Hochschule **RheinMain**
Design Informatik Medien

AUSWEG AUS DER ABHÄNGIGKEIT: MEHR DIGITALE SOUVERÄNITÄT MIT QUELLOFFENER HARDWARE?

Neue Wege für das Chipdesign

9. November 2023

Steffen Reith
Steffen.Reith@hs-rm.de

Theoretische Informatik
Hochschule **RheinMain**

EINLEITUNG

DIGITALE SOUVERÄNITÄT

Definition (CIO Bund)

„Digitale Souveränität“ beschreibt „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“

Quelle: **https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html**

DIGITALE SOUVERÄNITÄT

Definition (CIO Bund)

„Digitale Souveränität“ beschreibt „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“

Quelle: **https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html**

Wie soll (dort) **digitale Souveränität erreicht werden**?

- → Reduzierung der Abhängigkeiten von einzelnen Software-Anbietern
- → Studie zu Datenbankmanagementsystemen

DIGITALE SOUVERÄNITÄT

Definition (CIO Bund)

„Digitale Souveränität“ beschreibt „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“

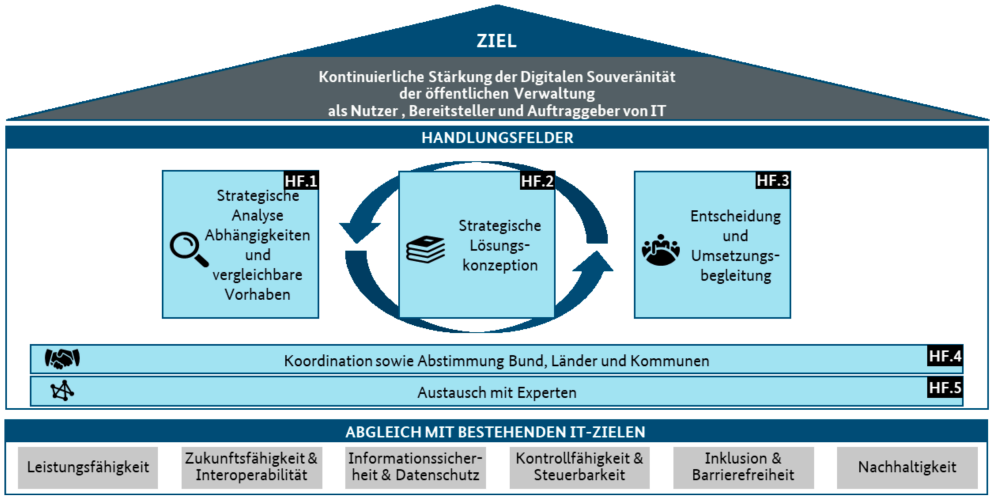
Quelle: **https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html**

Wie soll (dort) **digitale Souveränität erreicht werden**?

- → Reduzierung der Abhängigkeiten von einzelnen Software-Anbietern
- → Studie zu Datenbankmanagementsystemen

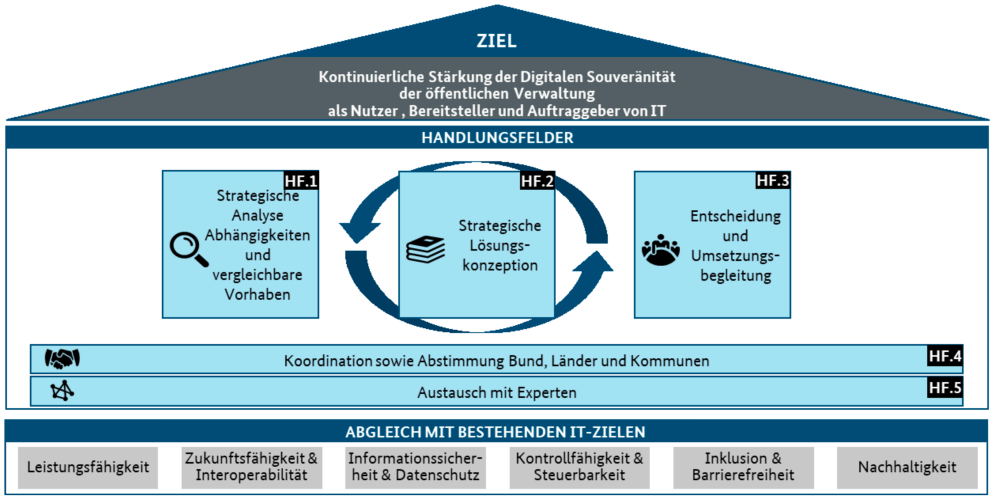
Meilensteine: Gründung des **Zentrums für Digitale Souveränität** (Open Source wichtig), Beginn der Umsetzung der **Deutschen Verwaltungscloud**

STÄRKUNG DER DIGITALEN SOUVERÄNITÄT



Quelle: Eckpunktepapier „Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung“, IT-Planungsrat, 2020

STÄRKUNG DER DIGITALEN SOUVERÄNITÄT



Quelle: Eckpunktepapier „Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung“, IT-Planungsrat, 2020

Bekannte Handlungsfelder (ohne Vollständigkeit / Wertung):

Software-Erstellung:	**Programmieren**, Mensch-Maschine-Schnittstellen, Testen
Safety & Security:	Sicherheitstechnologien, Kryptografie, **IT-Sicherheit** und Qualität von Software
Big-Data:	**Datenschutz**, Marktforschung (Persönlichkeitsprofile) und Gesundheit

SPRINGEN WIR ZU KURZ?

