COPACOBANA and Upcoming Architectures for Cryptanalysis

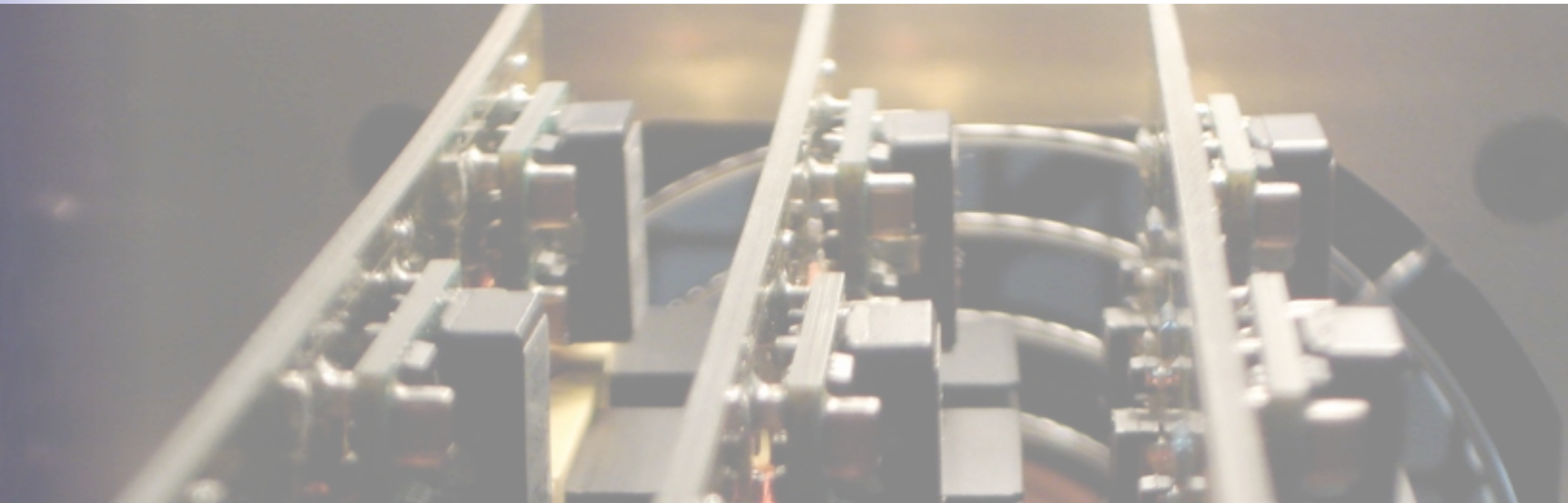
Department for Computer Science,
Christian-Albrechts-University of Kiel

Stefan Baumgart

For Workshop on Factoring Large Integers

Introduction

- About us
- Motivation
- Todays Approaches
- Our Approach
- Conclusion and Comments



Motivation: Academic Joint Venture

SHARCS 2005, Paris

Special-purpose Hardware for Attacking Cryptographic Systems

Motivation: Academic Joint Venture

SHARCS 2005, Paris

Special-purpose Hardware for Attacking Cryptographic Systems

Idea:

To break DES in less than

< 30 days	time
< 10.000,- US$	material costs

Motivation: Academic Joint Venture

SHARCS 2005, Paris

Special-purpose Hardware for Attacking Cryptographic Systems

Idea:

To break DES in less than

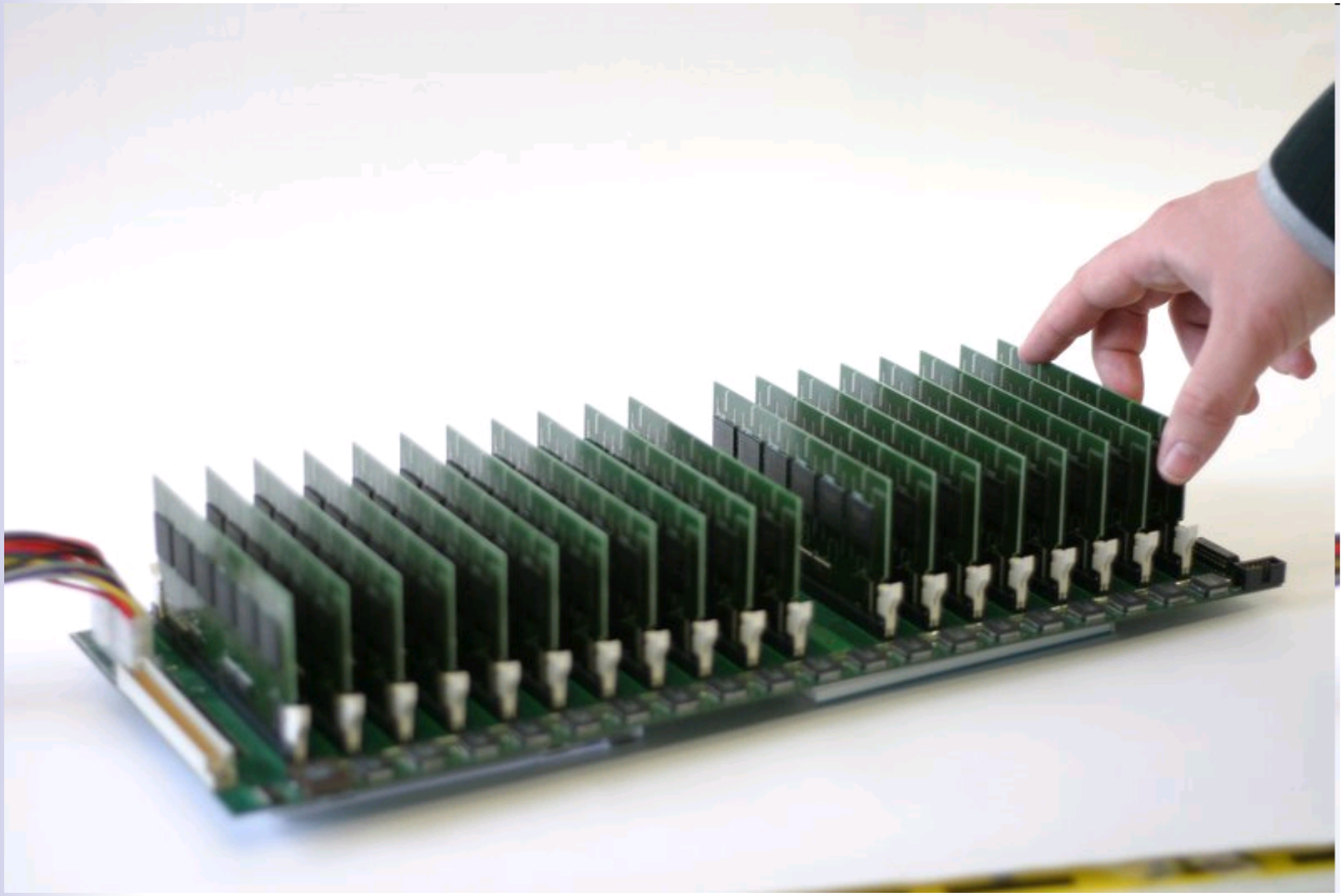
< 30 days	time
< 10.000,- US$	material costs

Team:

2 groups of the universities

- Bochum
- Kiel

Motivation: Academic Joint Venture



<u>Team:</u>

2 groups of the universities

- Bochum
- Kiel

infrastructure

Basic Design Problems

infrastructure

number of nodes

B.

A.

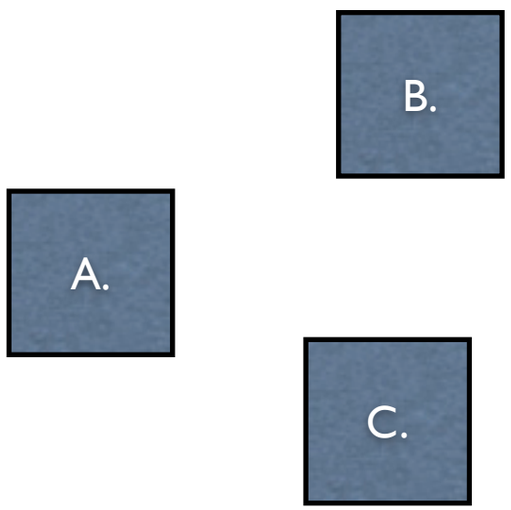
C.

