Technologie Überblick
Flash & Antifuse vs. SRAM

André Ehlert

Agenda

> Abgrenzungsmerkmale

Firm Error

Kopierschutz

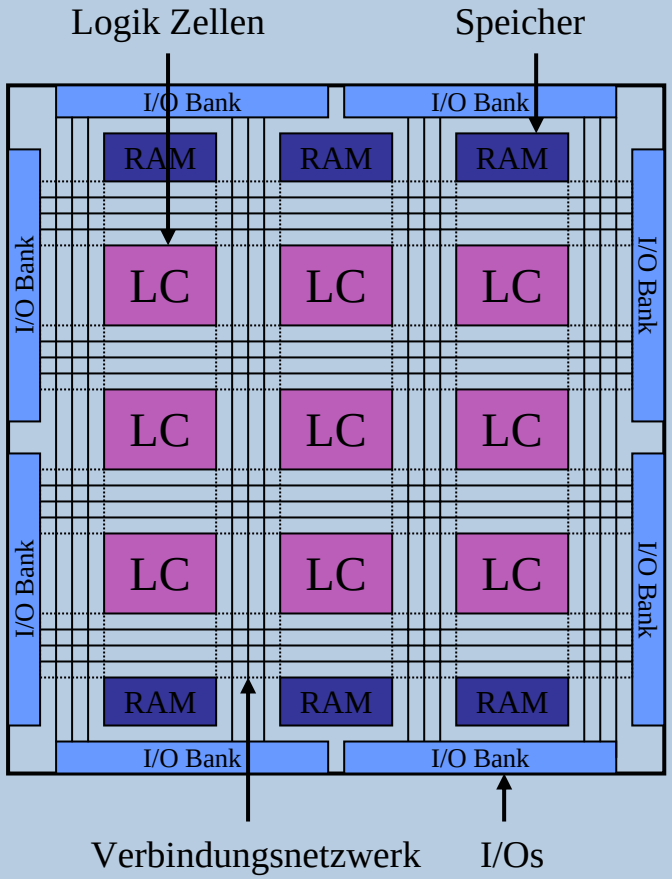
Leistungsaufnahme

Systemkosten

Zusammenfassung

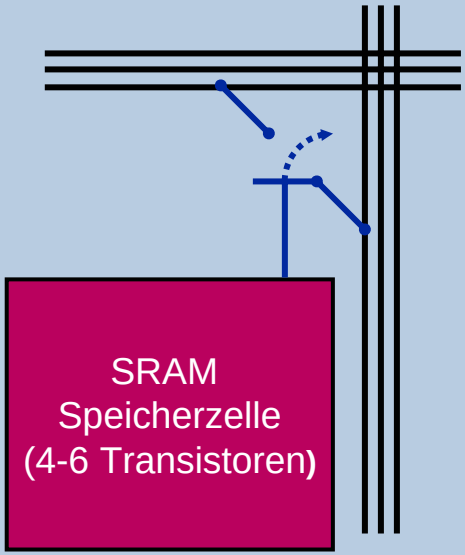
FPGA
Allgemeiner Aufbau und Funktion

- FPGA besteht aus
  - ***Logik Zellen*** **für Realisierung der Funktionsgeneratoren**
  - ***Verbindungsnetzwerk*** **um die Logik Zellen, RAM und I/Os miteinander zu verknüpfen**
  - ***RAM*** **Speicher zur Zwischenspeicherung von Daten**
  - ***I/Os*** **für die Ein- und Ausgabe von Daten**
- Eine Konfiguration speichert den Zustand von
  - **Verbindungsnetzwerk**
  - **I/Os**
  - **Logik Zellen**



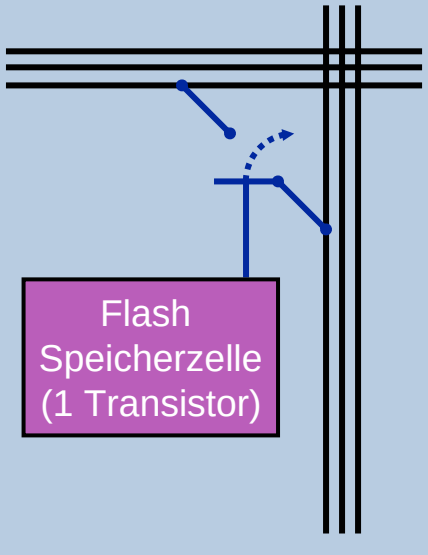
Verbindungsnetzwerk
Technische Realisierung