Cloud-Dienste:	Marktabschottung, **Datenmissbrauch** und Wettbewerbe
Mobile Computing:	**Netzwerksicherheit**, Fahrzeugelektronik und Wearable Computer
Künstliche Intelligenz:	Maschinelle Übersetzung, **Deepfakes**, selbstfahrende Fahrzeuge und autonome Waffen

SPRINGEN WIR ZU KURZ?

Cloud-Dienste:	Marktabschottung, **Datenmissbrauch** und Wettbewerbe
Mobile Computing:	**Netzwerksicherheit**, Fahrzeugelektronik und Wearable Computer
Künstliche Intelligenz:	Maschinelle Übersetzung, **Deepfakes**, selbstfahrende Fahrzeuge und autonome Waffen

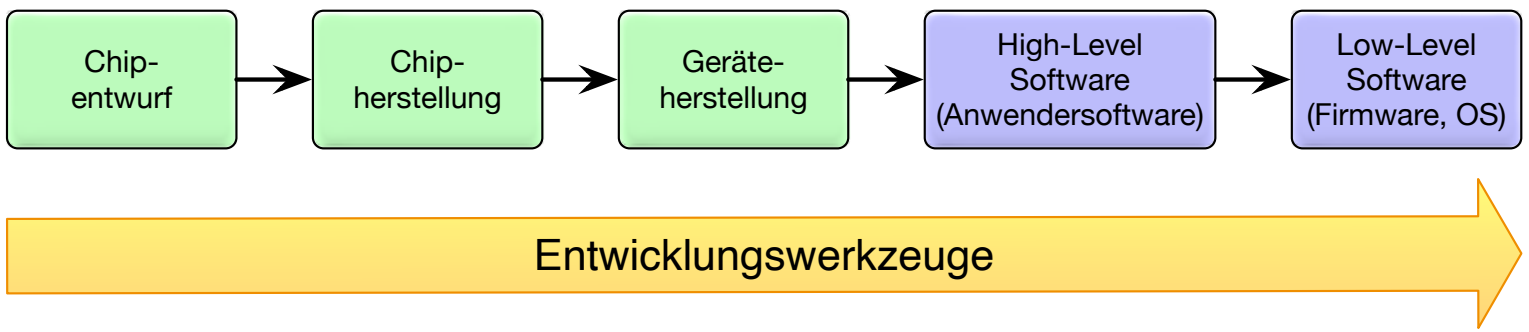
Die digitale Souveränität wird (gefühlt) nur als eine Art **erweiterte „Medienkompetenz“** gesehen.

SPRINGEN WIR ZU KURZ?

Cloud-Dienste:	Marktabschottung, **Datenmissbrauch** und Wettbewerbe
Mobile Computing:	**Netzwerksicherheit**, Fahrzeugelektronik und Wearable Computer
Künstliche Intelligenz:	Maschinelle Übersetzung, **Deepfakes**, selbstfahrende Fahrzeuge und autonome Waffen

Die digitale Souveränität wird (gefühlt) nur als eine Art **erweiterte „Medienkompetenz“** gesehen.

Eine weitere (meine?) Sichtweise:



Eine (extrem) vereinfachte IT-Wertschöpfungskette

SELBSTSTÄNDIG, SELBSTBESTIMMT UND SICHER

Um **digitale Souveränität zu erreichen** müssen wir **jeden Schritt** beherrschen und kontrollieren können!

SELBSTSTÄNDIG, SELBSTBESTIMMT UND SICHER

Um **digitale Souveränität zu erreichen** müssen wir **jeden Schritt** beherrschen und kontrollieren können!

Haben wir für jeden Schritt (noch) **ausreichend Kompetenzen** und **junge Leute**?

SELBSTSTÄNDIG, SELBSTBESTIMMT UND SICHER

Um **digitale Souveränität zu erreichen** müssen wir **jeden Schritt** beherrschen und kontrollieren können!

Haben wir für jeden Schritt (noch) **ausreichend Kompetenzen** und **junge Leute**?

Neben der eigentlichen Wertschöpfungskette müssen wir auch die **Entwicklungswerkzeuge** berücksichtigen, da sonst Hintertüren / Trojaner (automatisch) eingebaut werden können

> *Der Einsatz von **Open Source Software stärkt die Digitale Souveränität der Öffentlichen Verwaltung** entlang der drei eng verzahnten strategischen Ziele:*
>
> → *... Wechselmöglichkeit ...*
> → *... Gestaltungsfähigkeit ...*
> → *... Einfluss auf die Anbieter ...*

Quelle: **https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/zentrum-fuer-digitale-souveraenitaet/zentrum-fuer-digitale-souveraenitaet-node.html**

PROGENITOR

ZIELE

PROGENITOR wurde durch die Förderrichtlinie „**Cybersicherheitsforschung in Hessen**“ (HMdIS) ermöglicht und in Kooperation mit **Prof. Dr. Holger Hühnemohr** (HSRM) und der **HZD** durchgeführt.

Forschungsfrage

Kann man mit Hilfe von Open-Source Hardware und Open-Source Software einen kleinen VPN-Router (**Machbarkeitsstudie!**) für das Homeoffice bauen?

ZIELE

PROGENITOR wurde durch die Förderrichtlinie „**Cybersicherheitsforschung in Hessen**“ (HMdIS) ermöglicht und in Kooperation mit **Prof. Dr. Holger Hühnemohr** (HSRM) und der **HZD** durchgeführt.

Forschungsfrage

Kann man mit Hilfe von Open-Source Hardware und Open-Source Software einen kleinen VPN-Router (**Machbarkeitsstudie!**) für das Homeoffice bauen?

