flipflop mit Ausgang EQ.

3 Physikalische Position

Die Slice X36Y0 liegt unten links in der Taktregion X1Y0 auf dem FPGA Chip (vgl. Abbildung 1).

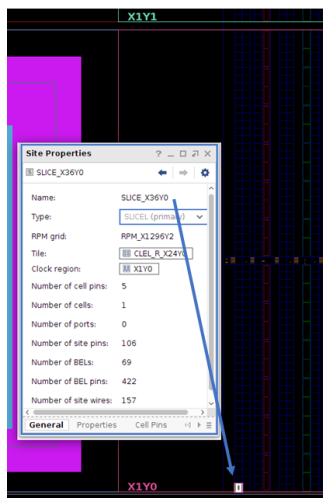


Abbildung 4: Lage der Slice Y36Y0 auf dem FPGA Chip.

Mit dem von HTV entwickelten Verfahren kann berechnet werden, dass der Flipflop mit dem Ausgang EQ der Slice X36Y0 durch die ersten 48 Bits in der PFA 00004B0C000₁₆ und deren benachbarten Frames konfiguriert wird.

4 Bitweise Designänderung

Betrachtet wird jeweils ein Ausschnitt (Bit 24 bis Bit 31) aus dem ersten Datenwort des ermittelten Frames. Wie erwartet, enthält der Bereich Bits mit dem Wert „1“ (vgl. Abbildung 5).

In den dargestellten Frames werden über den Internal Configuration Access Port (ICAP) die ersten 48 Bits bitweise gekippt (0 → 1 oder 1 → 0) und geprüft, ob das jeweilige Bitkippen zu einem signifikanten Einfluss führt.

Es zeigt sich, dass drei Bits den Ausgang des Flipflops dauerhaft auf 1 setzen und ein Bit, mit dem der Ausgang dauerhaft auf 0 gesetzt werden kann, existiert.

Sobald die Bits zurückgekippt werden, ist die ursprüngliche Funktion des Designs wieder gegeben.

Analyse von Bitkippern auf den Flipflop-Ausgang EQ

Bitoffset	24	25	26	27	28	29	30	31
Frame (PFA: 00004B0C000)	0	1	1	0	0	0	0	0
Frame +1	0	0	0	0	0	0	0	0
Frame +2	0	0	0	0	0	0	0	0
Frame +3	0	1	0	0	0	0	0	0
Frame +4	1	0	0	0	0	0	0	0
Frame +5	0	0	0	0	0	0	0	0
Frame +6	0	0	0	0	0	0	0	0
Frame +7	0	0	0	0	0	0	0	0
Frame +8	1	0	0	0	0	0	0	1

Legende

Kein Effekt	
Signifikanter Effekt	Flipflop Ausgang dauerhaft high
Signifikanter Effekt	Flipflop Ausgang dauerhaft low

Abbildung 5: Signifikante Bits zur Beeinflussung des Flipflops Ausgangs EQ.

5 Analyse der Bitfehler

1. Lage der signifikanten Bits:

Die Bits mit einem signifikanten Einfluss auf das Design liegen in unterschiedlichen Frames, aber nahe beieinander (nur zwischen Bit 24 und 29).

2. Kipprichtung:

Signifikante Effekte treten nicht nur bei einem Übergang von 1 nach 0, sondern auch bei einem Übergang von 0 nach 1 auf.

3. Anzahl signifikanter Bits:

Es existieren zu einem Flipflop Ausgang in einer Slice mindestens 4 Bits, die einen signifikanten Effekt aufweisen.

4. Steuerung des Flipflops:

Je nach Lage des geänderten Bits liefert der Ausgang des Flipflops konstant entweder 0 oder 1.

5. Reversibilität der Bitkipper:

Alle bei HTV induzierten Bitfehler konnten sich wieder korrigieren lassen. Das Design zeigte danach immer die originale Funktionsweise. Ein bleibender Schaden im physikalischen Chip konnte nicht festgestellt werden.

6 Fazit

Mit dieser Forschung konnte gezeigt werden, dass in der Konfiguration eines FPGAs signifikante Bits existieren, die zu einer Änderung der Flipflop Ausgänge führen.

Mit dem von der HTV GmbH in Bensheim entwickelten Verfahren können die signifikanten Bits auf dem gesamten FPGA-Chip für alle Flipflops berechnet werden.