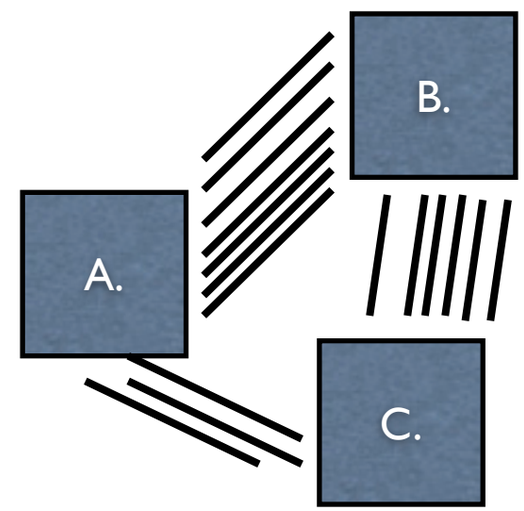
Basic Design Problems

infrastructure

number of nodes

number of connections

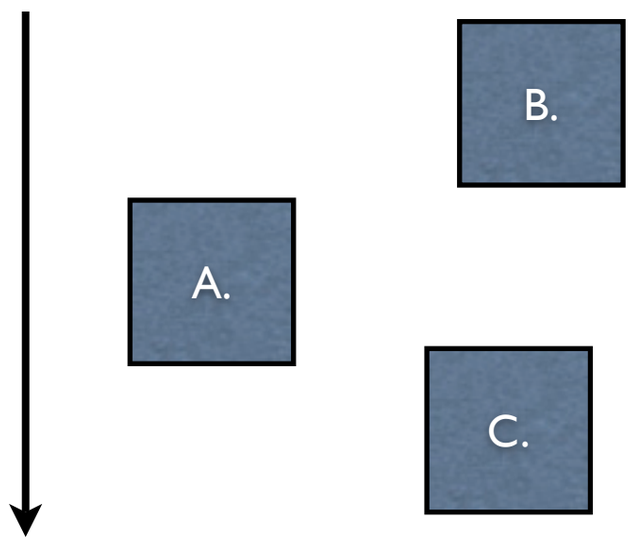




Basic Design Problems

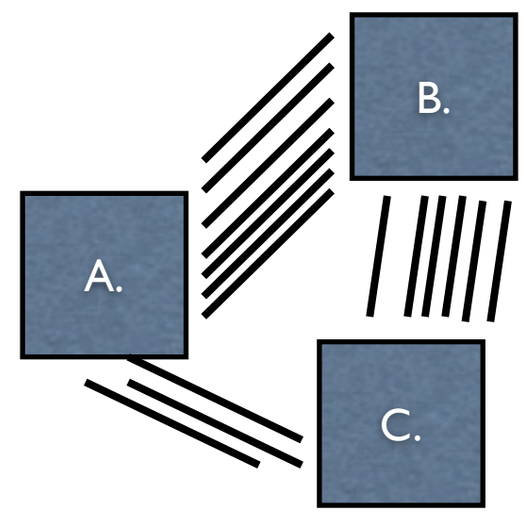
infrastructure

number of nodes



size of the pcb

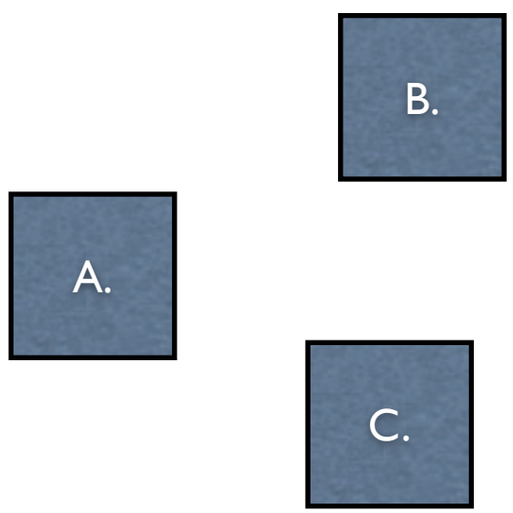
number of connections



Basic Design Problems

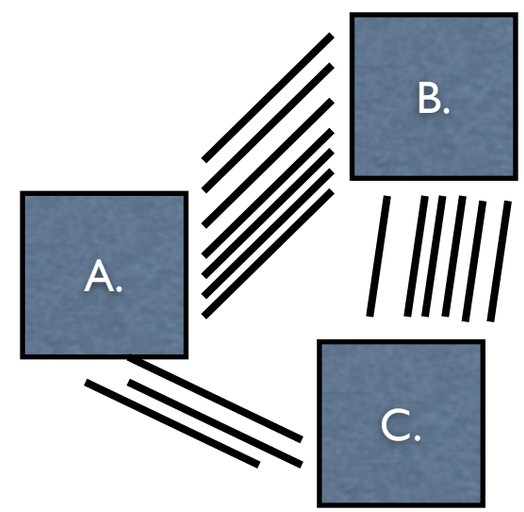
infrastructure

number of nodes



size of the pcb

number of connections

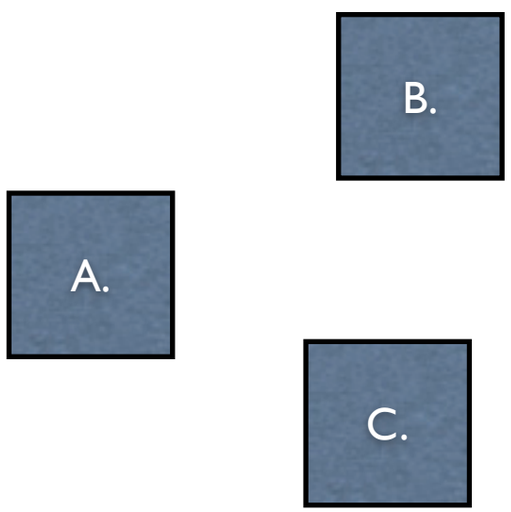


number of layers of a pcb

Basic Design Problems

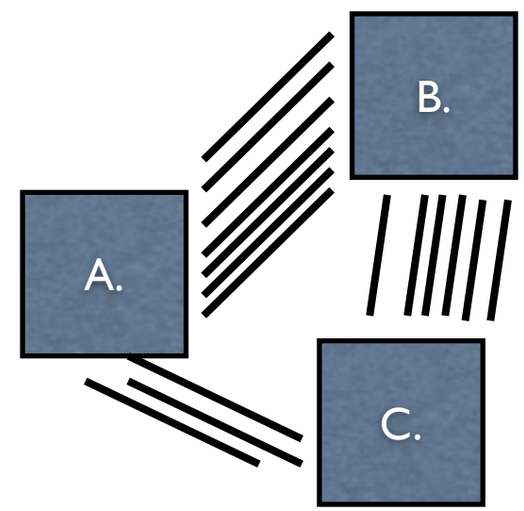
infrastructure

number of nodes



size of the pcb

number of connections



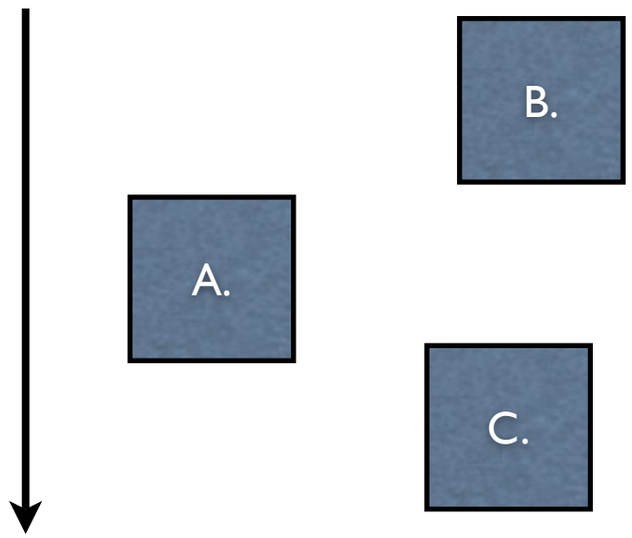
number of layers of a pcb

seems to be a graph problem

Basic Design Problems

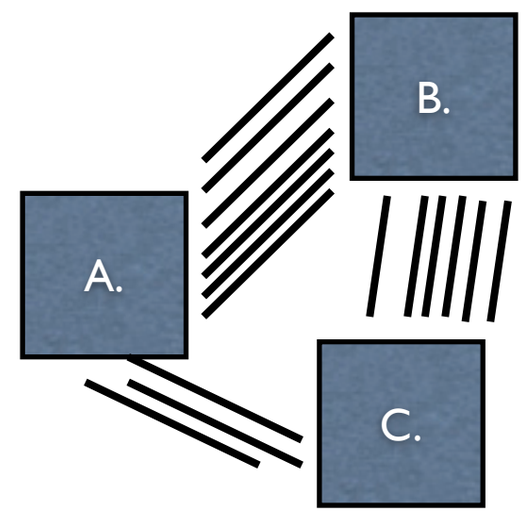
infrastructure

number of nodes



size of the pcb

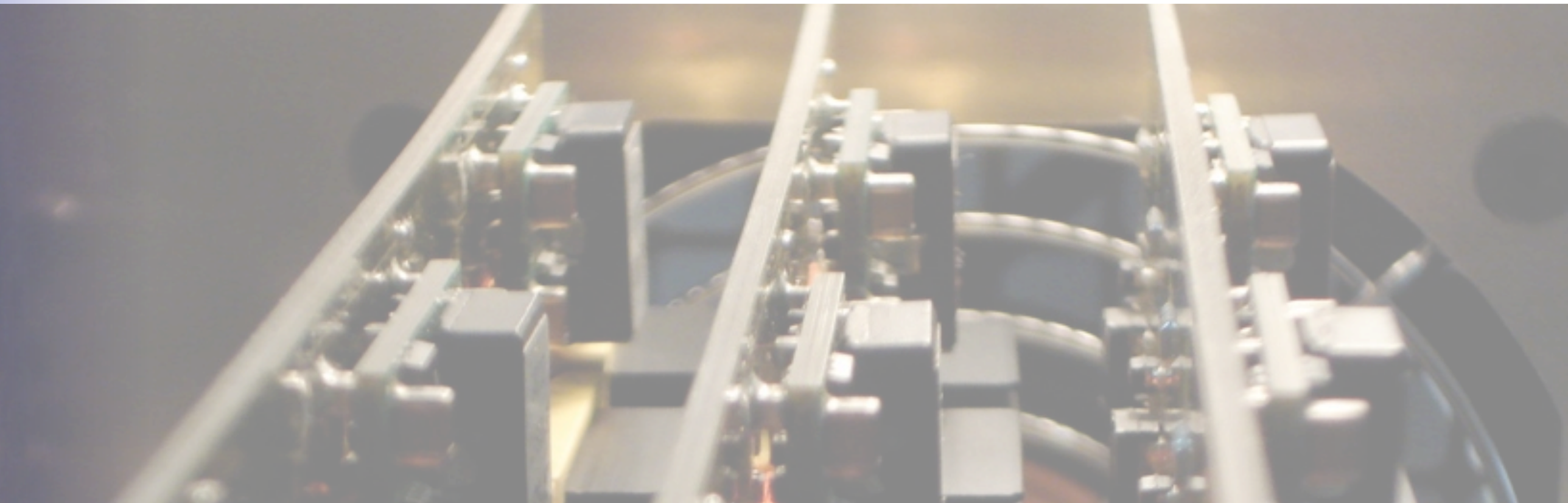
number of connections



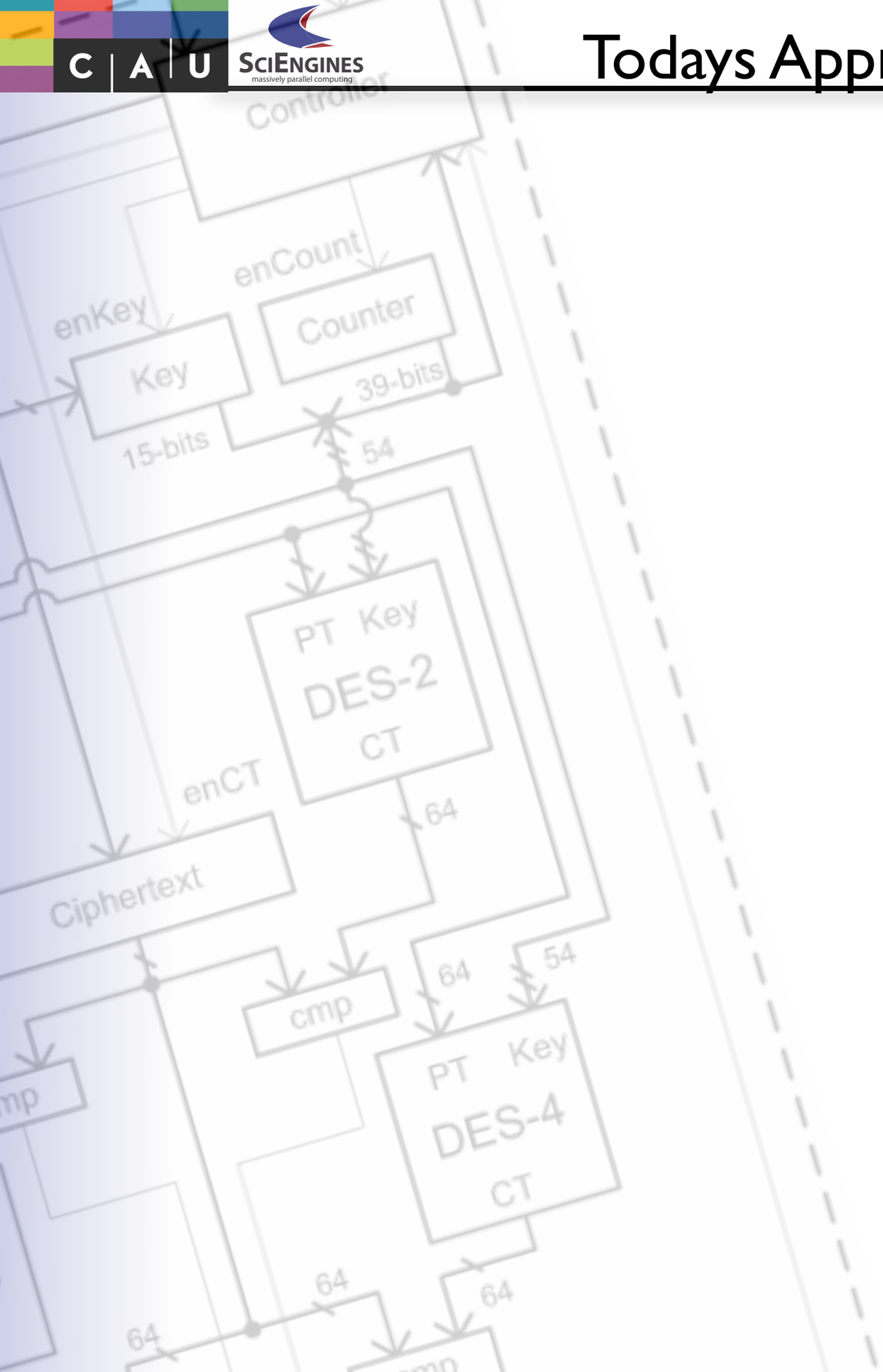
number of layers of a pcb

can it be produced and driven

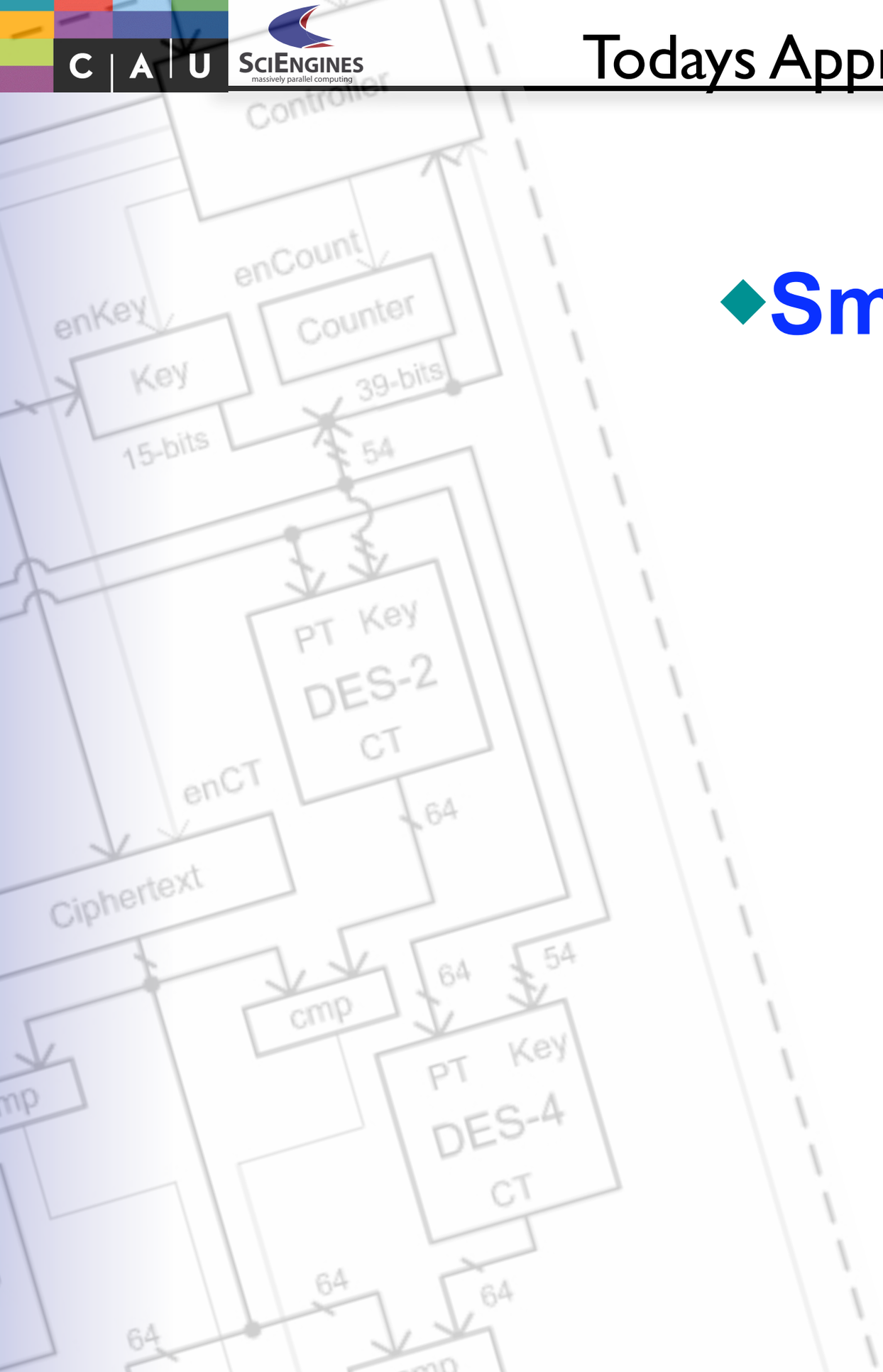
- About us
- Motivation
- **Todays Approaches**
- **Our Approach**
- **Conclusion and Comments**