Vorgaben des Projekts:

- → **Keine** Produktion (für den **Massenmarkt**)
- → Marktfähiger **Preis kein Ziel** (geht es überhaupt?)
- → Möglichst viele **Komponenten** der Wertschöpfungskette **als Open-Source** (soweit möglich)
- → Nur **offene Entwicklungswerkzeuge** (soweit möglich)

CHIPENTWURF

Aktuell sind drei ISA (Instruction Set Architecture) breiter bekannt: **x86** (PCs), **ARM** (Mobiltelefone) und **RISC-V**

Achtung: x86 und ARM sind **von den Herstellern geschützt**!

[1] **https://github.com/SpinalHDL/VexRiscv**
[2] **https://github.com/enjoy-digital/litex**

CHIPENTWURF

Aktuell sind drei ISA (Instruction Set Architecture) breiter bekannt: **x86** (PCs), **ARM** (Mobiltelefone) und **RISC-V**

Achtung: x86 und ARM sind **von den Herstellern geschützt**!

Da weitere Werkzeuge und Software später notwendig:

verwende eine innovative **Open-Source Implementierung** von **RISC-V** (Vexriscv[1])

Ein Computersystem ist **viel mehr als eine CPU**. Benötigen Schnittstellen (z.B. **Ethernet**, USB, Massenspeicher) und die Ansteuerung von **Arbeitsspeicher** (DRAM):

verwende LiteX[2] ein **SoC builder framework**

[1] **https://github.com/SpinalHDL/VexRiscv**
[2] **https://github.com/enjoy-digital/litex**

CHIPENTWURF - FAZIT

Mit Open-Source Hardware kann ein **lauffähiges Computersystem entwickelt** werden!

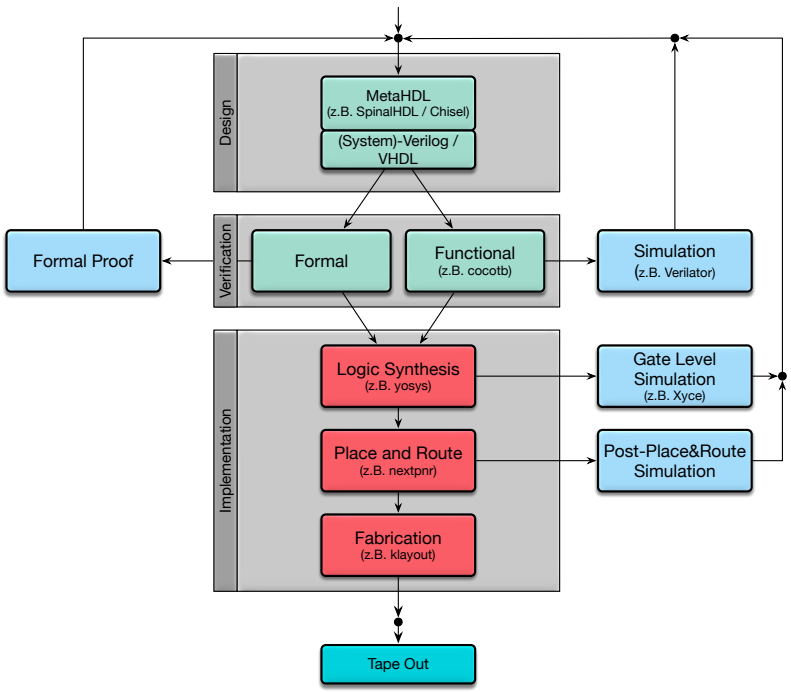
CHIPENTWURF - FAZIT

Mit Open-Source Hardware kann ein **lauffähiges Computersystem entwickelt** werden!

Aber: „**There is no free lunch**!“ (Ethernet, DRAM)

Viele Schritte der Chipentwicklung für **einfache Systeme** können mit Open-Source Werkzeugen durchgeführt werden.

Die Synthese für die verbreiteten FPGAs von Xilinx/AMD noch in sehr frühen Stadium. PROGENITOR verwendet ein **propritäres Tool** (Vivado)!



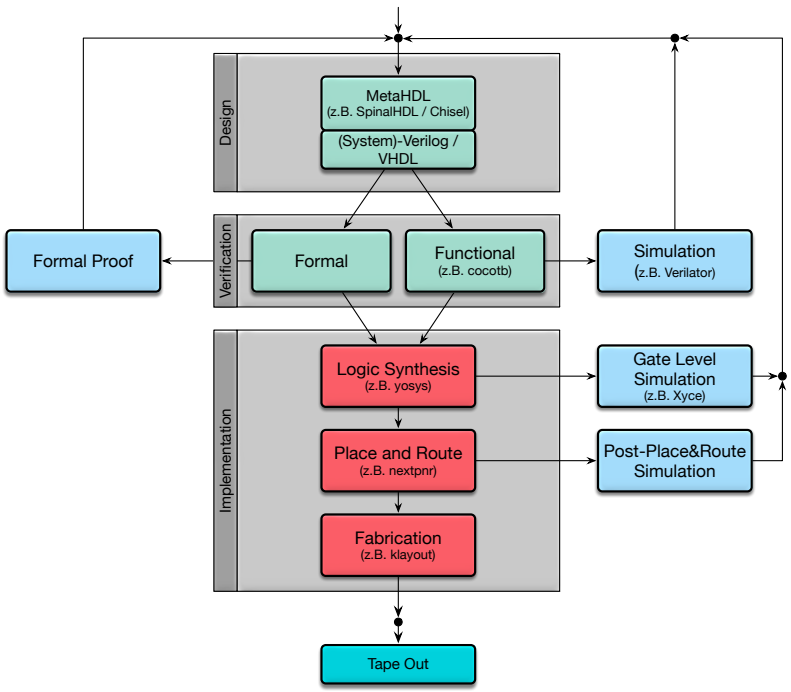
CHIPENTWURF - FAZIT

Mit Open-Source Hardware kann ein **lauffähiges Computersystem entwickelt** werden!