SRAM FPGA



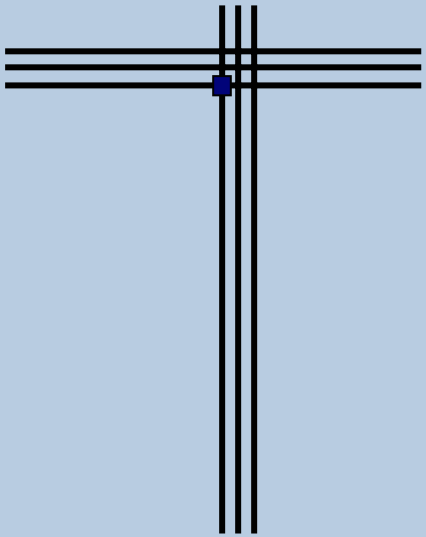
Reprogrammierbar

Flash FPGA



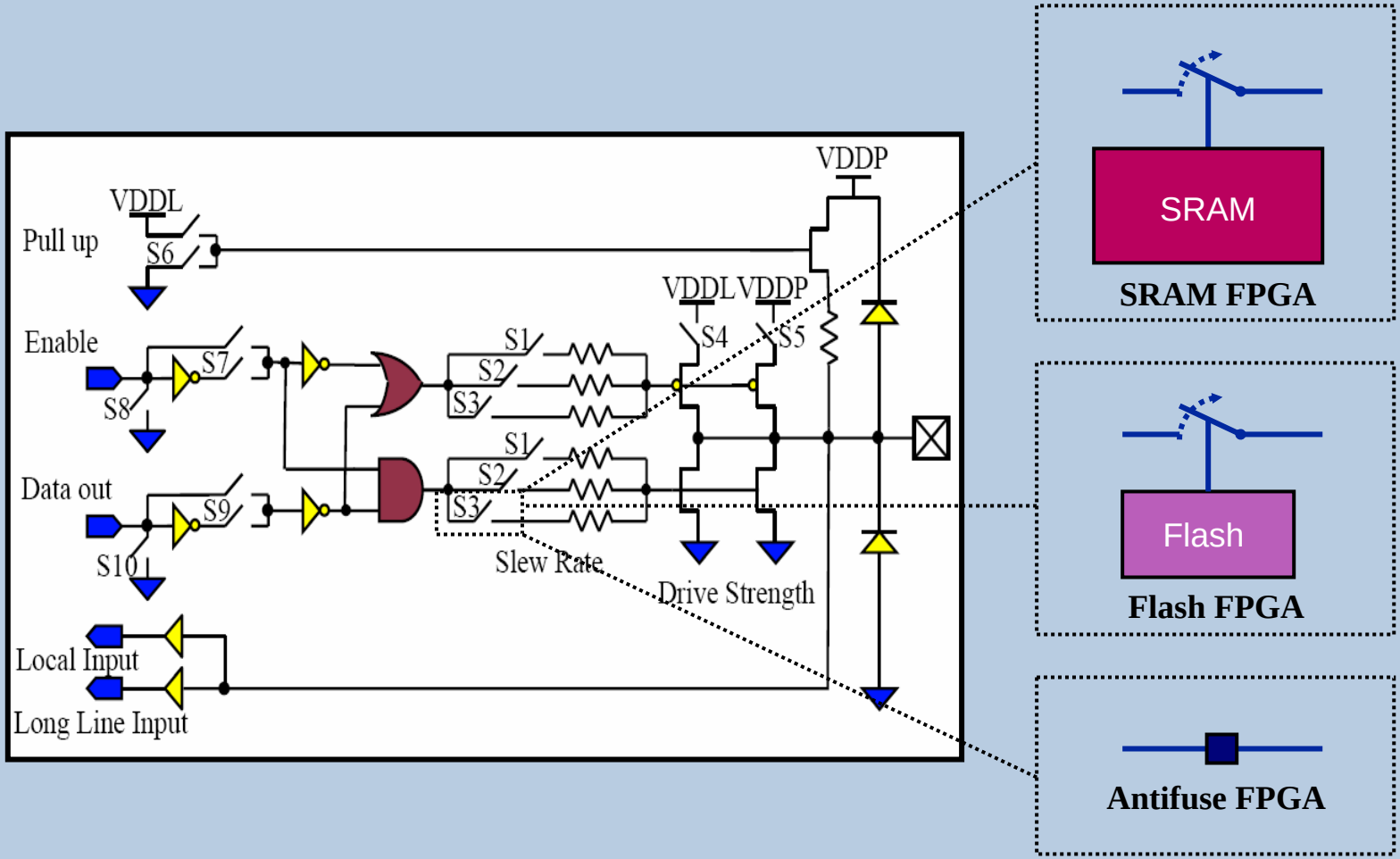
Reprogrammierbar

Antifuse FPGA



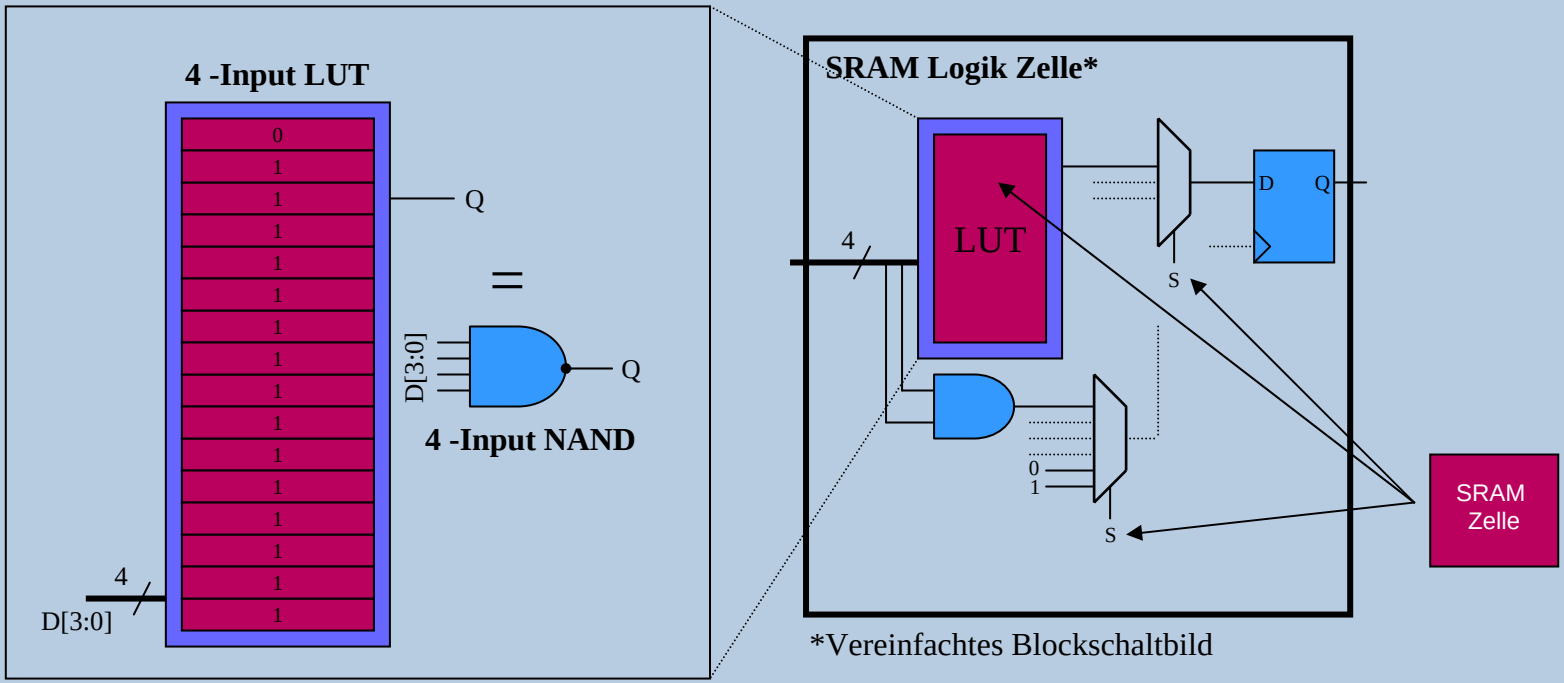
Nicht Reprogrammierbar (OTP)

I/Os
Technische Realisierung



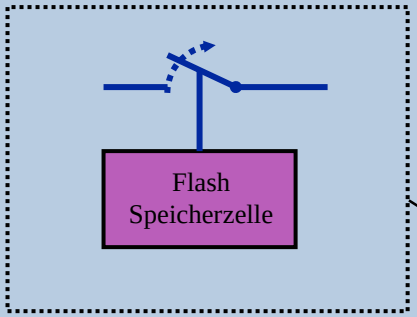
Aufbau Logik Zelle: SRAM
Beispiel: Spartan (Xilinx)

- **Lookup Tabellen (LUT) dienen der Implementierung von booleschen Funktionen**
- **SRAM Zellen werden für die Realisierung der LUT sowie für die innere Konfiguration der Logik Zellen verwendet**

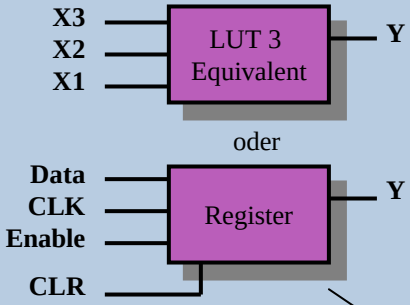


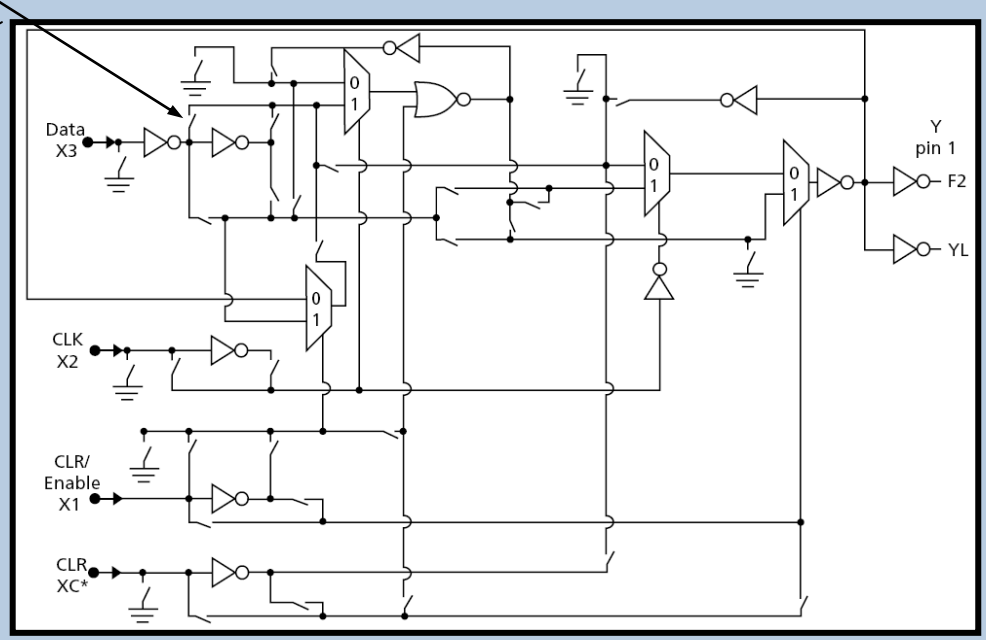
Beispiel: Realisierung einer 4-Input NAND Logik

Aufbau Logik Zelle: Flash
Beispiel: ProASIC3



Eine boolesche Funktion, ein Register oder ein Latch werden durch das Verdrahten von Gattern und Multiplexern innerhalb einer Versa Tile realisiert