Todays Approaches

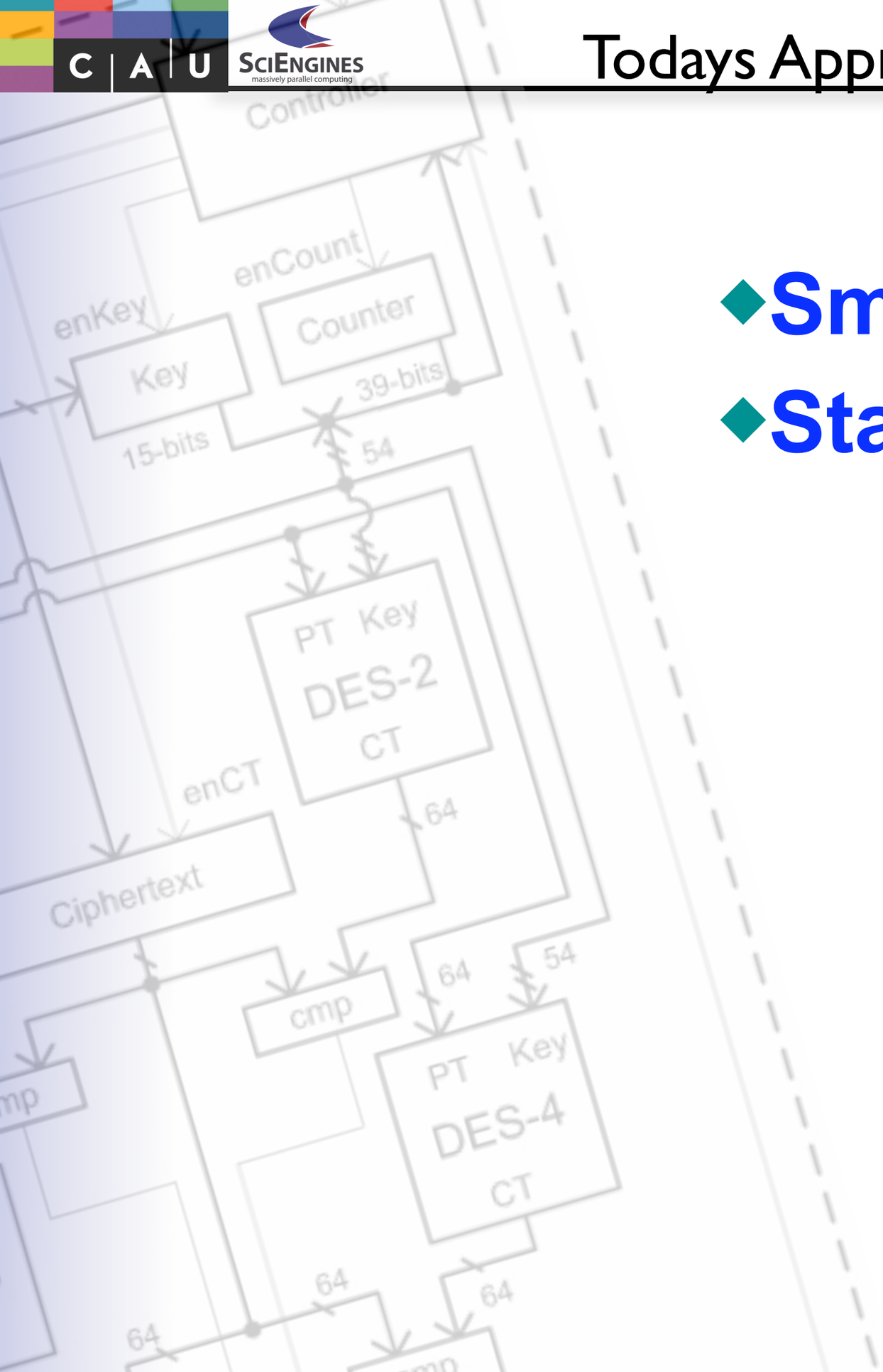


Todays Approaches



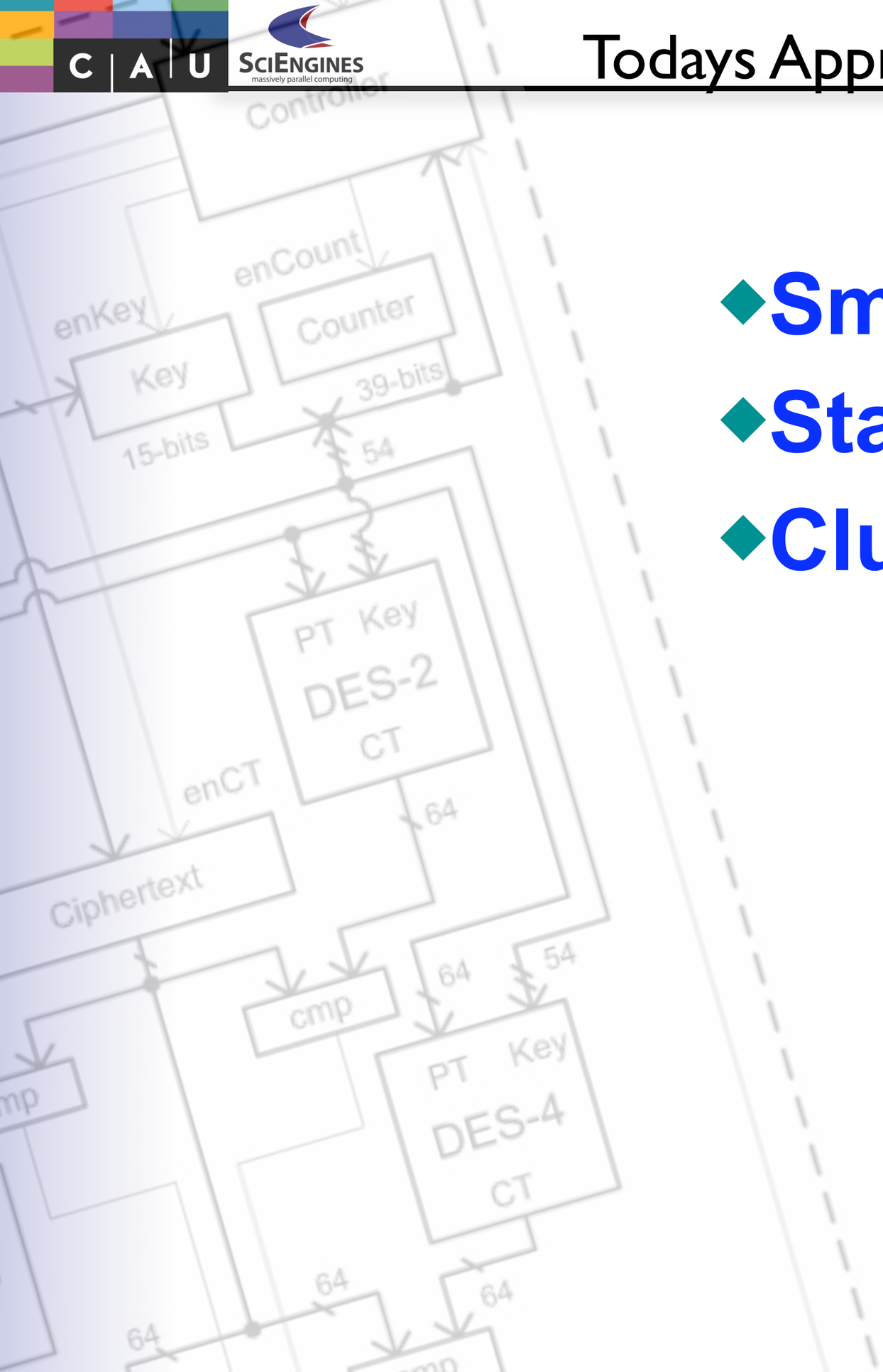
- **Smart Brains**

Todays Approaches



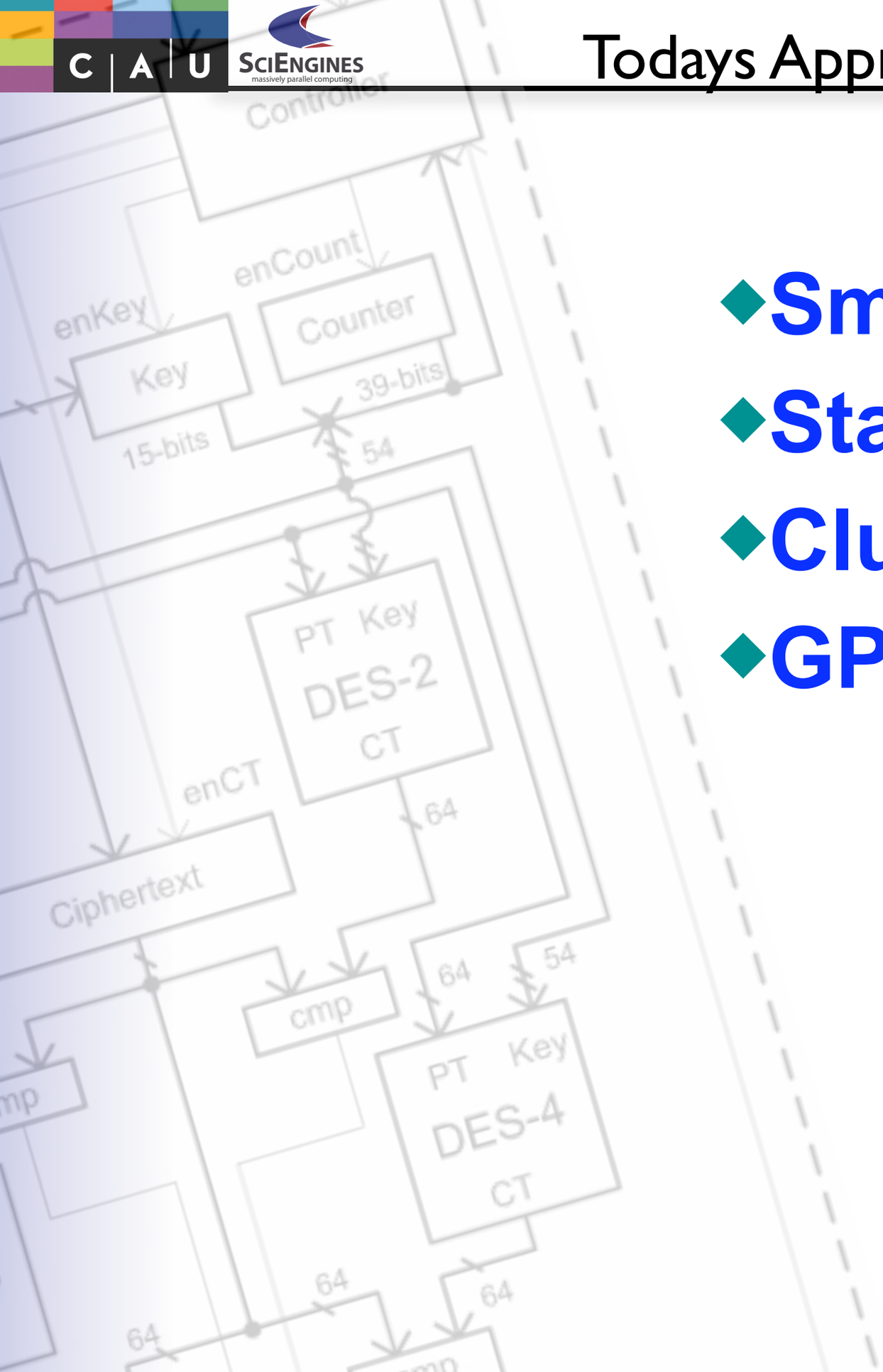
- **Smart Brains**
- **Standard PCs**

Todays Approaches



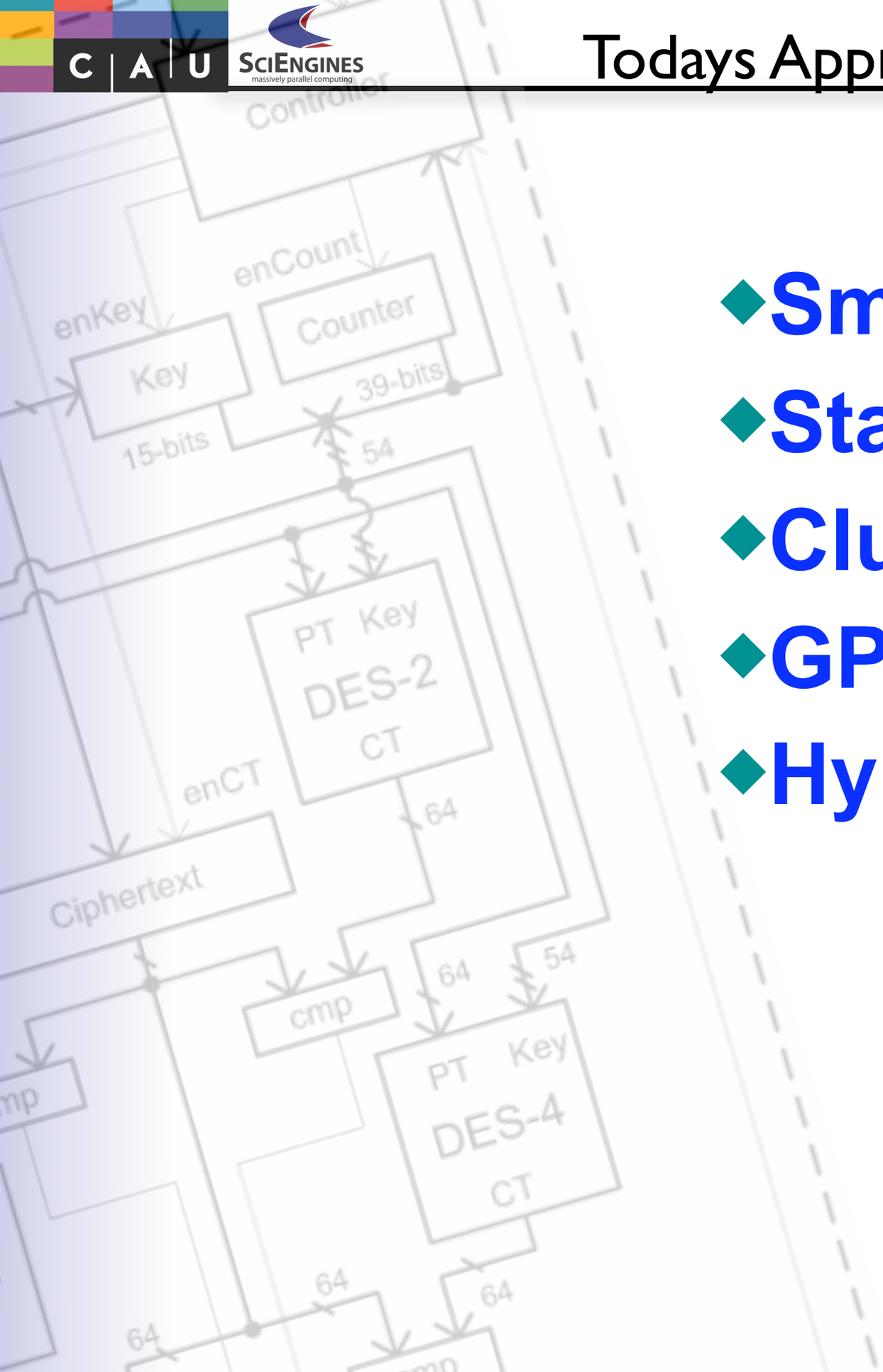
- **Smart Brains**
- **Standard PCs**
- **Cluster**