Aber: „**There is no free lunch**!“ (Ethernet, DRAM)

Viele Schritte der Chipentwicklung für **einfache Systeme** können mit Open-Source Werkzeugen durchgeführt werden.

Die Synthese für die verbreiteten FPGAs von Xilinx/AMD noch in sehr frühen Stadium. PROGENITOR verwendet ein **propritäres Tool** (Vivado)!



CHIPHERSTELLUNG

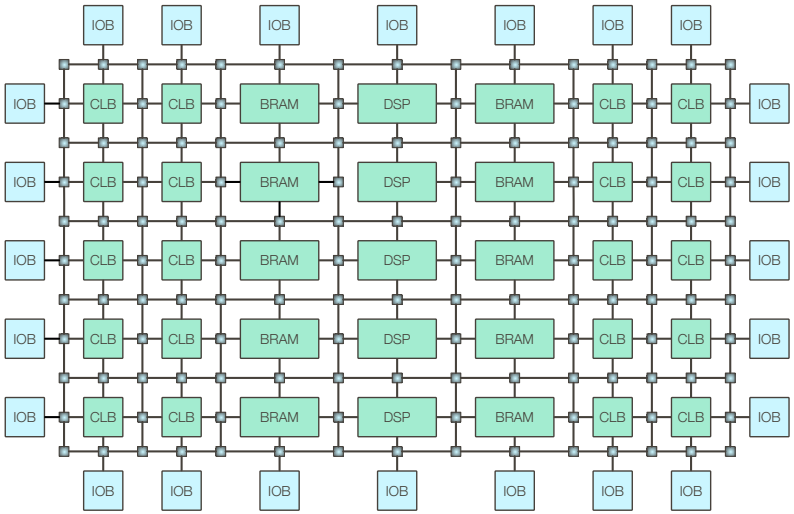
Zum **Projektstart** konnte in Deutschland **kein Open-Source** Chip (ASIC) produziert werden. Es ist noch unklar, ob die nun verfügbare Technologie leistungsfähig genug für einen VPN-Router ist:

Frühe Entscheidung: **Verwenden ein FPGA** (frei konfigurierbarer Logikbaustein / Rapid Prototyping)

CHIPHERSTELLUNG

Zum **Projektstart** konnte in Deutschland **kein Open-Source** Chip (ASIC) produziert werden. Es ist noch unklar, ob die nun verfügbare Technologie leistungsfähig genug für einen VPN-Router ist:

Frühe Entscheidung: **Verwenden ein FPGA** (frei konfigurierbarer Logikbaustein / Rapid Prototyping)



Struktur eines FPGA

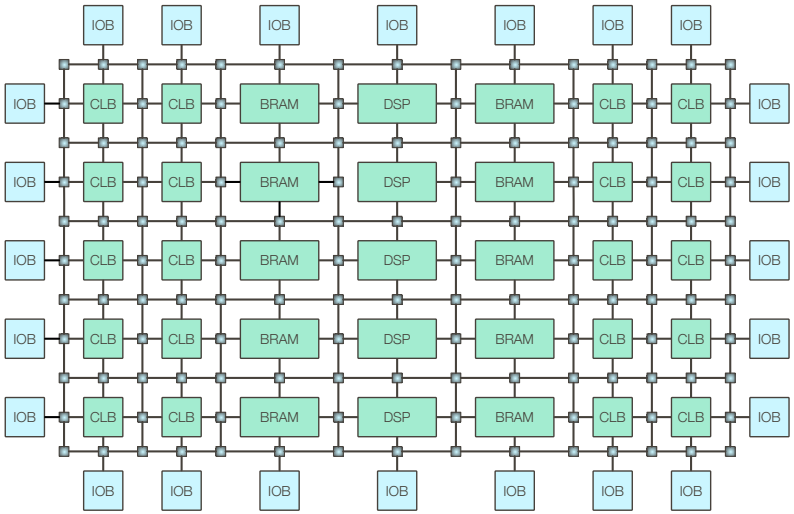
Schwierige Liefersituation

(Aktuell: Possible to order, delivery time on request)

CHIPHERSTELLUNG

Zum **Projektstart** konnte in Deutschland **kein Open-Source** Chip (ASIC) produziert werden. Es ist noch unklar, ob die nun verfügbare Technologie leistungsfähig genug für einen VPN-Router ist:

Frühe Entscheidung: **Verwenden ein FPGA** (frei konfigurierbarer Logikbaustein / Rapid Prototyping)