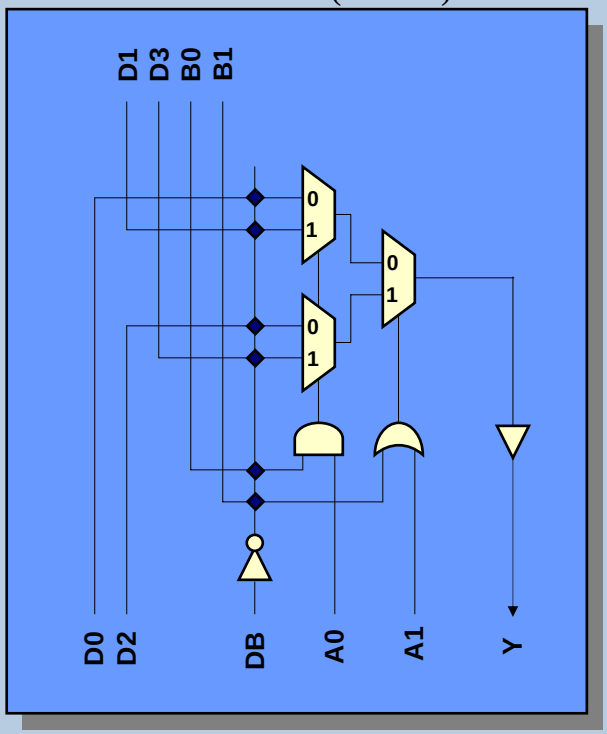


Aufbau Logik Zelle: Antifuse
Beispiel: Axcelerator

- **Logik Zellen bestehen aus K- und R-Zellen**
- **Boolesche Funktion werden in K-Zellen realisiert**
- **Register werden durch R-Zellen realisiert**

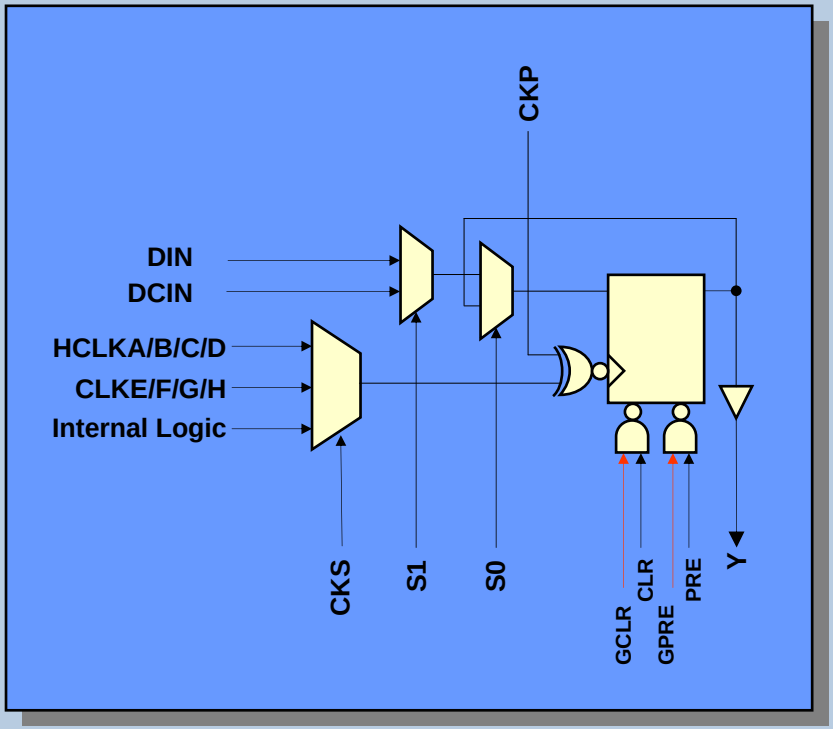
Logik Zelle

Kombinatorische Zelle (K-Zelle)



+

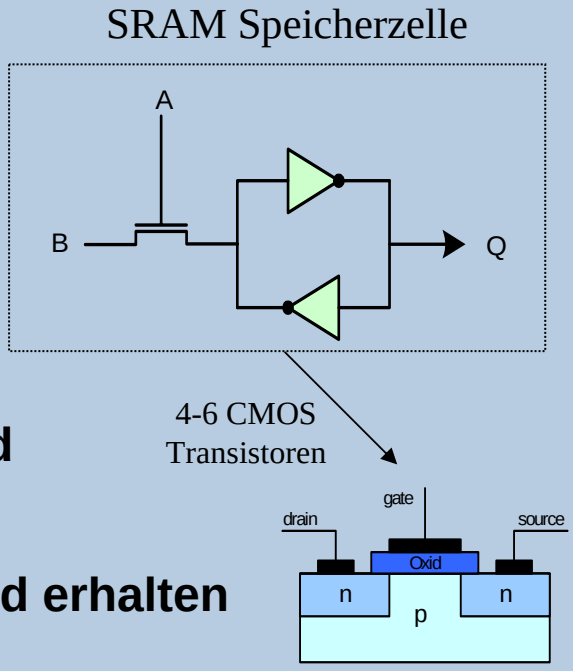
Register Zelle (R-Zelle)



Beispiel: Axcelerator

SRAM Speicherzelle

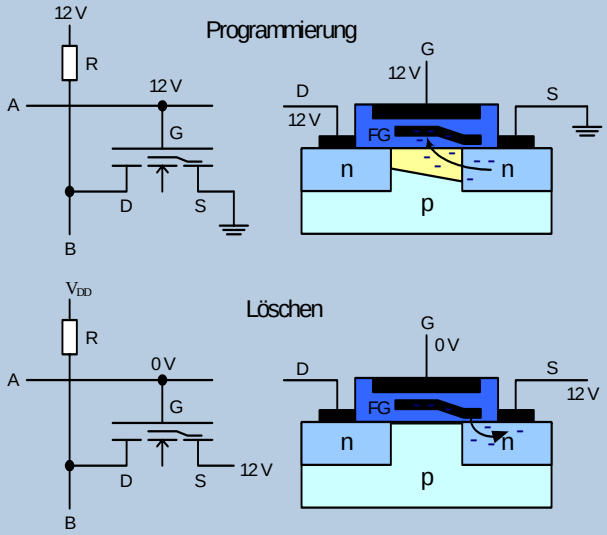
4-6 Transistoren speichern ein Bit



- Programmierung
  - **Aktivierung der Adressleitung A**
  - **Anlegen des Eingangswert B**
  - **Inverter kippen in vorgegebenen Zustand**
- Lesen
  - **Nach dem Deaktivieren bleibt der Zustand erhalten**
  - **Verbindungsnetzwerk**
    - **Ausgang Q treibt einen Schalttransistor**
  - **Input/Output**
    - **Ausgang Q treibt einen Schalttransistor**
  - **Logik Zelle (Look Up Table)**
    - **Ausgang Q definiert Speicherzustand in einer LUT-Zelle**

FLASH Speicherzelle

Ein Transistor speichert ein Bit

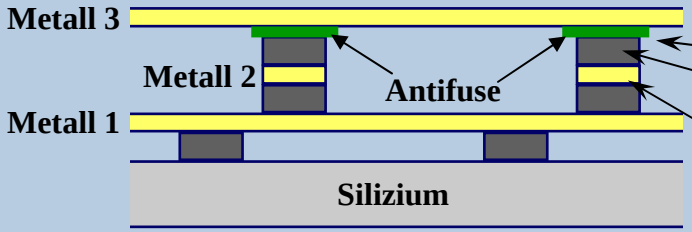


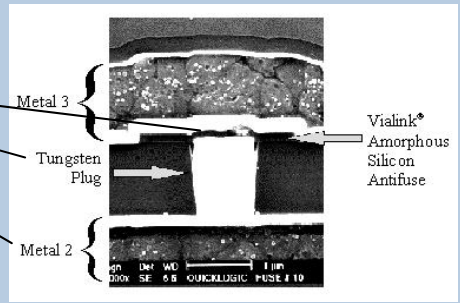
- **Programmierung**
  - **Elektronen werden in das FG gezogen (*Lawineneffekt*)**
  - **Schwellspannung des Transistors wird verschoben**
  - **Bei einem H-Pegel am Gate sperrt der Transistor (B = ‘1‘)**
- **Löschen**
  - **Elektronen werden durch *Tunneleffekt* vom FG “abgesaugt“**
  - **Schwellspannung des Transistors liegt wieder bei Core-Spannung**
  - **Bei einem H-Pegel am Gate leitet der Transistor (B = ‘0‘)**
- **Lesen**
  - **Ausgang B treibt einen weiteren Schalttransistor**
  - **Zustand des FG bestimmt den Schaltzustand**