Todays Approaches



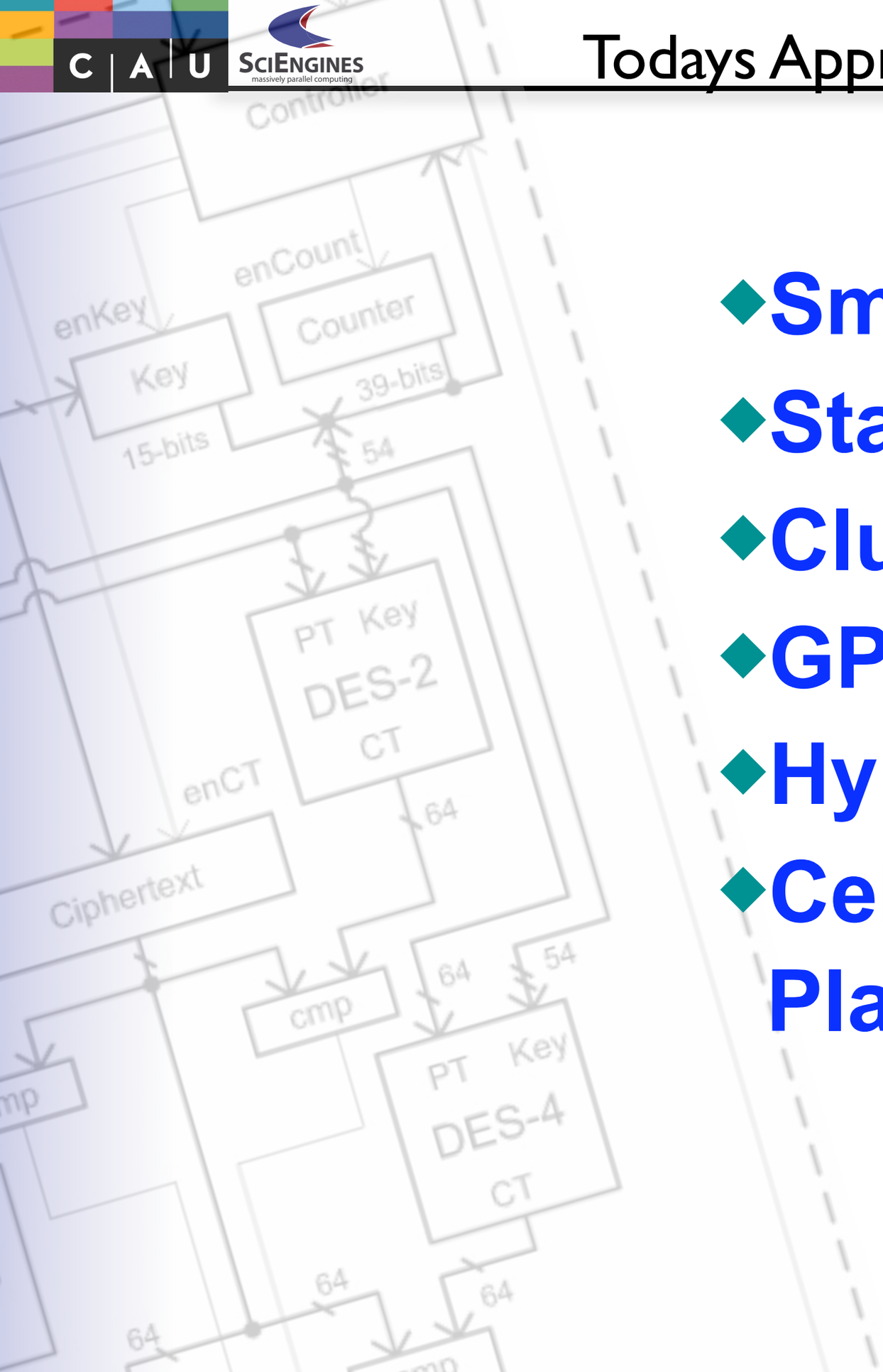
- Smart Brains
- Standard PCs
- Cluster
- GPUs

Todays Approaches



- Smart Brains
- Standard PCs
- Cluster
- GPUs
- Hybrid-Cluster

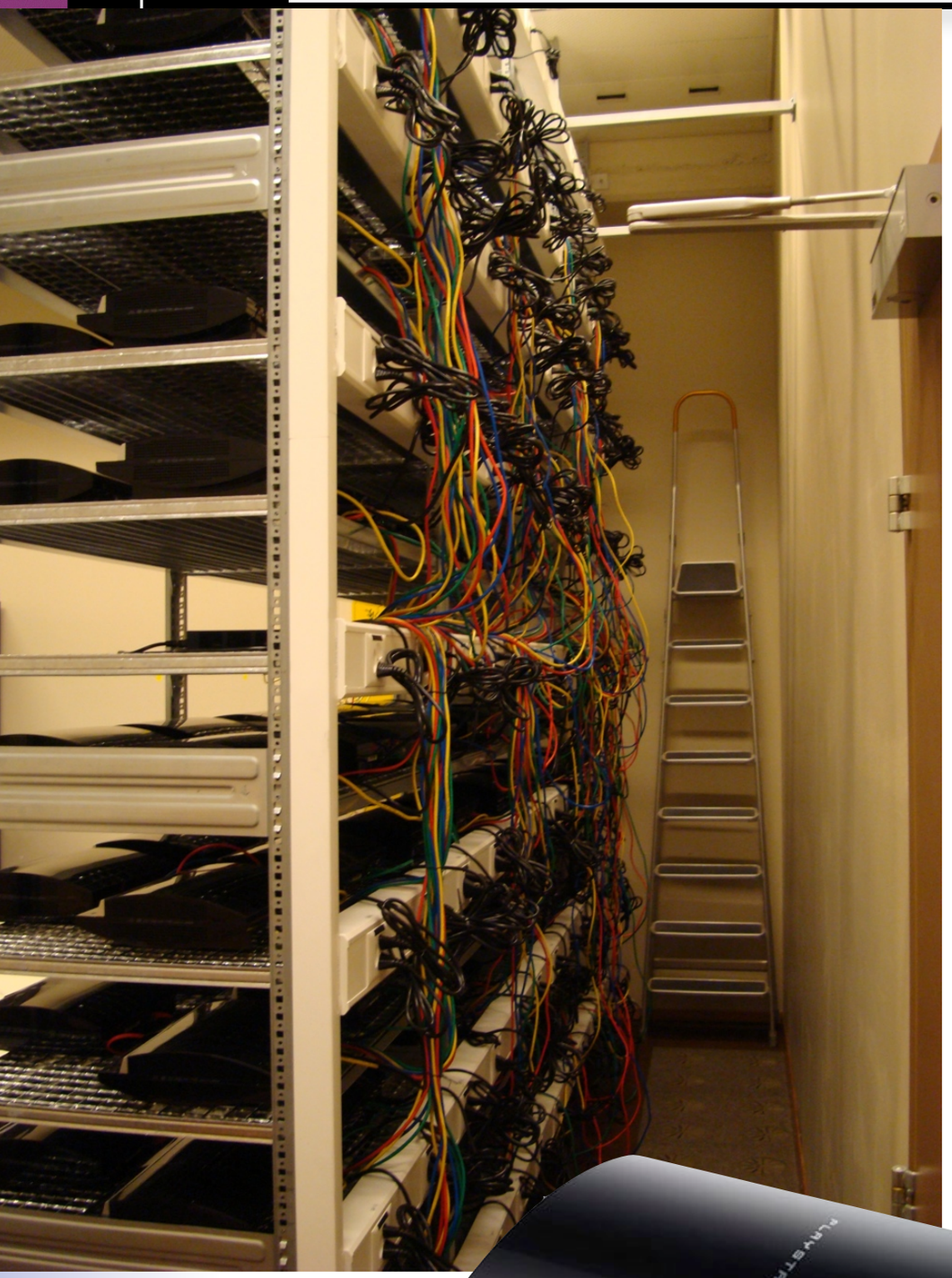
Todays Approaches

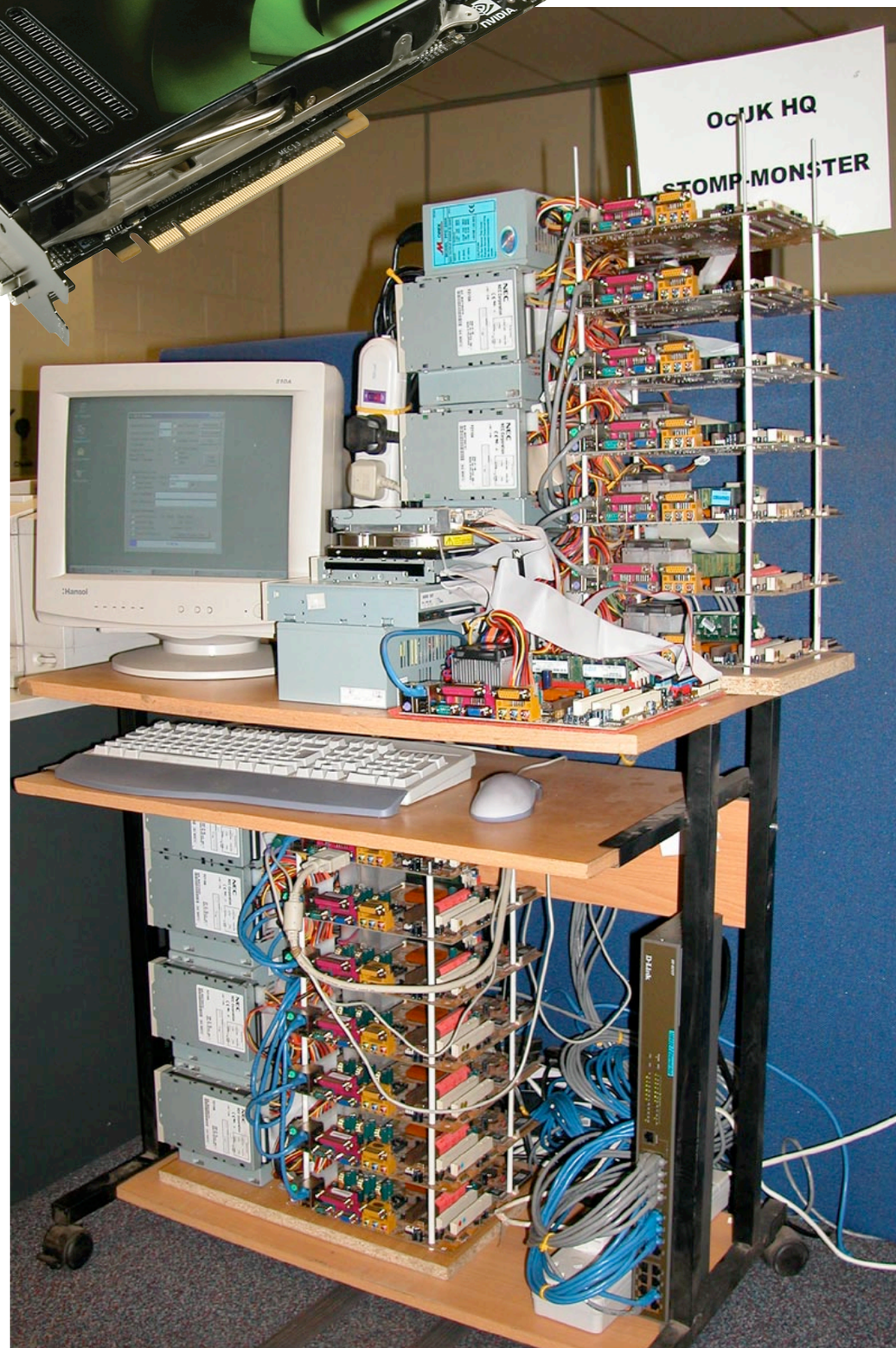


- Smart Brains
- Standard PCs
- Cluster
- GPUs
- Hybrid-Cluster
- Cell-, XBox-, Playstation-Cluster