Struktur eines FPGA

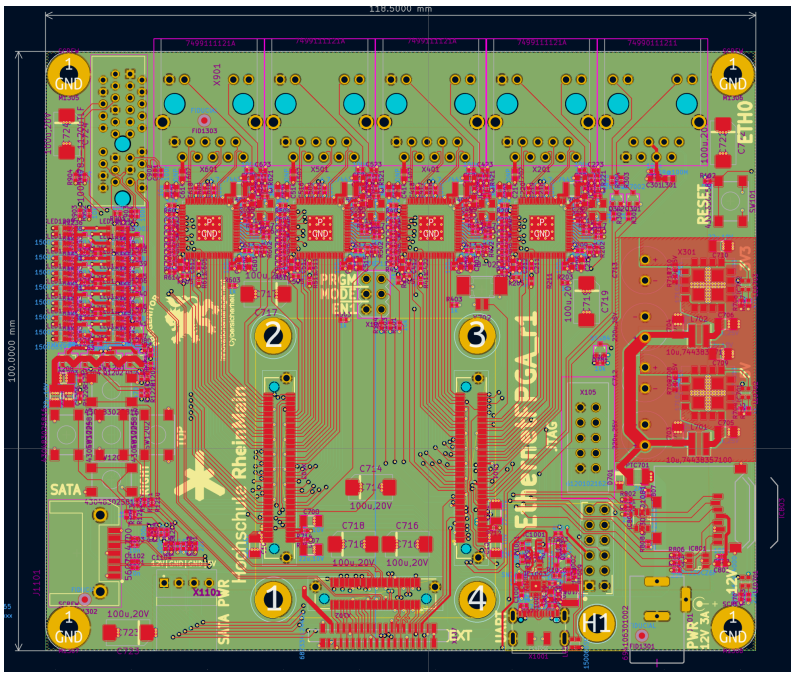
Schwierige Liefersituation

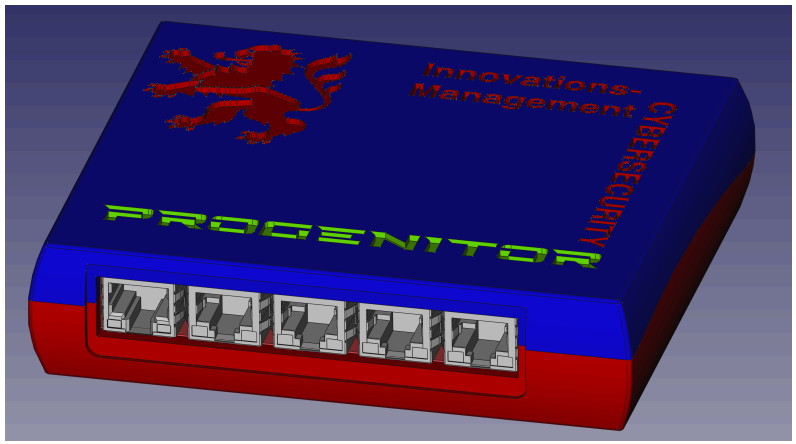
(Aktuell: Possible to order, delivery time on request)

Die Forschung an **Open-Source Hardware** ist ein **essenzieller Baustein für mehr digitale Souveränität**!

GERÄTEHERSTELLUNG

Für das Platinenlayout existiert das komfortable Open-Source Tool **KiCAD**[3] mit aktiver Nutzer- und Entwicklergemeinde und für das Gehäuse ein quelloffenes CAD-Programm **FreeCAD**[4]:





[3] **https://www.kicad.org/**
[4] **https://www.freecad.org**

LOW-LEVEL SOFTWARE

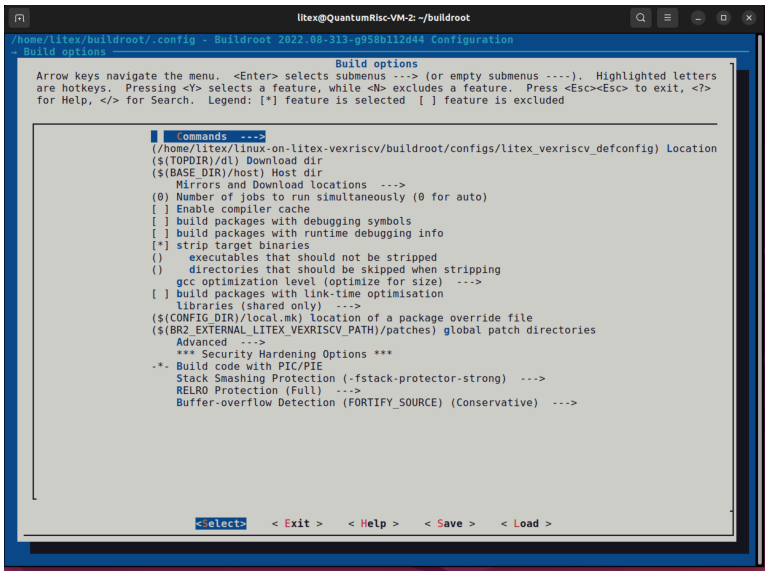
Eine Anpassung von **OpenWRT** (Linux-Distribution für eingebettete Systeme / Router) an RISC-V war aufgrund technischer Probleme **nicht möglich**.

[5] **https://buildroot.org/**

LOW-LEVEL SOFTWARE

Eine Anpassung von **OpenWRT** (Linux-Distribution für eingebettete Systeme / Router) an RISC-V war aufgrund technischer Probleme **nicht möglich**.

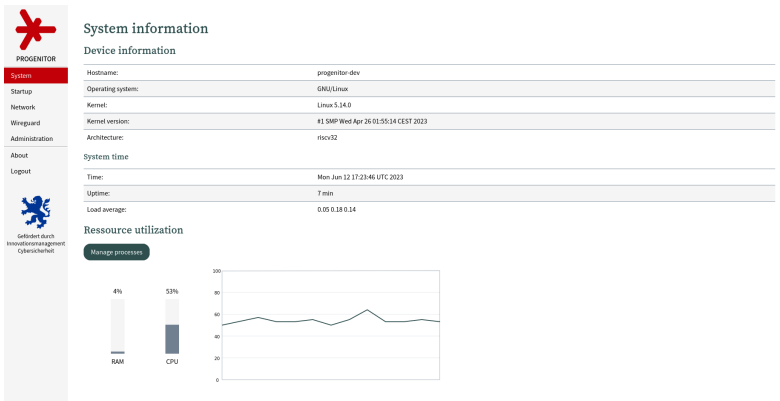
Ausweg: Als Basissoftware kann ein RISC-V Port von Linux mit der Softwaredistribution **buildroot**[5] verwendet werden.