Antifuse

Programmierung

- **Isolierschicht wird durch Anlegen einer Programmierspannung durchgebrannt**
- **Dadurch wir dauerhaft ein niederohmiger elektrischer Kontakt hergestellt**
- **Programmiervorgang ist irreversibel, d.h. Löschen bzw. Reprogrammierung ist nicht mehr möglich (OTP)**





Beispiel: M2M (Metal to Metal) Antifuse

$C_{Antifuse}$ = 1 fF
$R_{Antifuse}$ = 25Ohm

Agenda

Actel

Abgrenzungsmerkmale

> Firm Error

Kopierschutz

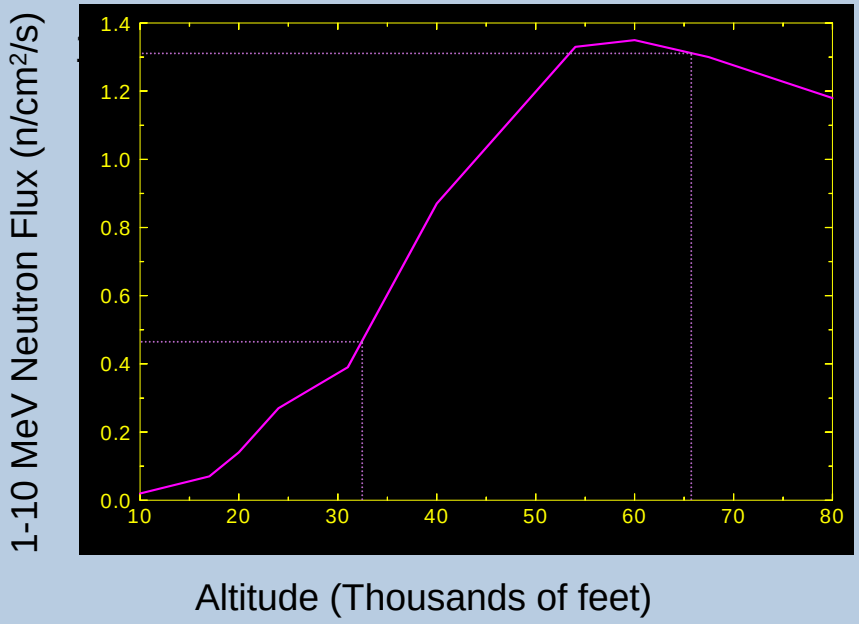
Leistungsaufnahme

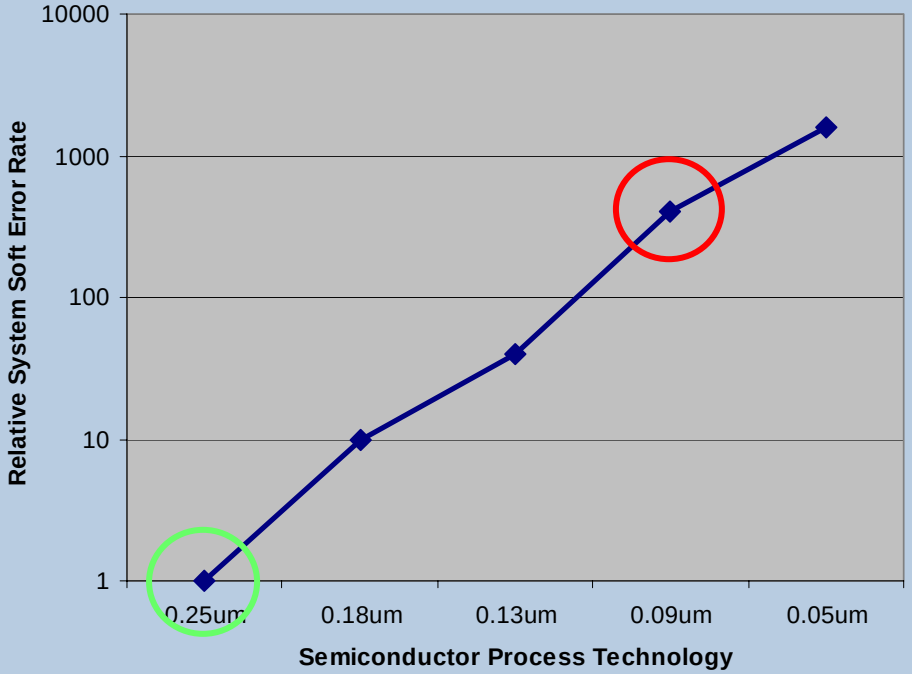
Systemkosten

Zusammenfassung

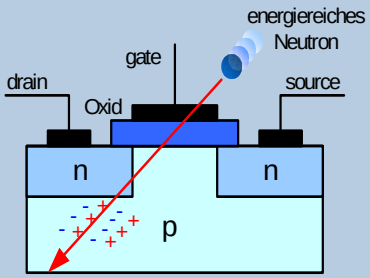
Firm Error

- **Neutronenstrahlung steigt mit der Höhe (max. bei ca. 20km)**
  - **In 10km Höhe ca. 150mal, in 20km Höhe ca. 600mal größer als auf Meereshöhe**
  - **Strahlung auf Meereshöhe nicht vernachlässigbar**
  - **Strahlung steigt vom Äquator zu den Polen hin an (6fach)**
- **Kleinere Prozessgeometrie empfindlicher gegenüber Neutronen**