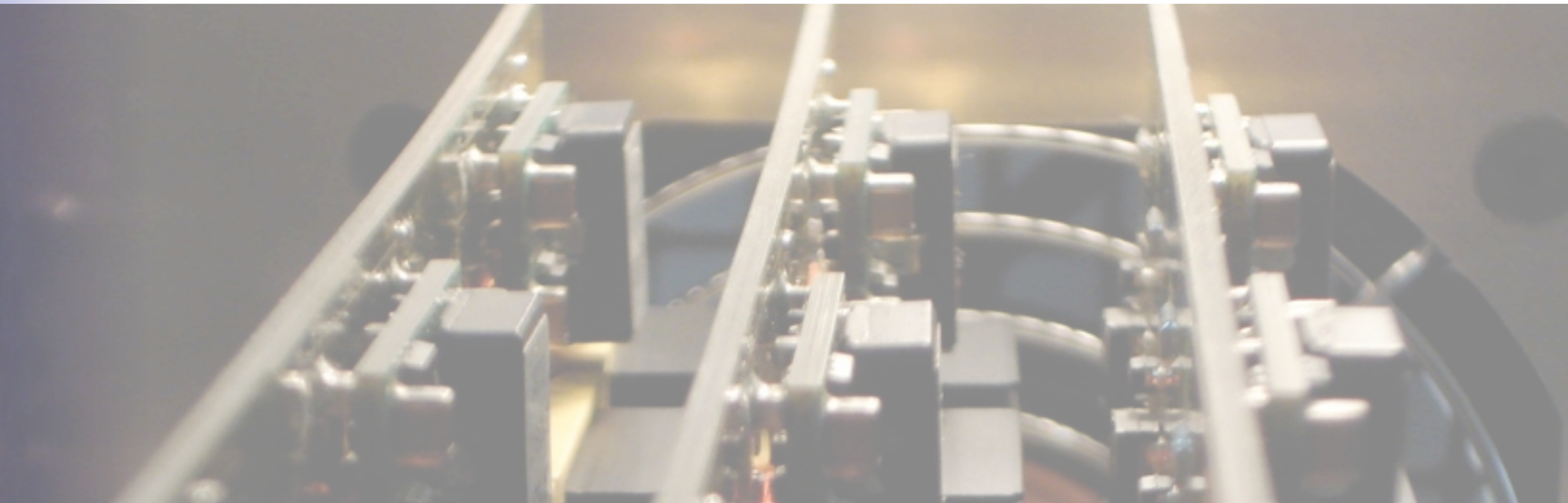
Supercomputers, Clouds, Grids & Cluster

Playstations + GPUs



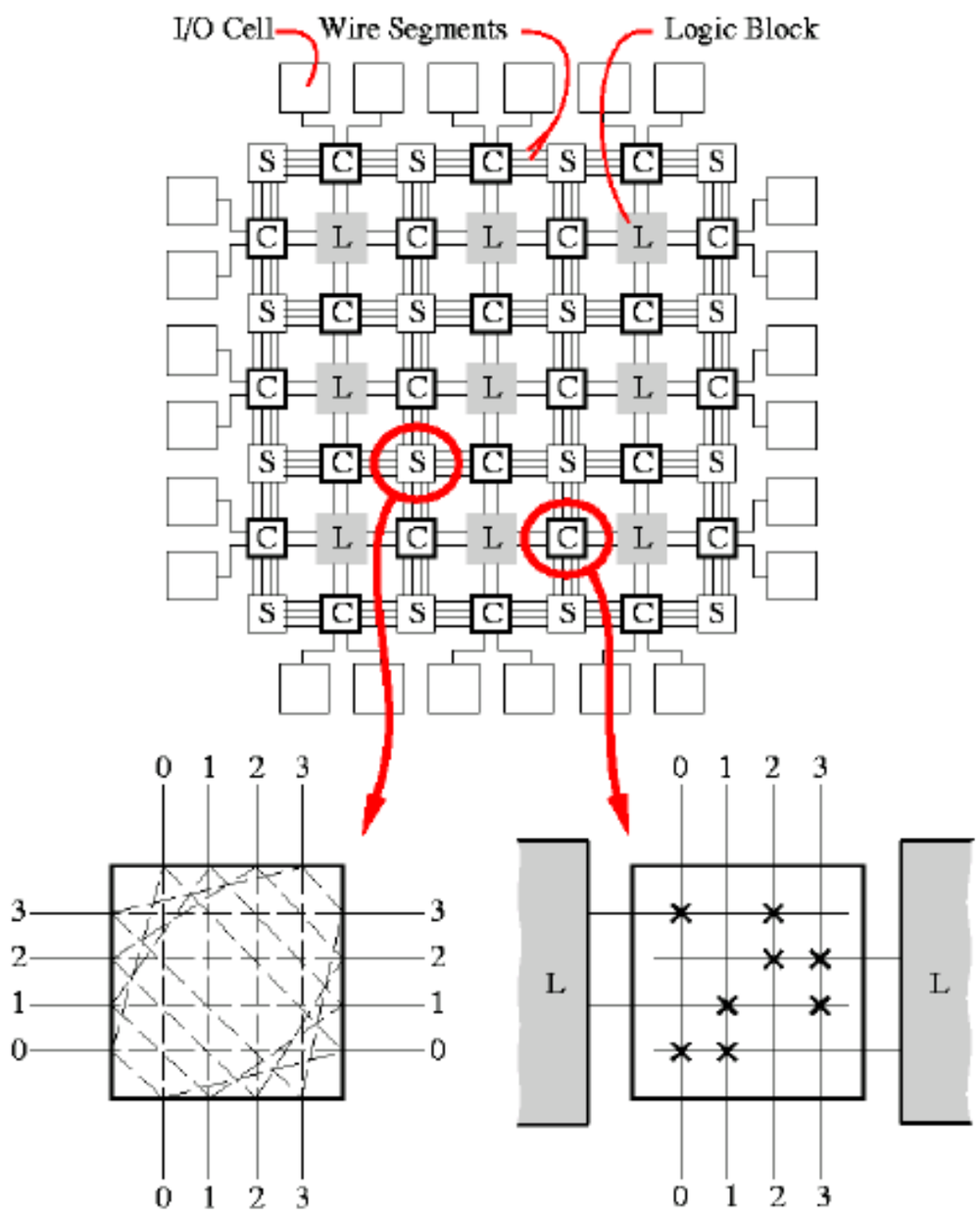


- About us
- Motivation
- Todays Approaches
- **Our Approach**
- **Conclusion and Comments**

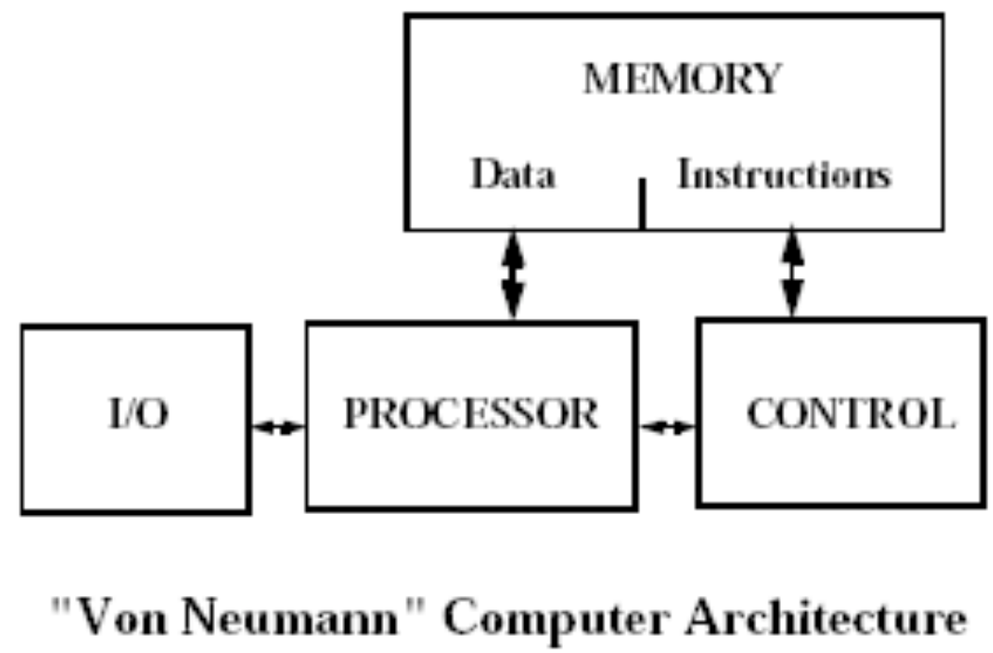


FPGA vs. CPU

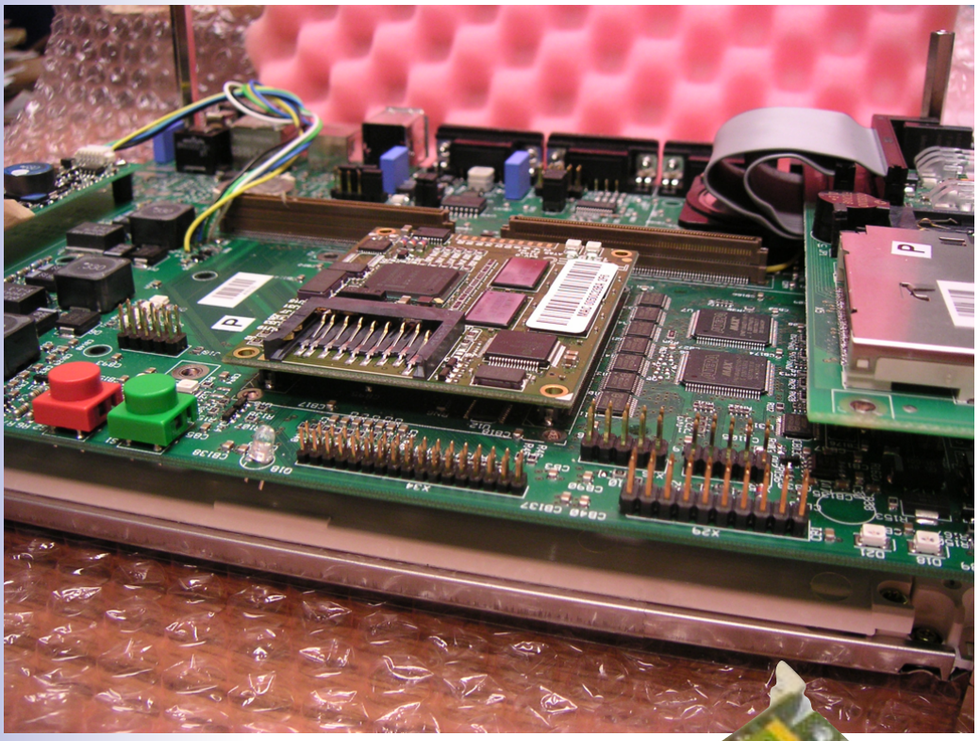
Field Programmable Gate Array (FPGA)

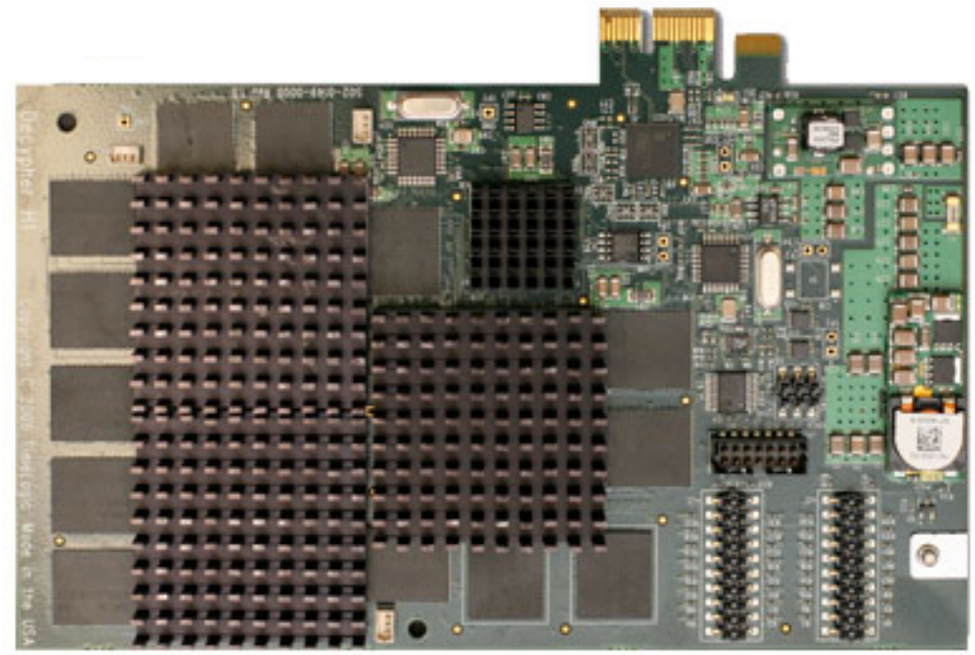


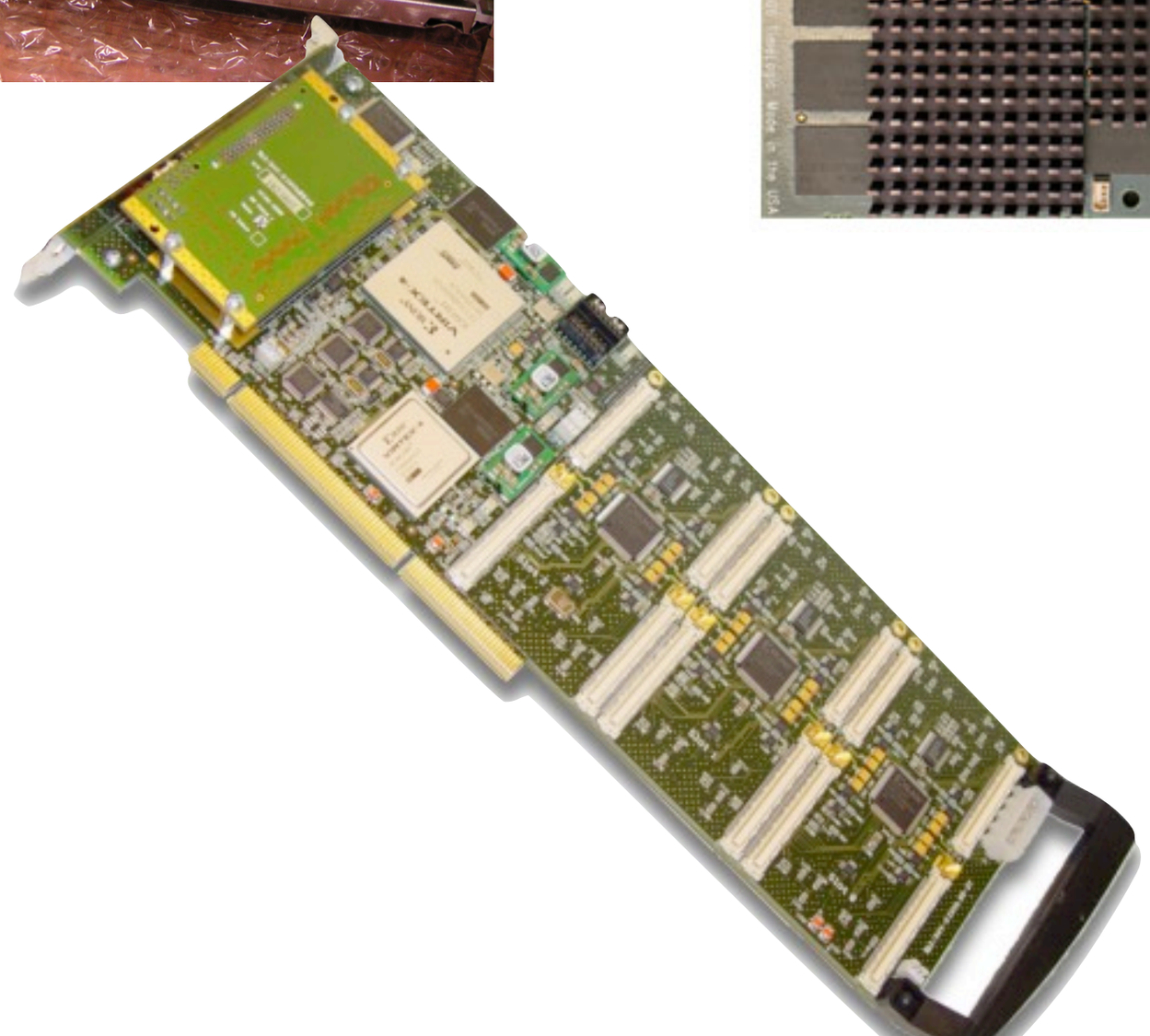
- Central Processing Unit (CPU)