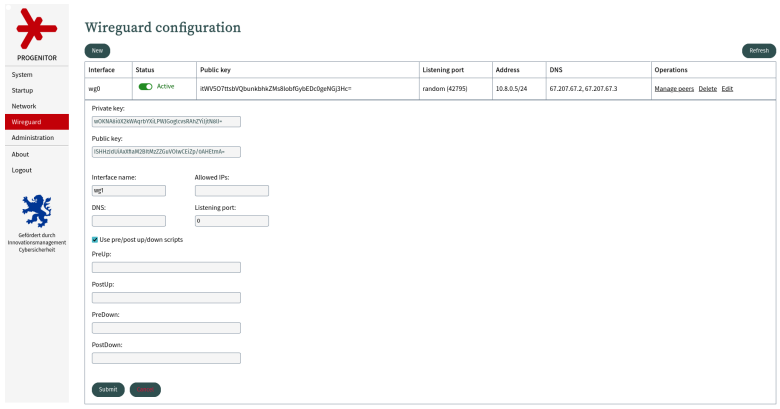


[5] **https://buildroot.org/**

HIGH-LEVEL SOFTWARE

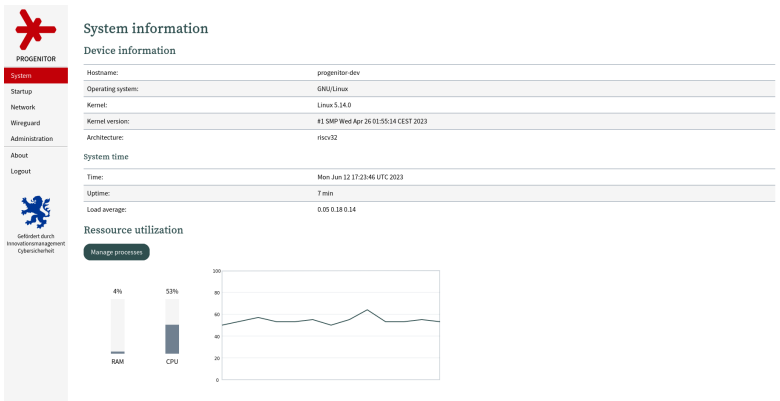
Die Entwicklung einer **Web-basierten Benutzeroberfläche** für den VPN-Router mit Wireguard ist mit dem RISC-V/Linux-Softwarestack eine „Routineaufgabe“:

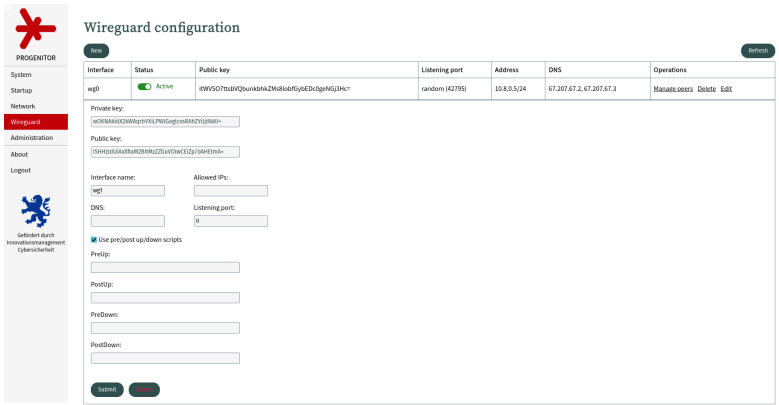




HIGH-LEVEL SOFTWARE

Die Entwicklung einer **Web-basierten Benutzeroberfläche** für den VPN-Router mit Wireguard ist mit dem RISC-V/Linux-Softwarestack eine „Routineaufgabe“:

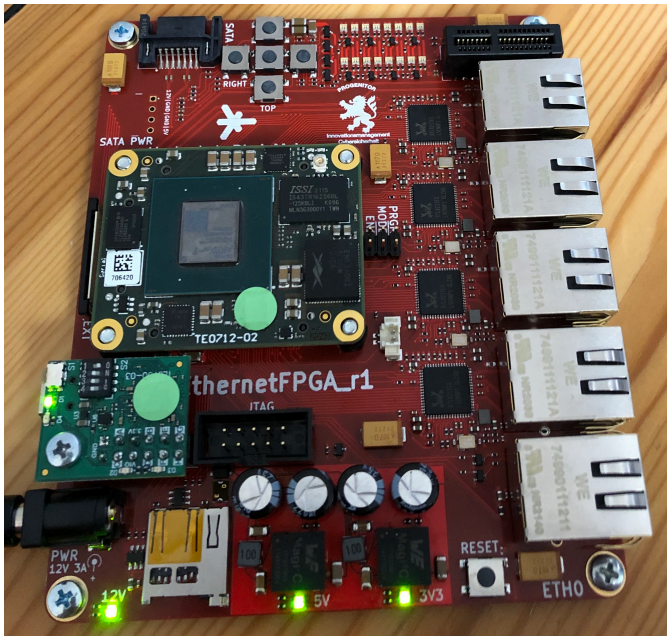


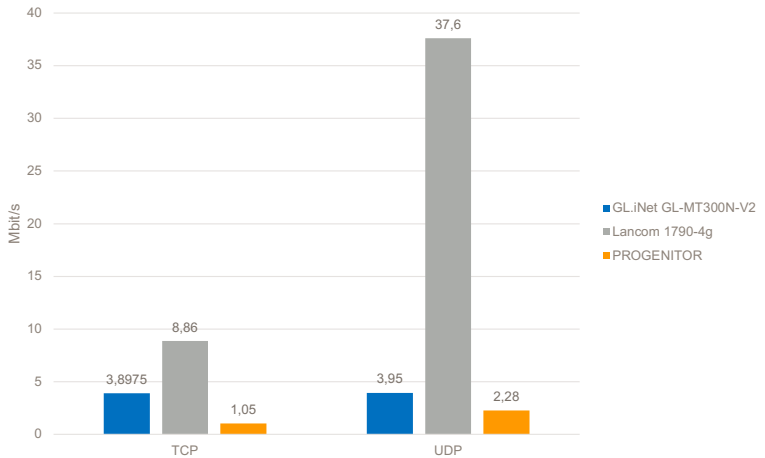


Ein **leistungsschwaches** und **teueres** aber **nützliches System** kann schon **heute** mit **Open-Source Hardware entwickelt** werden!

YOU HAVE CHOSEN THE RED PILL! WELCOME TO THE REAL WORLD!

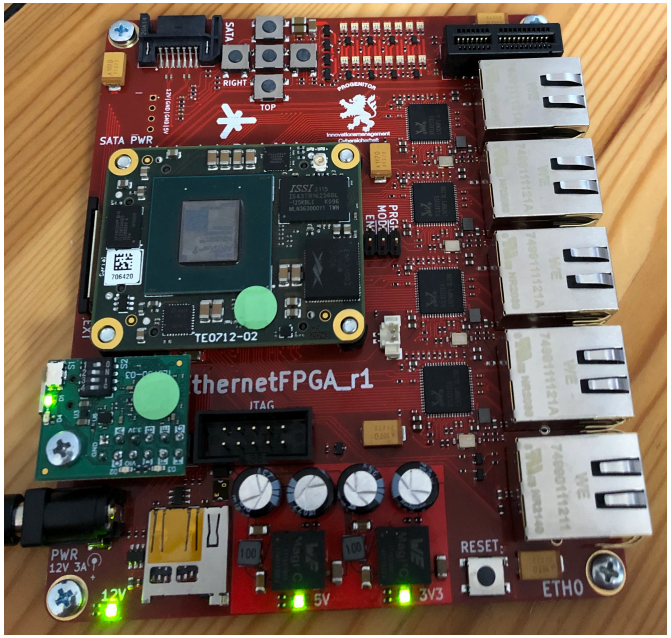
Die praktische Realisierung ermöglicht Messungen:

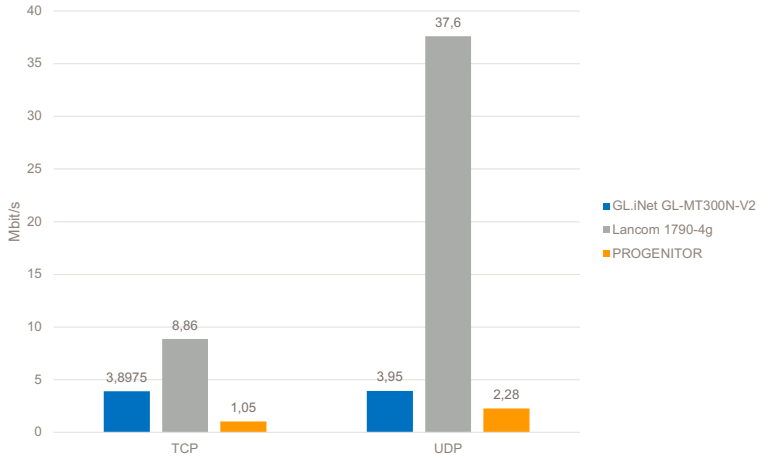




YOU HAVE CHOSEN THE RED PILL! WELCOME TO THE REAL WORLD!

Die praktische Realisierung ermöglicht Messungen:





PROGENITOR ist langsam, aber ein **vollständiger VPN-Router** der **ausschließlich mit Open-Source** Prinzipen realisiert wurde. Die Synthesetools für Xilinx/AMD sind schon jetzt ersetzbar!

Nächstes Ziel: Ersetzen des FPGAs durch einen **ASIC**

VE-HEP

DIFFICULT TO SEE. ALWAYS IN MOTION IS THE FUTURE.

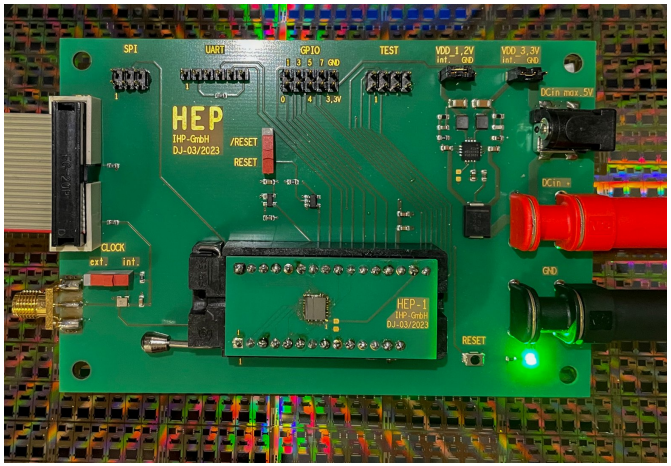
Das BMBF-geförderte Projekt **VE-HEP**[6] entwickelt ein **RISC-V basiertes Sicherheitsmodul**[7] (TPM). Erste erfolgreiche Version in 130nm. Gefertigt in Frankfurt (Oder).