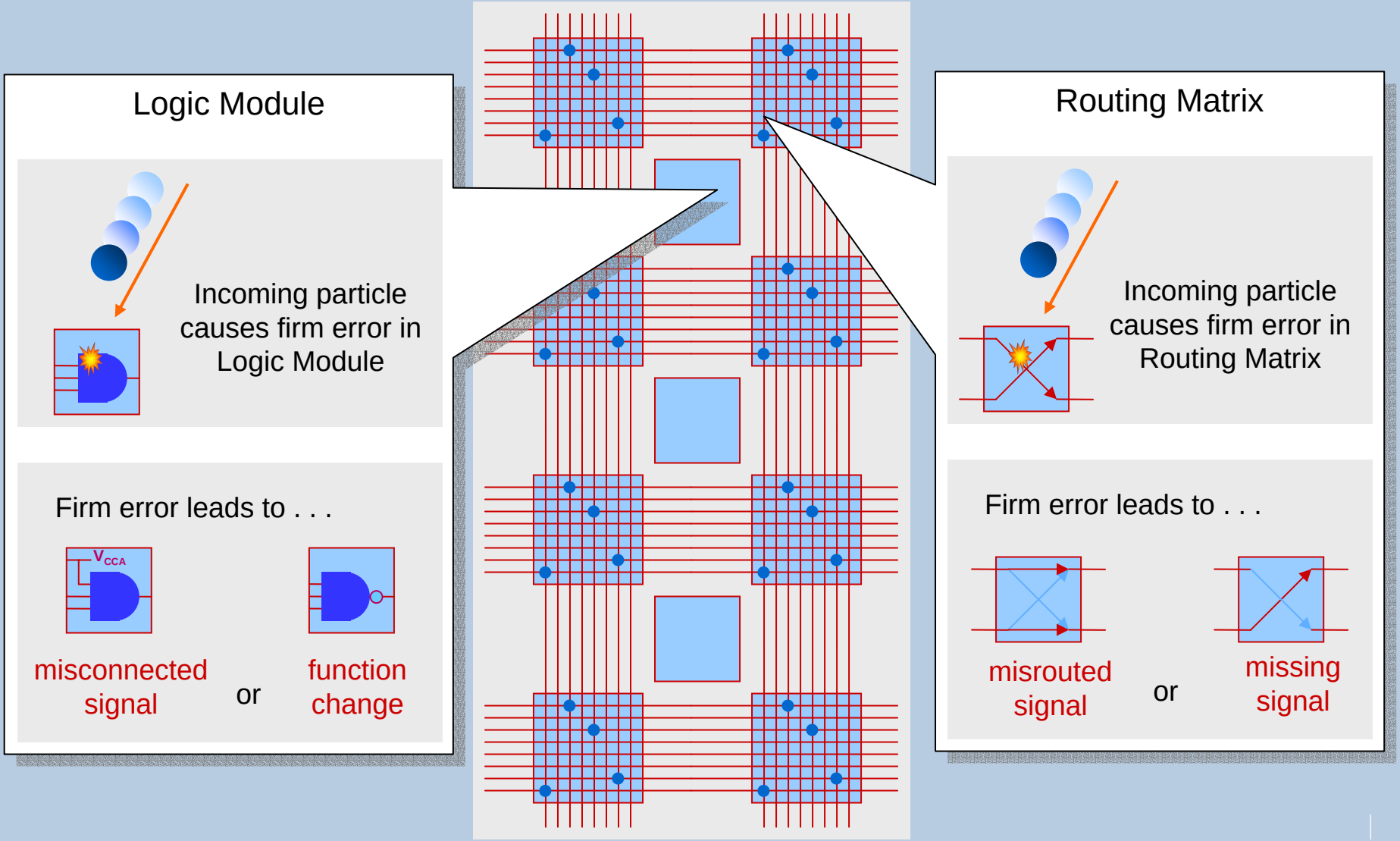


Firm Error



- ***Soft Error*** **: Ungewollte reversible Änderung des Inhalts einer Speicherzelle**
  - **SRAM, DRAM Zellen**
  - **FlipFlops**
- **Soft Errors entstehen beim Auftreffen energiereicher Teilchen auf dem Chip (Neutronen, Ionen, ...)**
- **Teilchen kommen von**
  - **Radioaktive Isotope im Gehäuse (Verunreinigung)**
  - **Kosmische Strahlung erzeugt in der Erdatmosphäre energiereiche Neutronen durch Kernreaktion. Diese Neutronen reagieren dann mit Si-Atomen im Chip.**
- ***Firm Error*** **: Soft Error tritt im FPGA Konfigurationsspeicher auf**

Firm Error
Einfluss auf die Konfiguration



Firm Error
FIT-Raten Untersuchung von iROC

FPGA	Technology	Equivalent Functional Failure FIT Rates per Device			
		Ground-Level Applications		Commercial Aviation	Military Aviation
		Sea Level	5,000 Ft	30,000 Ft	60,000 Ft
Actel AX1000 1M-Gate	0.15µm Antifuse	No Failures Detected	No Failures Detected	No Failures Detected	No Failures Detected
Actel APA1000 1M-Gate	0.22µm Flash	No Failures Detected	No Failures Detected	No Failures Detected	No Failures Detected
Actel A3P1000 1M-Gate	0.13µm Flash	No Failures Detected	No Failures Detected	No Failures Detected	No Failures Detected
Xilinx XC2V3000 3M-Gate	0.15µm SRAM	1,150 FITs	3,900 FITs	170,000 FITs	540,000 FITs
Xilinx XC3S1000 1M-Gate	90nm SRAM	320 FITs	1,100 FITs	47,000 FITs	150,000 FITs
Altera EP1C20 1M-Gate	0.13µm SRAM	460 FITs	1,600 FITs	67,000 FITs	220,000 FITs
Altera EP2C20 1M-Gate	90nm SRAM	700 FITs	2,400 FITs	103,000 FITs	330,000 FITs
Altera EP2S30 2M-Gate	90nm SRAM	1,500 FITs	5,200 FITs	225,000 FITs	710,000 FITs

- **FIT (Failure in Time): Anzahl der Fehler in 10^9 Stunden**
  - **Akzeptierte FIT Raten für kommerzielle Anwendungen: FIT < 100**
  - **Akzeptierte FIT Raten für industrielle Anwendungen: FIT < 50**

Agenda

Abgrenzungsmerkmale

Firm Error

> Kopierschutz

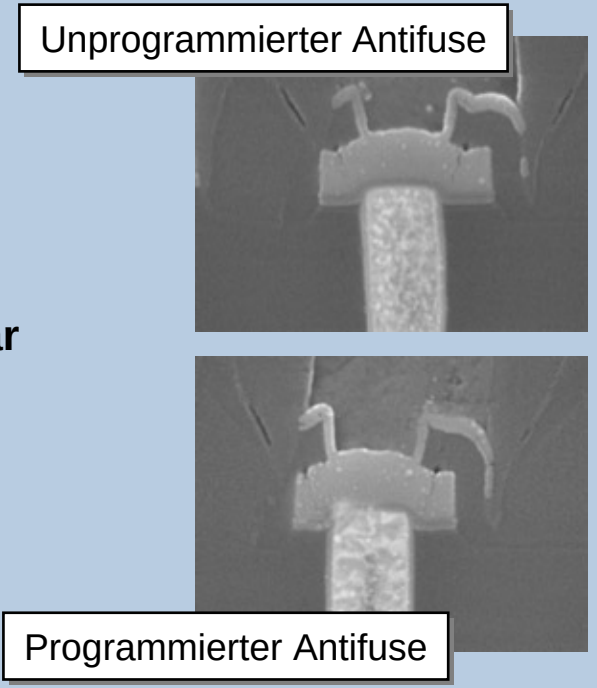
Leistungsaufnahme

Systemkosten

Zusammenfassung

Sicherheitsklassen

- Klasse 1
  - **Nicht sicher, ohne großen Aufwand kopierbar**
  - **SRAM FPGAs, Gate-Arrays (Semi Customer)**
- Klasse 2
  - **Nur mit hohem Geräte- und Zeitaufwand kopierbar**
  - **Kein Rücklesemechanismus für Flash & Antifuse**
  - **Flash:**
    - **Flash Transistoren liegen unter 7 Metallisierungsebenen.**
    - **Speicherzustand der Floating Gates schwierig zu erfassen**
  - **Antifuse:**
    - **Nur 3-5% der bis zu 50 Millionen Antifuses werden für ein Design genutzt**
- Klasse 3
  - **In Speziallabors mit sehr hohem Zeitaufwand kopierbar**
  - **Standardzellen ICs (Full Customer)**



Flash & Fuse Lock

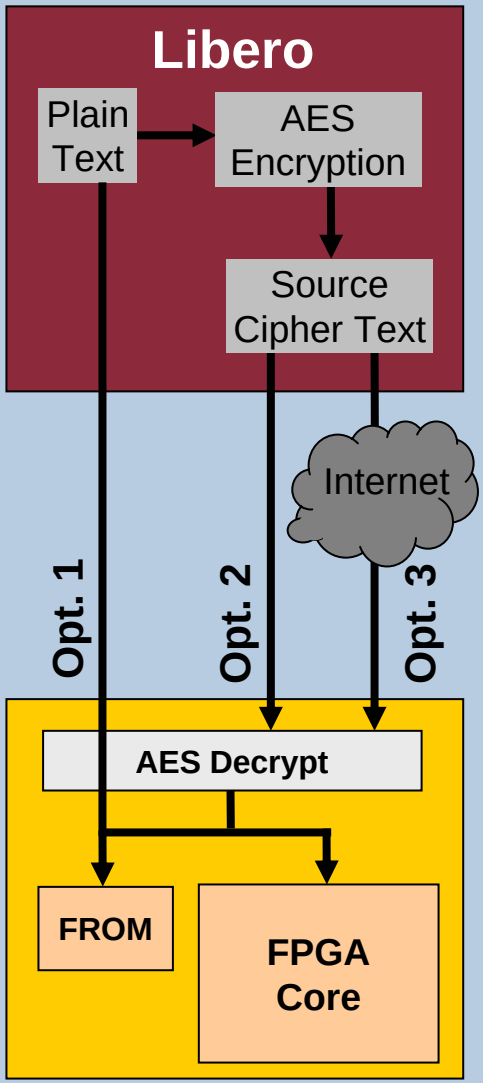
Flash: 2 verschiedene Security Mechanismen

- **Key-Lock**
  - **Benutzerdefinierter Schlüssel (128 Bit)**
  - **Programmieren, Löschen und Verifizieren nur mit 128 Bit Schlüssel**
- **Permanent Lock**
  - **Bauteil kann weder ausgelesen noch reprogrammiert werden (OTP)**