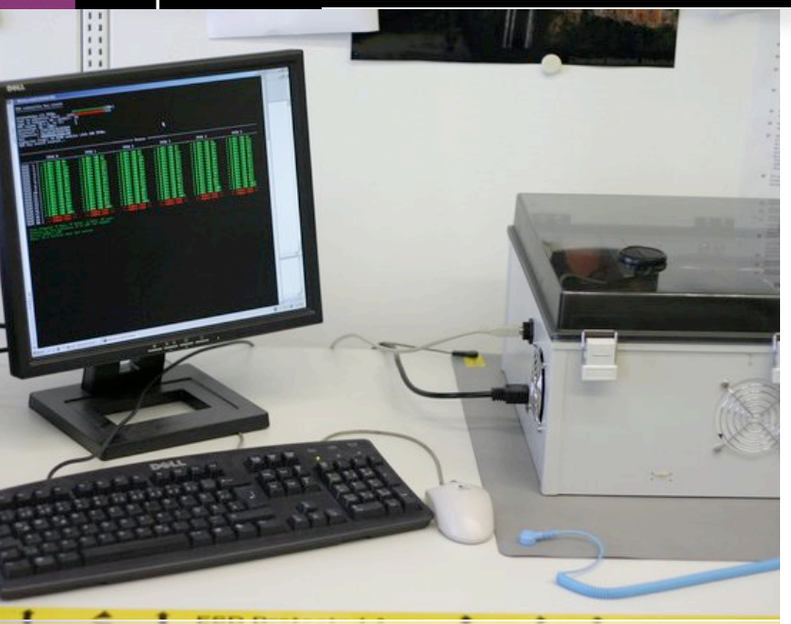
Single Chip

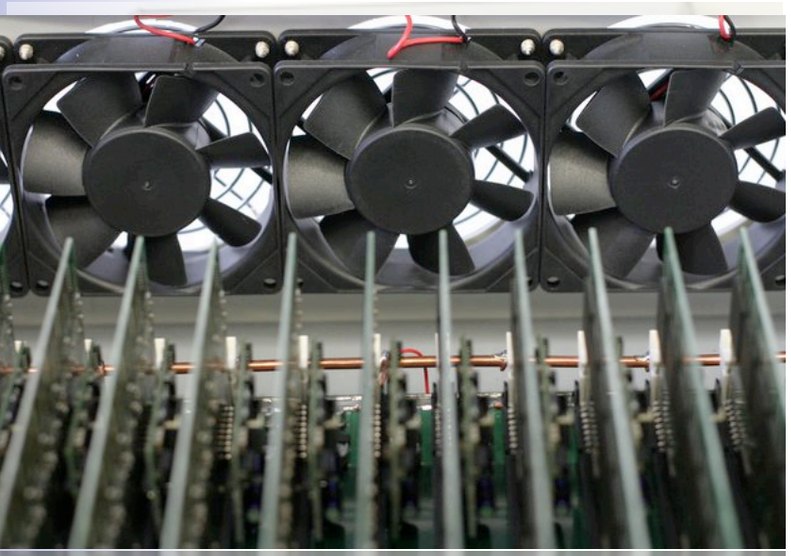






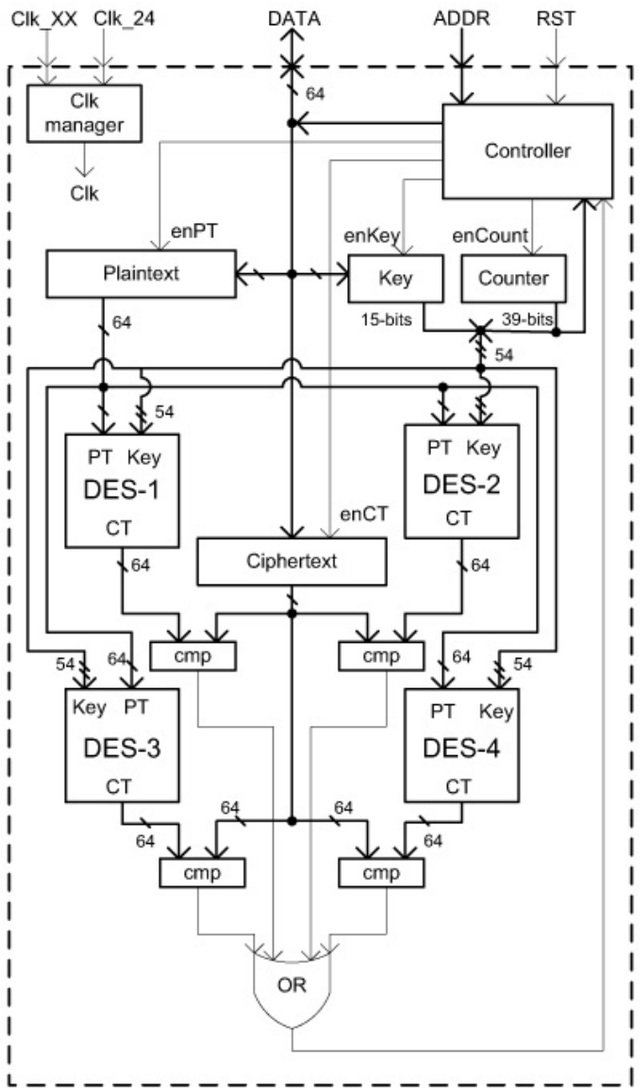
COPACOBANA





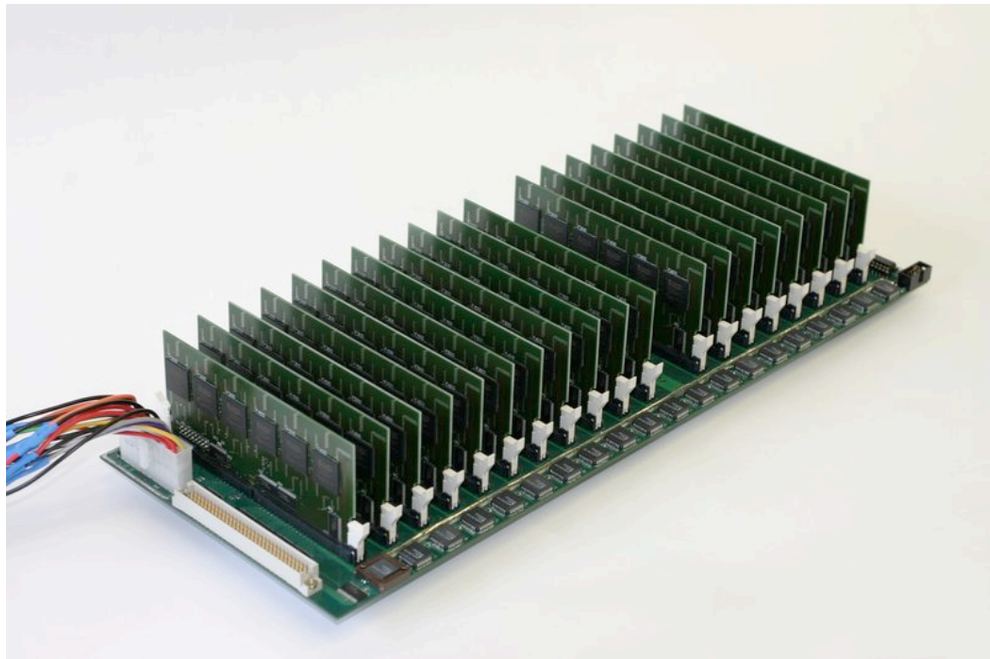
- Cracking DES ?
  - Data Encryption Standard 56 Bit key length

- Exhaustive key search (FPGA based):
  - 4 completely pipelined DES engines per FPGA (courtesy of the crypto group of UCL)
  - one key per clock cycle per DES engine
  - One FPGA@100MHz: 400 mio. keys/ sec