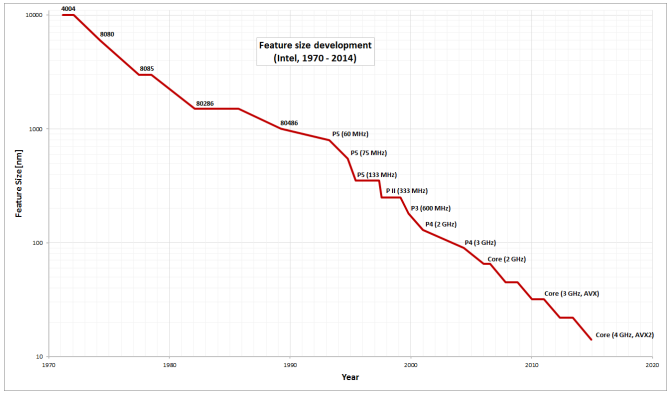
[6] **https://hep-alliance.org/**

[7] **https://www.ihp-microelectronics.com/fileadmin/user_upload/PM_2021-14-04_Project_HEP_EN.pdf**

DIFFICULT TO SEE. ALWAYS IN MOTION IS THE FUTURE.

Das BMBF-geförderte Projekt **VE-HEP**[6] entwickelt ein **RISC-V basiertes Sicherheitsmodul**[7] (TPM). Erste erfolgreiche Version in 130nm. Gefertigt in Frankfurt (Oder).





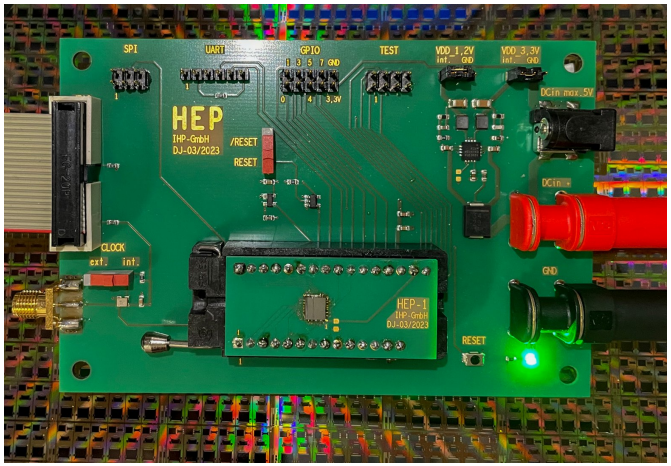
Feature size development (Intel 1970 - 2014) Frank Klemm, Wikipedia, CC BY-SA 3.0, 2014

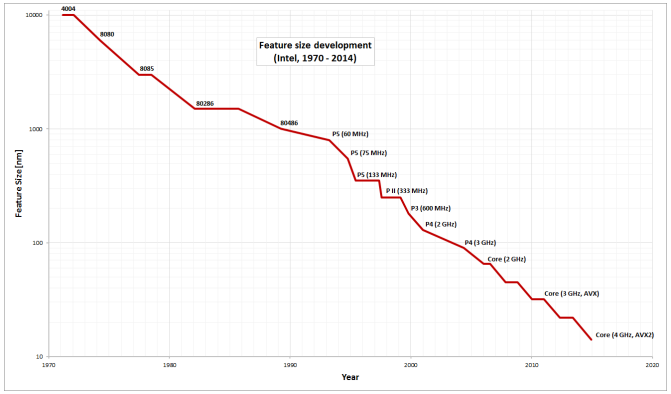
[6] **https://hep-alliance.org/**

[7] **https://www.ihp-microelectronics.com/fileadmin/user_upload/PM_2021-14-04_Project_HEP_EN.pdf**

DIFFICULT TO SEE. ALWAYS IN MOTION IS THE FUTURE.

Das BMBF-geförderte Projekt **VE-HEP**[6] entwickelt ein **RISC-V basiertes Sicherheitsmodul**[7] (TPM). Erste erfolgreiche Version in 130nm. Gefertigt in Frankfurt (Oder).





Feature size development (Intel 1970 - 2014) Frank Klemm, Wikipedia, CC BY-SA 3.0, 2014

Vergleich zu **Pentium III**: Launched February 28, 1999, Discontinued April 2004, Feature size 250 nm to 130 nm, Clock 400 MHz to 1.4 GHz

[6] **https://hep-alliance.org/**

[7] **https://www.ihp-microelectronics.com/fileadmin/user_upload/PM_2021-14-04_Project_HEP_EN.pdf**

THIS IS THE WAY

Takeaway 1

Ohne die vollständige **Kontrolle der Hardware** ist **digitale Souveränität** nicht möglich!

THIS IS THE WAY

Takeaway 1

Ohne die vollständige **Kontrolle der Hardware** ist **digitale Souveränität** nicht möglich!

Takeaway 2

Wir müssen **junge Leute** fördern, denn sie werden den Wandel gestalten!

THIS IS THE WAY

Takeaway 1

Ohne die vollständige **Kontrolle der Hardware** ist **digitale Souveränität** nicht möglich!

Takeaway 2

Wir müssen **junge Leute** fördern, denn sie werden den Wandel gestalten!

Takeaway 3

Langfristige substantielle Anstrengungen für **leistungsfähige** Systeme sind **notwendig**!

ENDE

Vielen Dank!