Antifuse (OTP):

- **Fuse-Lock**
  - **Bauteil kann weder verifiziert noch über Debugschnittstelle getestet werden**

AES im ProASIC3



- **Neben Flash Lock verfügt die ProASIC3/E Familie zusätzlich über AES Entschlüsselung**
- **Die Konfigurationsdaten können durch einen vom Anwender frei wählbaren 128 Bit Schlüssel verschüsselt werden**
- **Die Konfigurationsdaten werden im Baustein durch den vorher vereinbarten AES Schlüssel wieder entschlüsselt**
- **Im Baustein ist hierzu ein dedizierter AES Decoder integriert**
- **FPGA und FROM können unabhägig mit AES programmiert werden**

Agenda

Abgrenzungsmerkmale

Firm Error

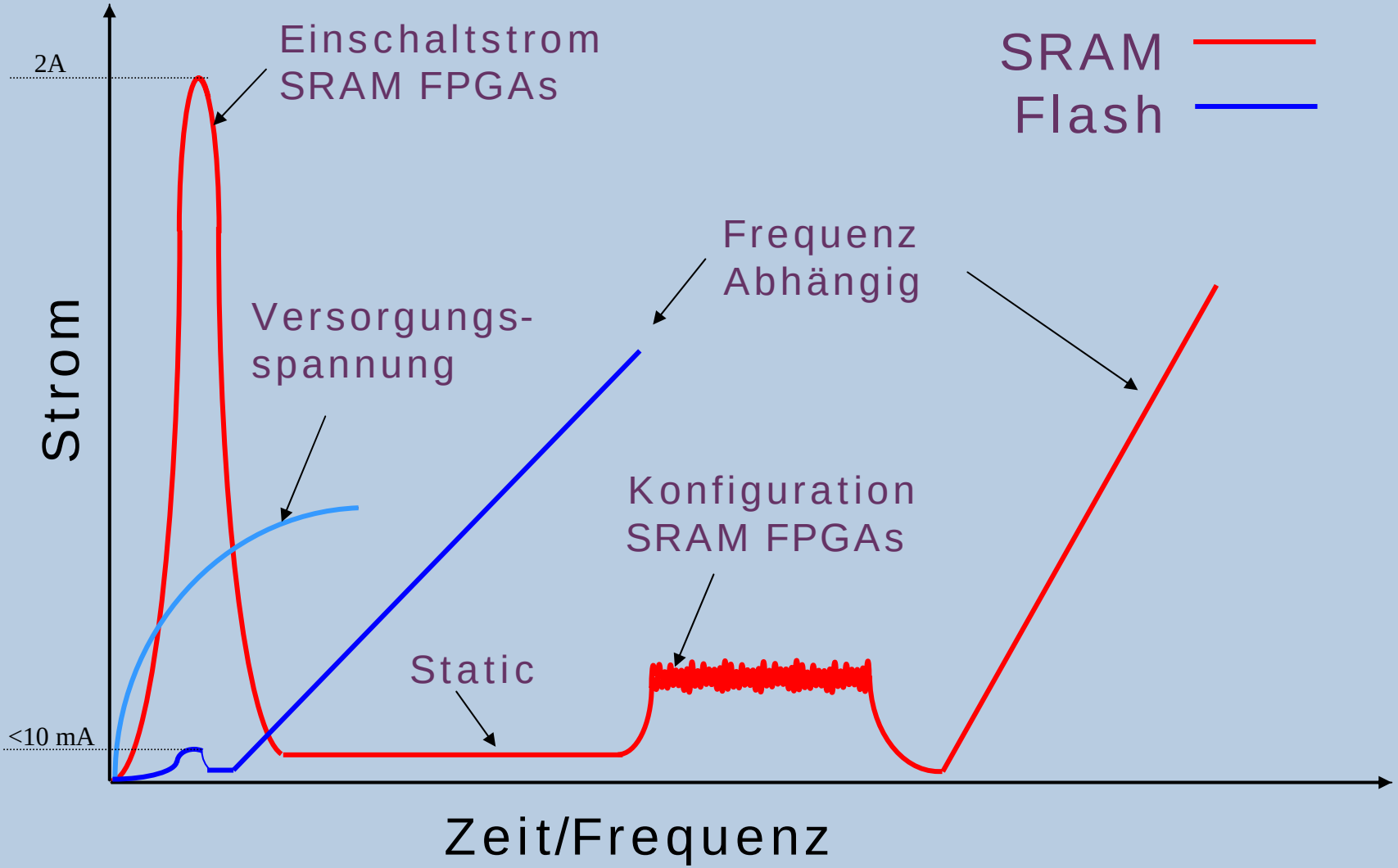
Kopierschutz

> Leistungsaufnahme

Systemkosten

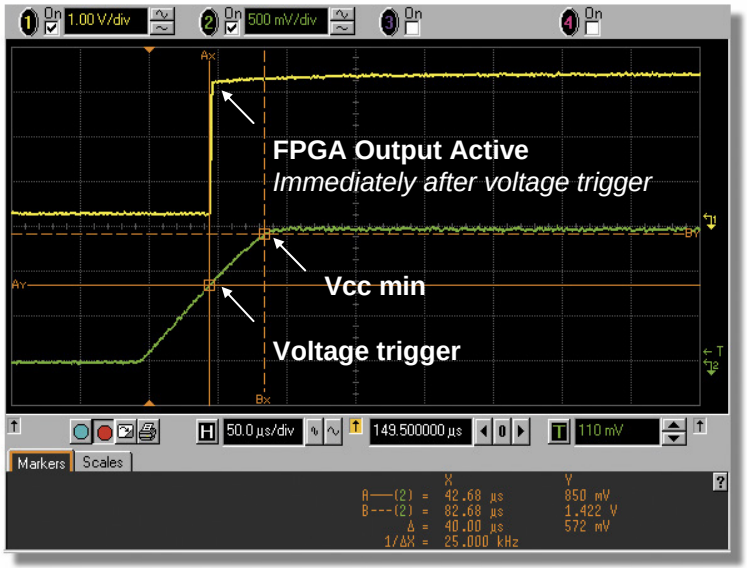
Zusammenfassung

Einschaltstrom

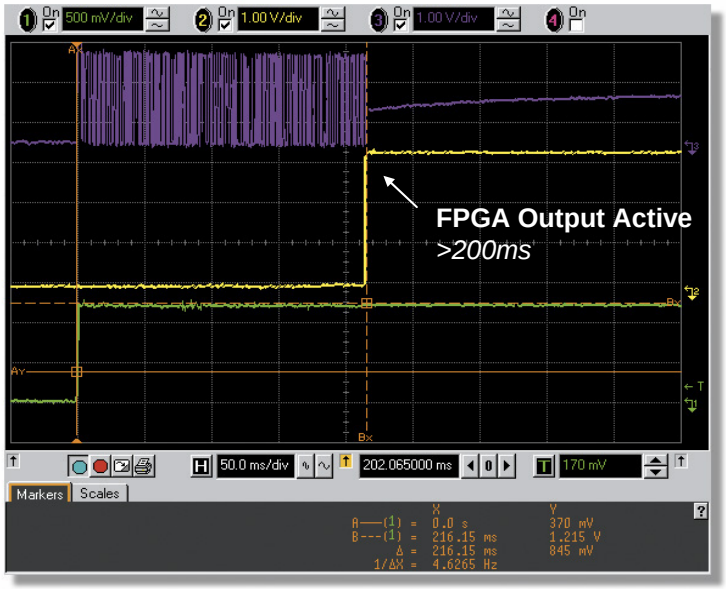


Live At Power Up

ProASIC3: A3PE600

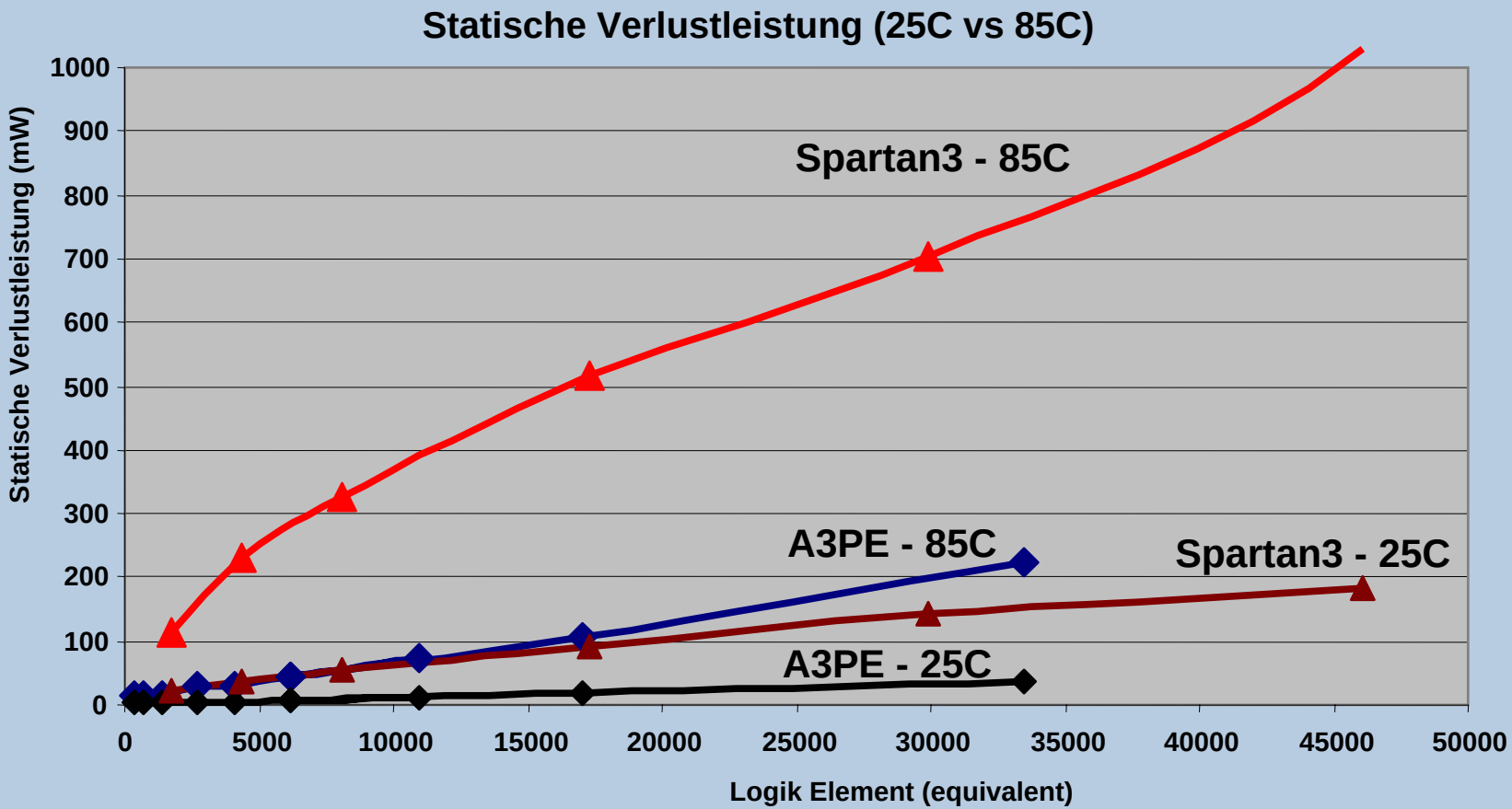


Spartan 3: XC3S200

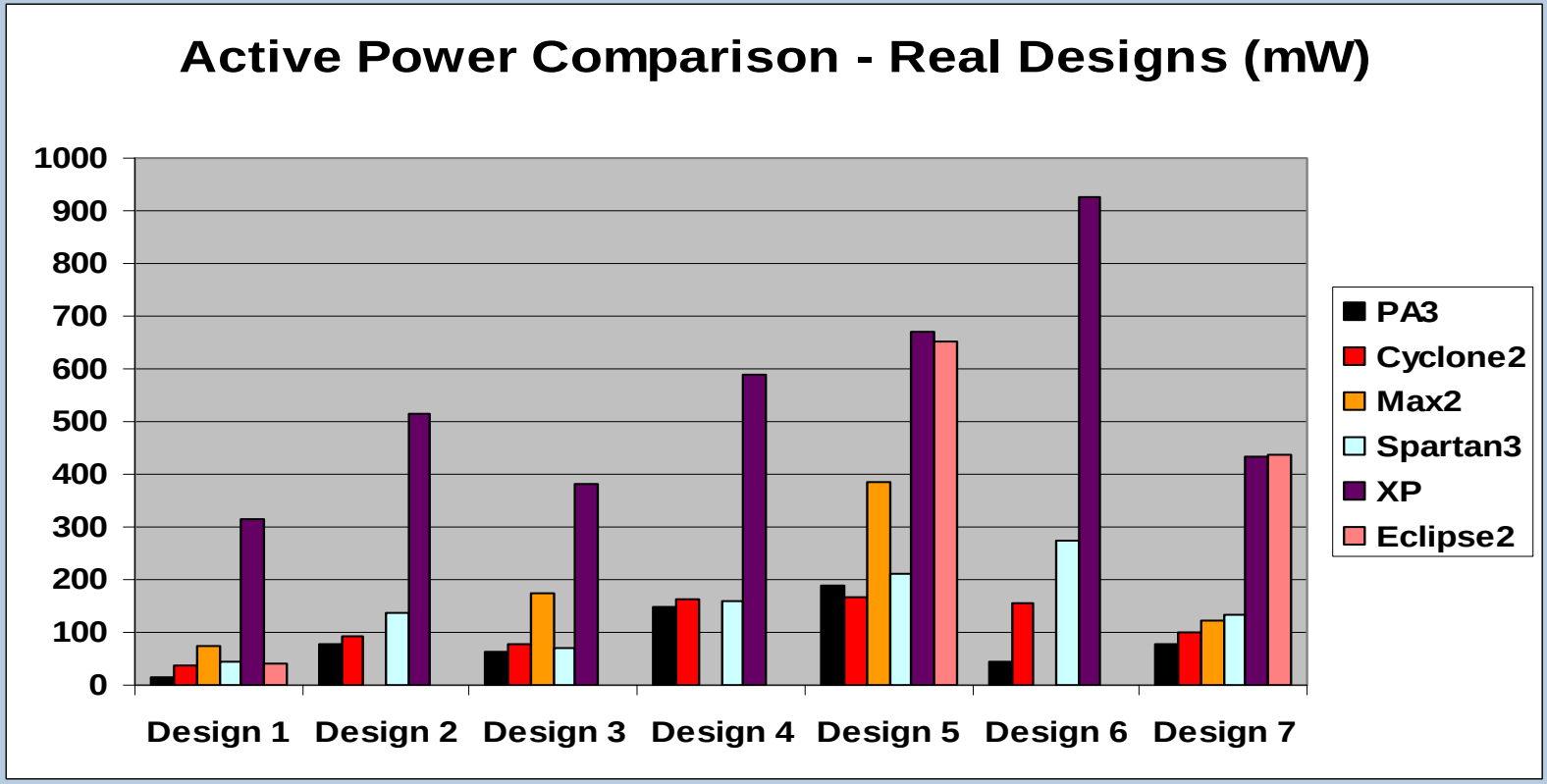


- Live At Power Up
  - **ProASIC3 aktiv innerhalb <10µs**
  - **SRAM Bausteine benötigen > 200 ms**