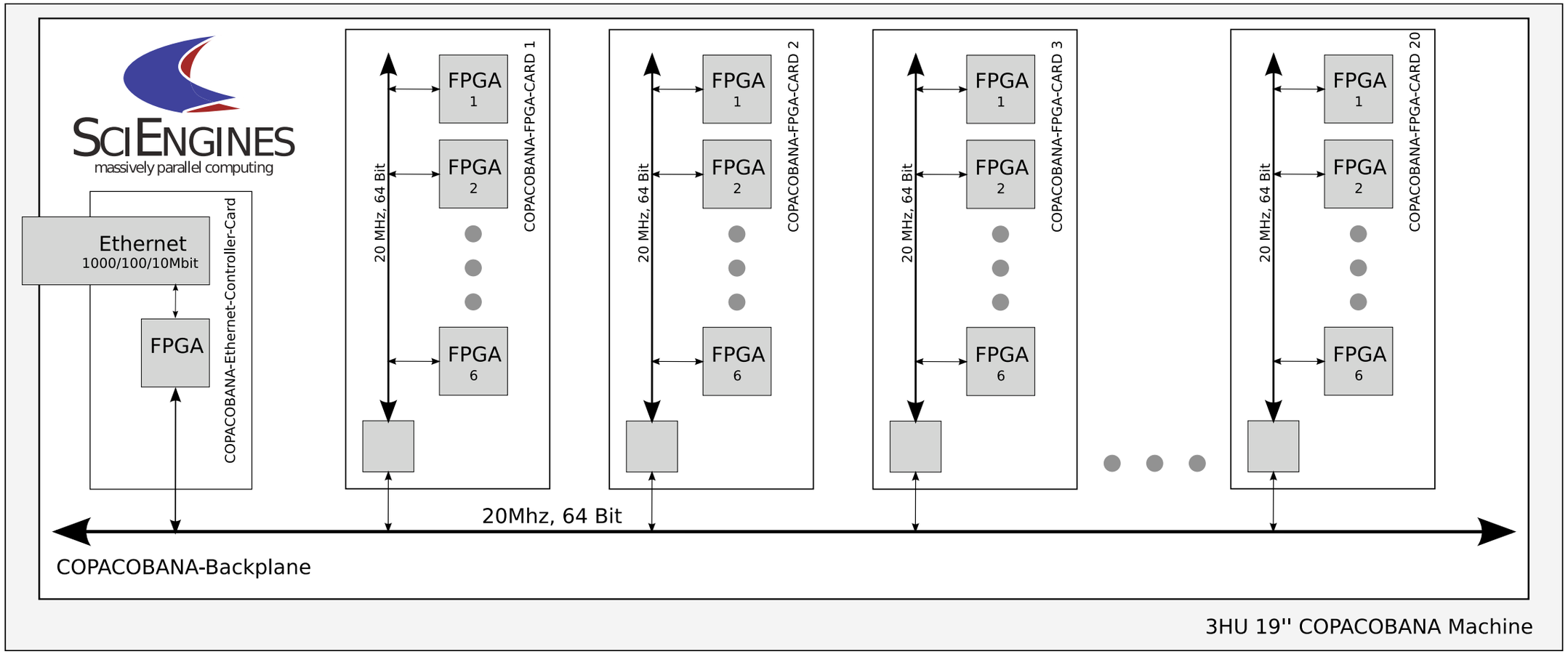


COPACOBANA

- COPACOBANA Raw Prototype ~9.000€

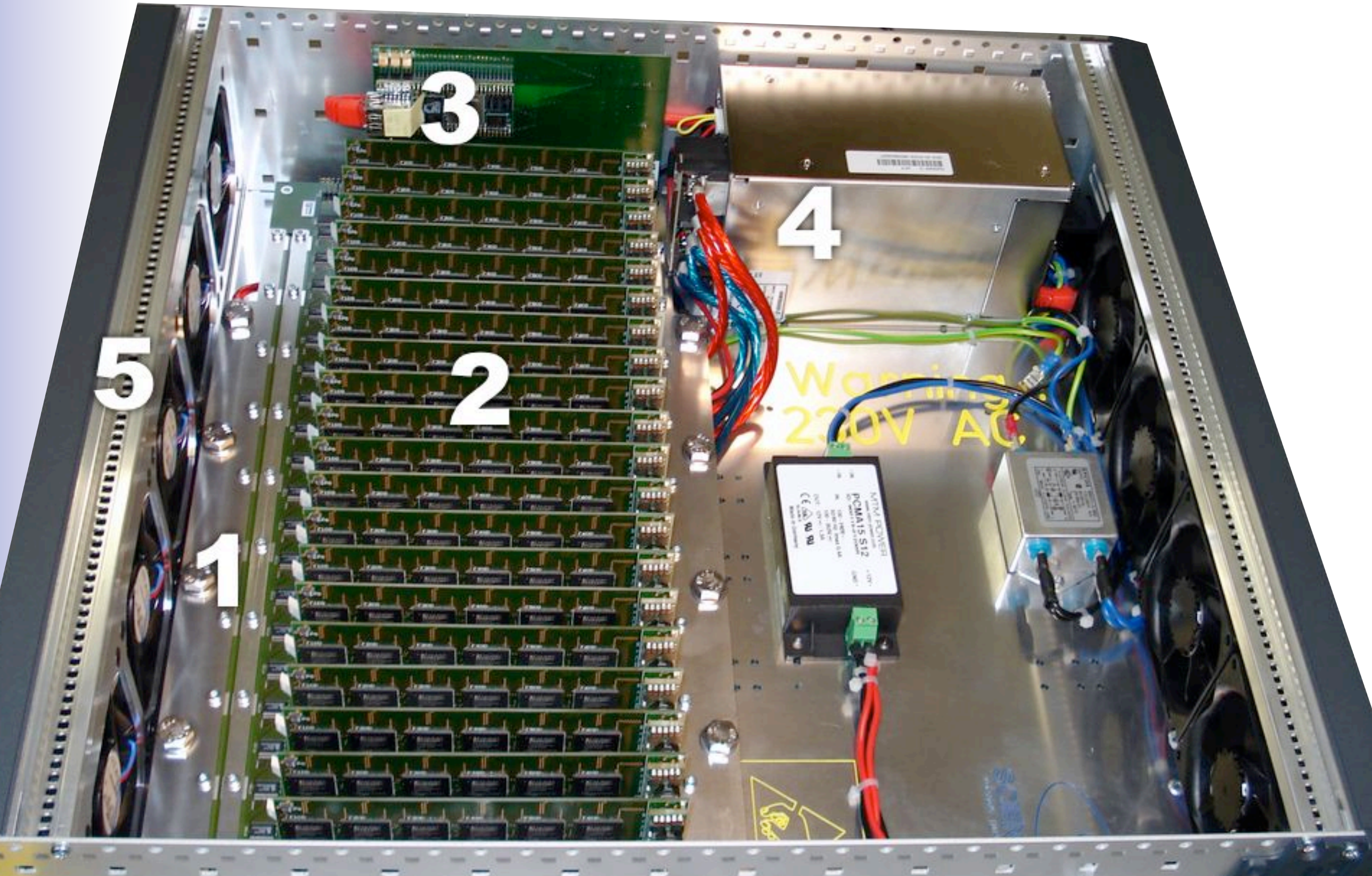


COPACOBANA

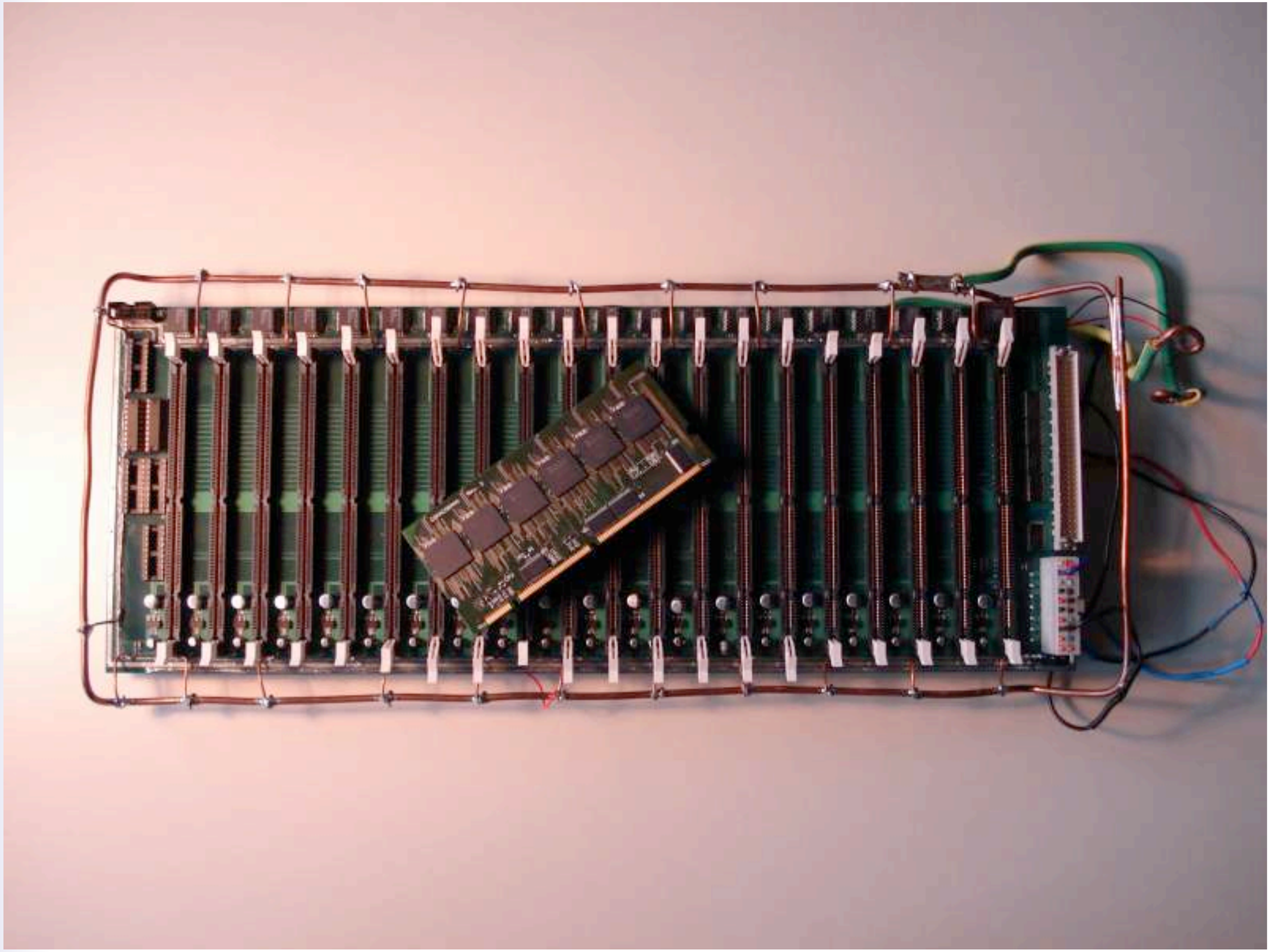

SciEngines
massively parallel computing
Ethernet
1000/100/10Mbit
FPGA
COPACOBANA-Ethernet-Controller-Card
20 MHz, 64 Bit
FPGA 1
FPGA 2
FPGA 6
COPACOBANA-FPGA-CARD 1
COPACOBANA-FPGA-CARD 2
COPACOBANA-FPGA-CARD 3
COPACOBANA-FPGA-CARD 20
20Mhz, 64 Bit
COPACOBANA-Backplane
3HU 19'' COPACOBANA Machine