Statische Verlustleistung: Temperaturvergleich



Aktive Verlustleistung



Agenda

Abgrenzungsmerkmale

Firm Error

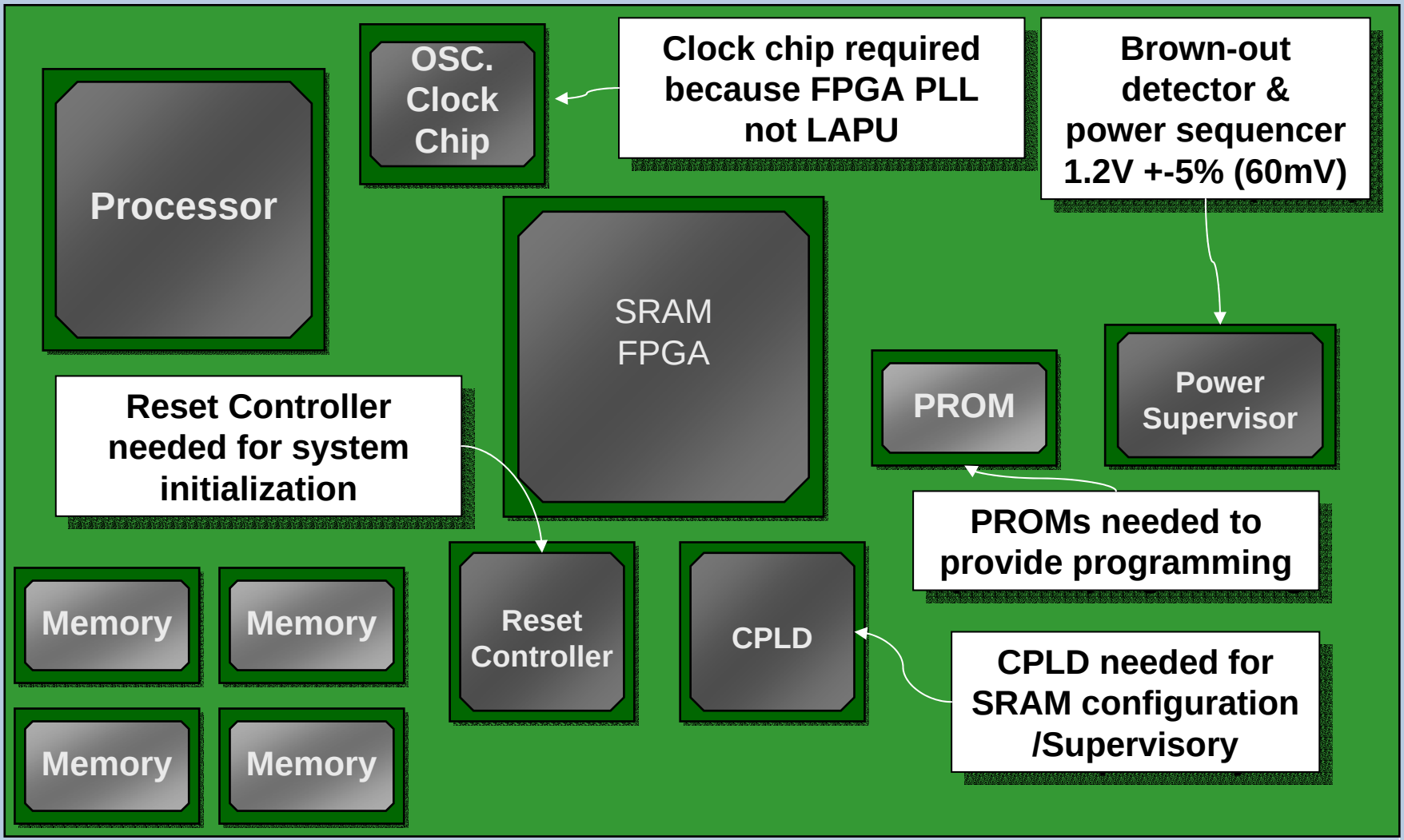
Kopierschutz

Leistungsaufnahme

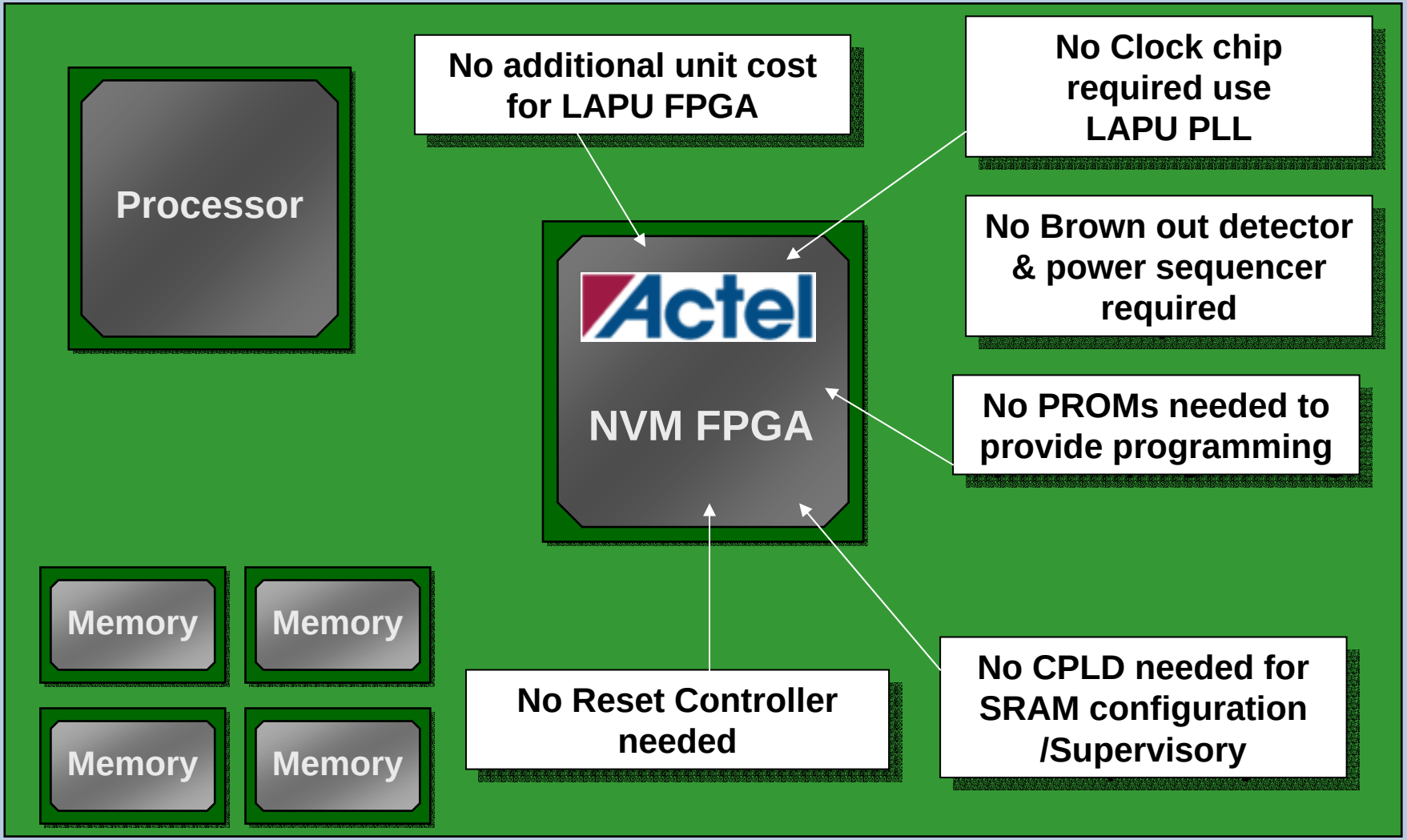
> Systemkosten

Zusammenfassung

System Kosten: SRAM FPGA



System Kostenost: NVM FPGA



Agenda

Abgrenzungsmerkmale

Firm Error

Kopierschutz

Leistungsaufnahme

Systemkosten

> Zusammenfassung

Zusammenfassung
Vorteile Flash und Antifuse

- **Firm Error Immun**
  - **Immun gegen Neutronen und Alpha Strahlung**
  - **Keine Firm Errors von iROC beobachtet**
- **Designschutz**
  - **Flash/Fuse-Lock: Verhindert Zugriff auf Baustein**
  - **AES: Konfigurationsdaten werden verschlüsselt**
- **Leistungsaufnahme**
  - **Geringer Einschaltstrom (<10mA) und statische Verlustleistung**
  - **Extrem geringer dynamischer Leistungsverbrauch bei Antifuse FPGA (Antifuse Switch < 25Ohm)**
- **Systemkosten**
  - **LAPU Eigenschaft benötigt keine weiteren Komponenten (Flash/EPROM, CPLD,..) und spart PCB Fläche**