COPACOBANA
www.copacobana.org

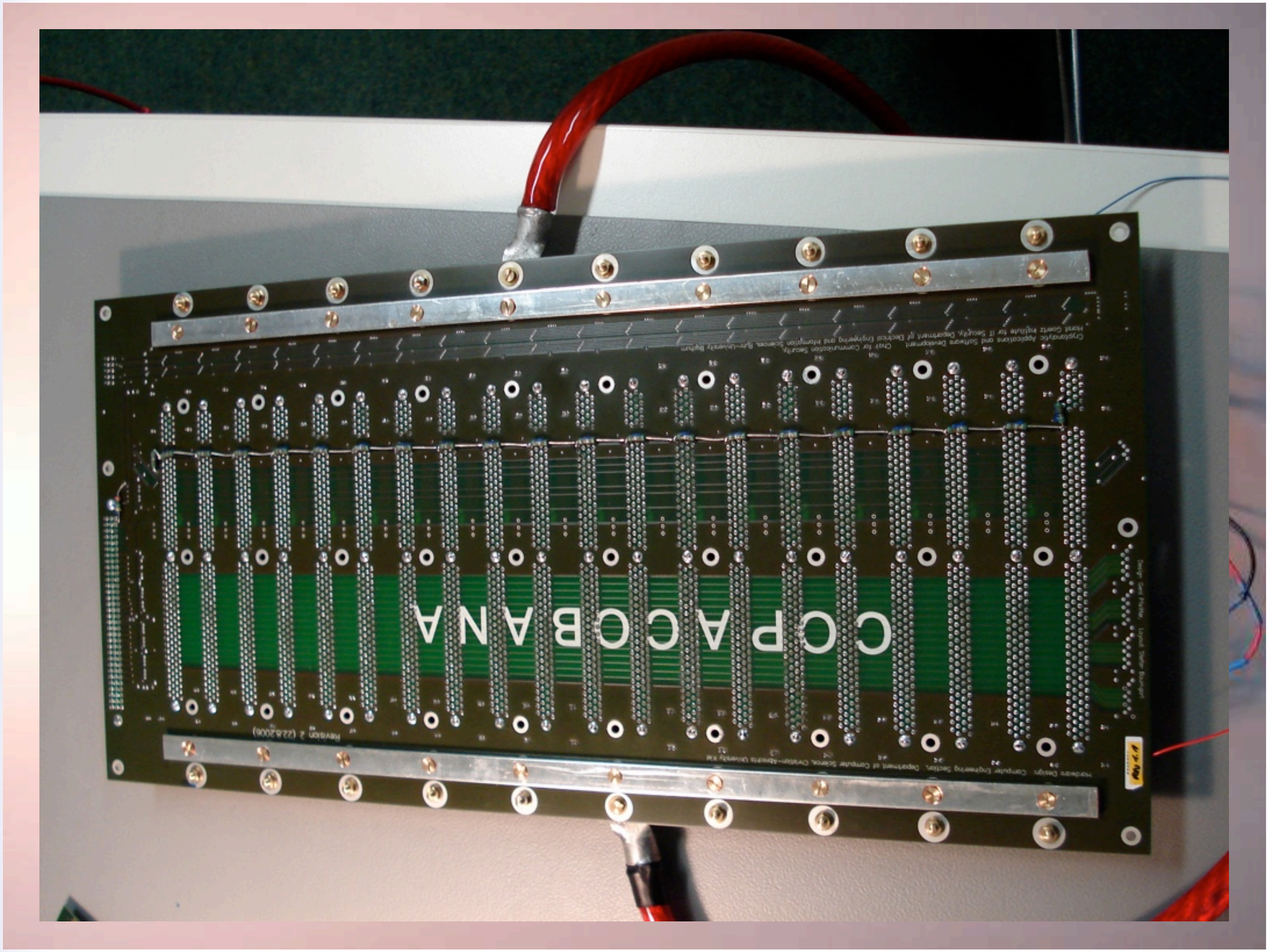
COPACOBANA



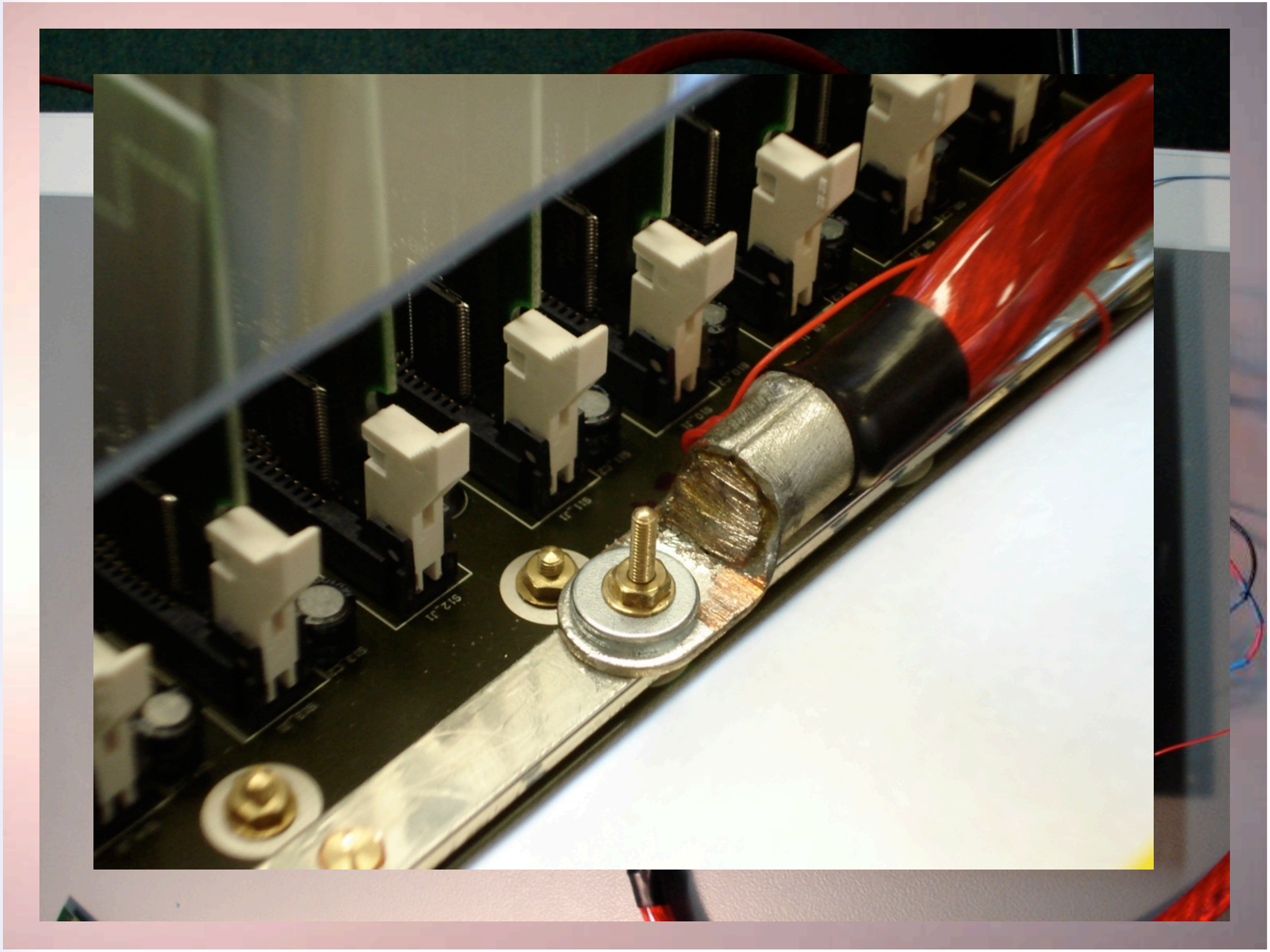
COPACOBANA, a way to power



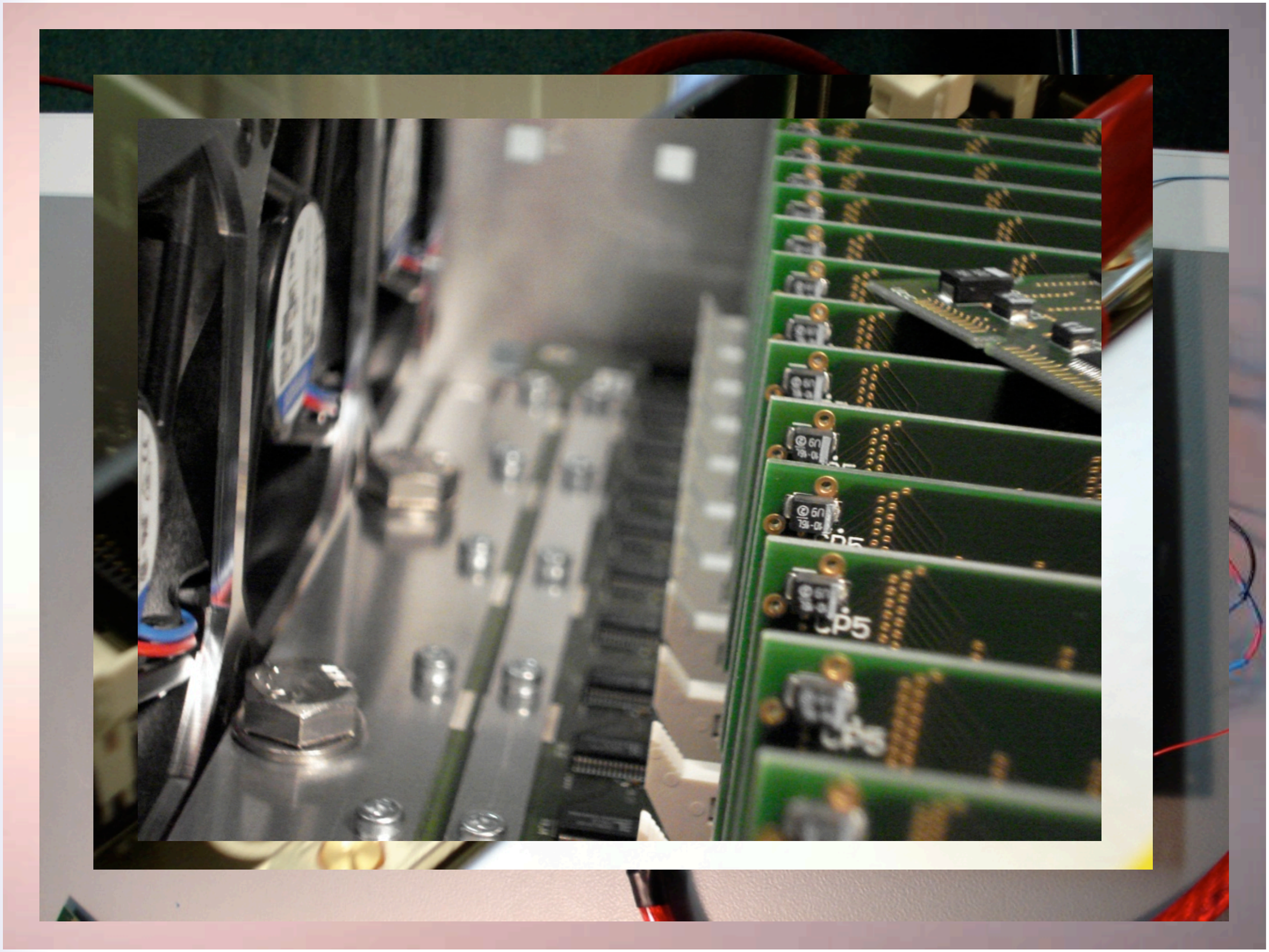
COPACOBANA, a way to power



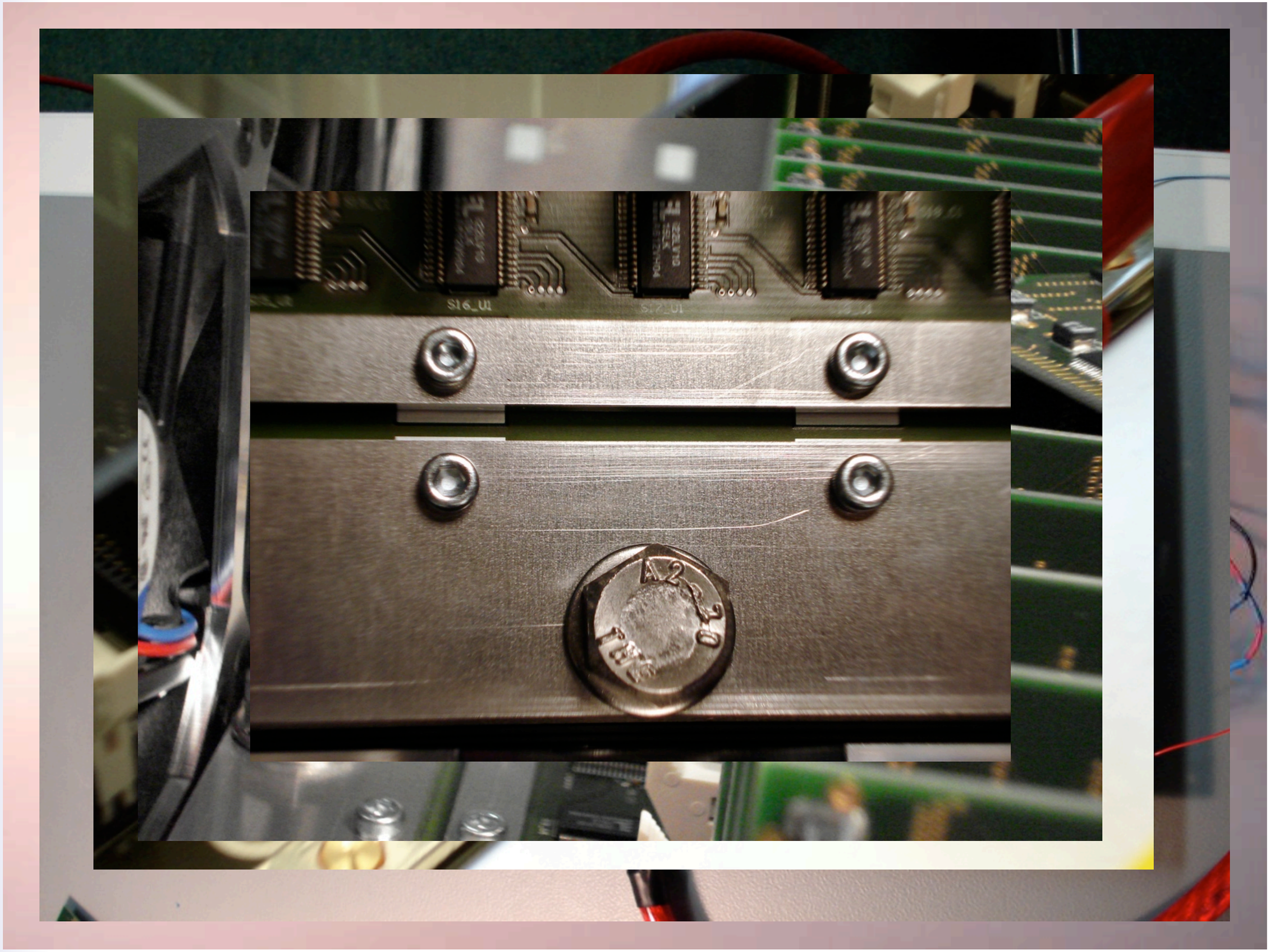
COPACOBANA, a way to power



COPACOBANA, a way to power

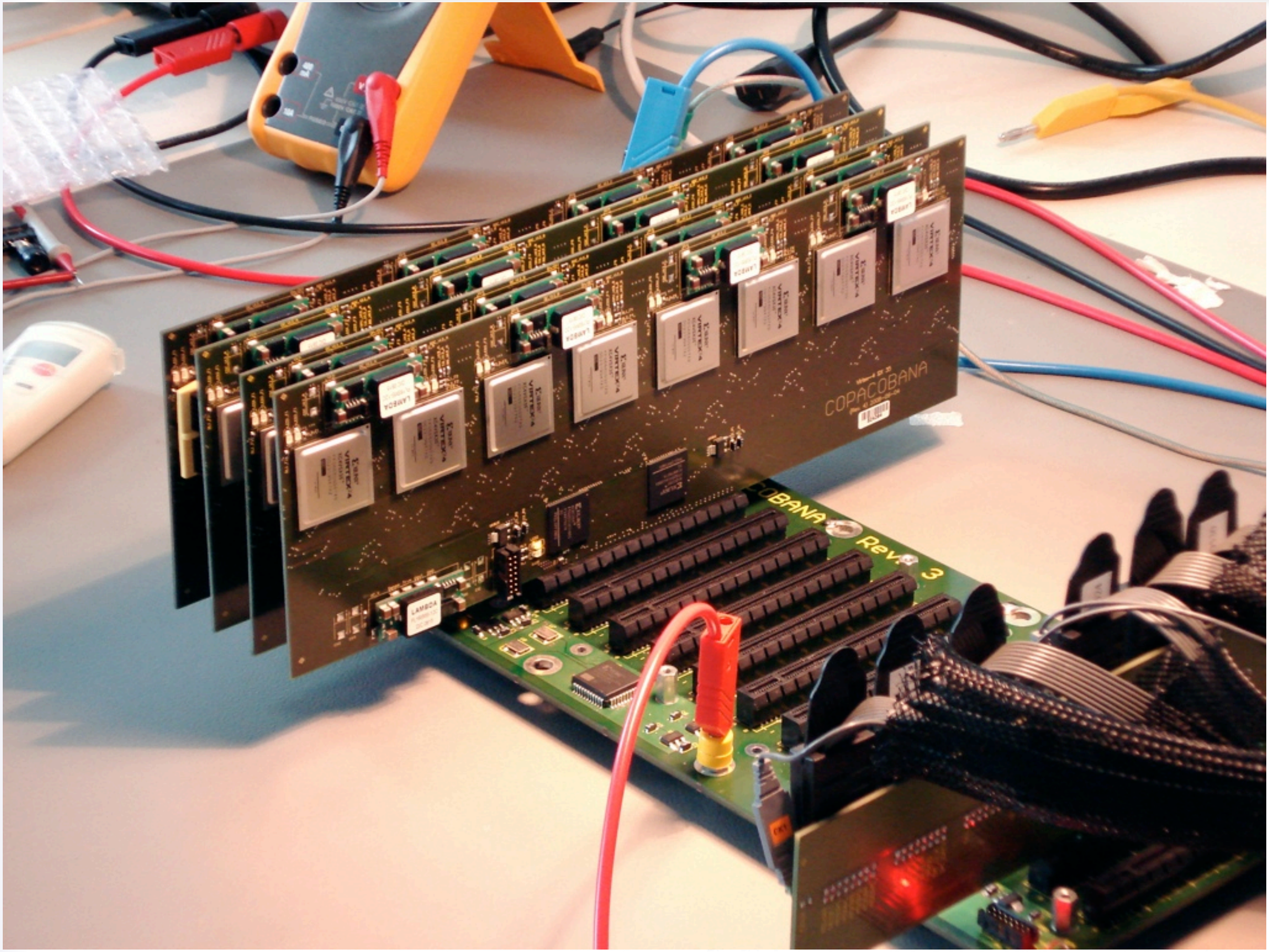


COPACOBANA, a way to power

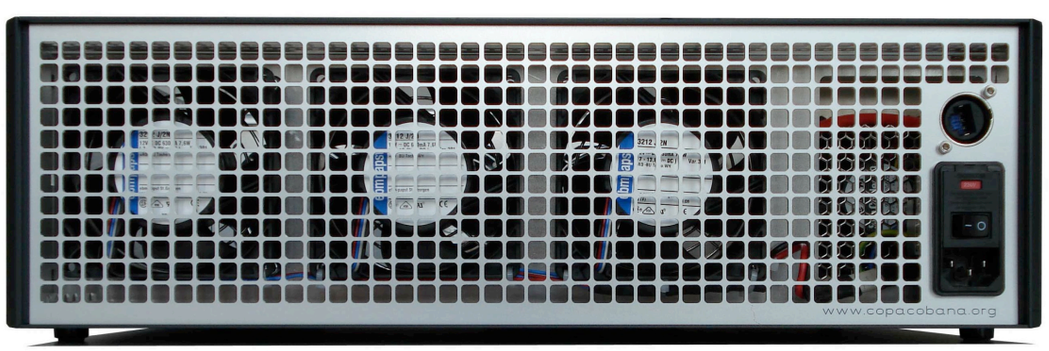


(REV 0) COPACOBANA Virtex-4

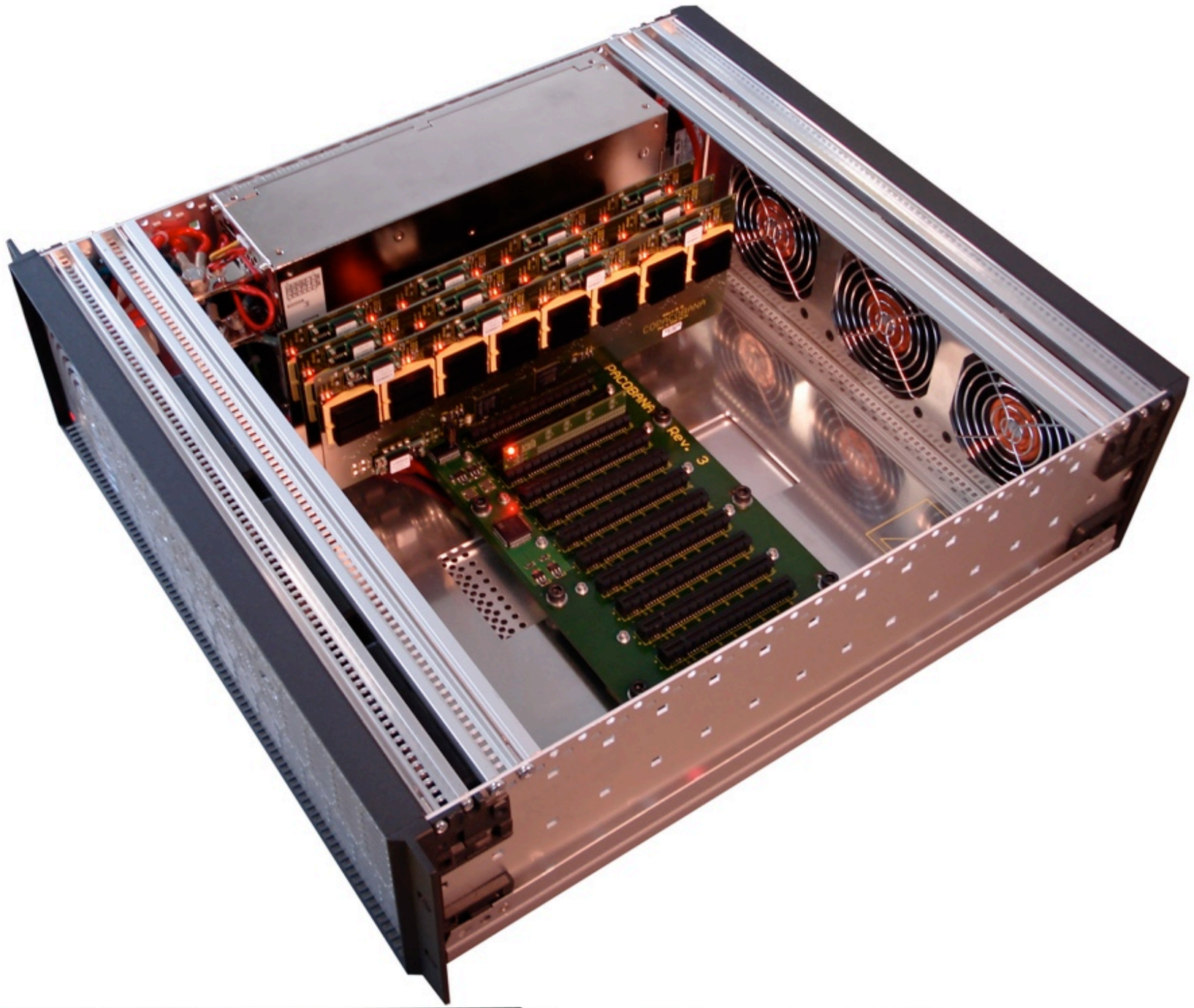
(REV 0) COPACOBANA Virtex-4

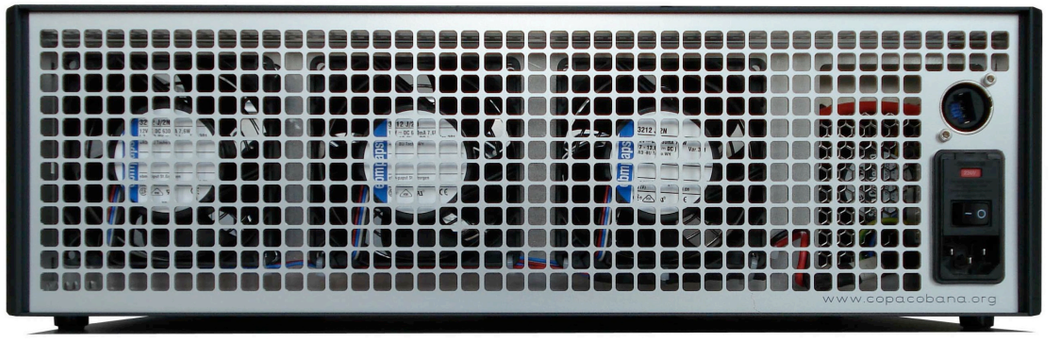


(REV 0) COPACOBANA Virtex-4

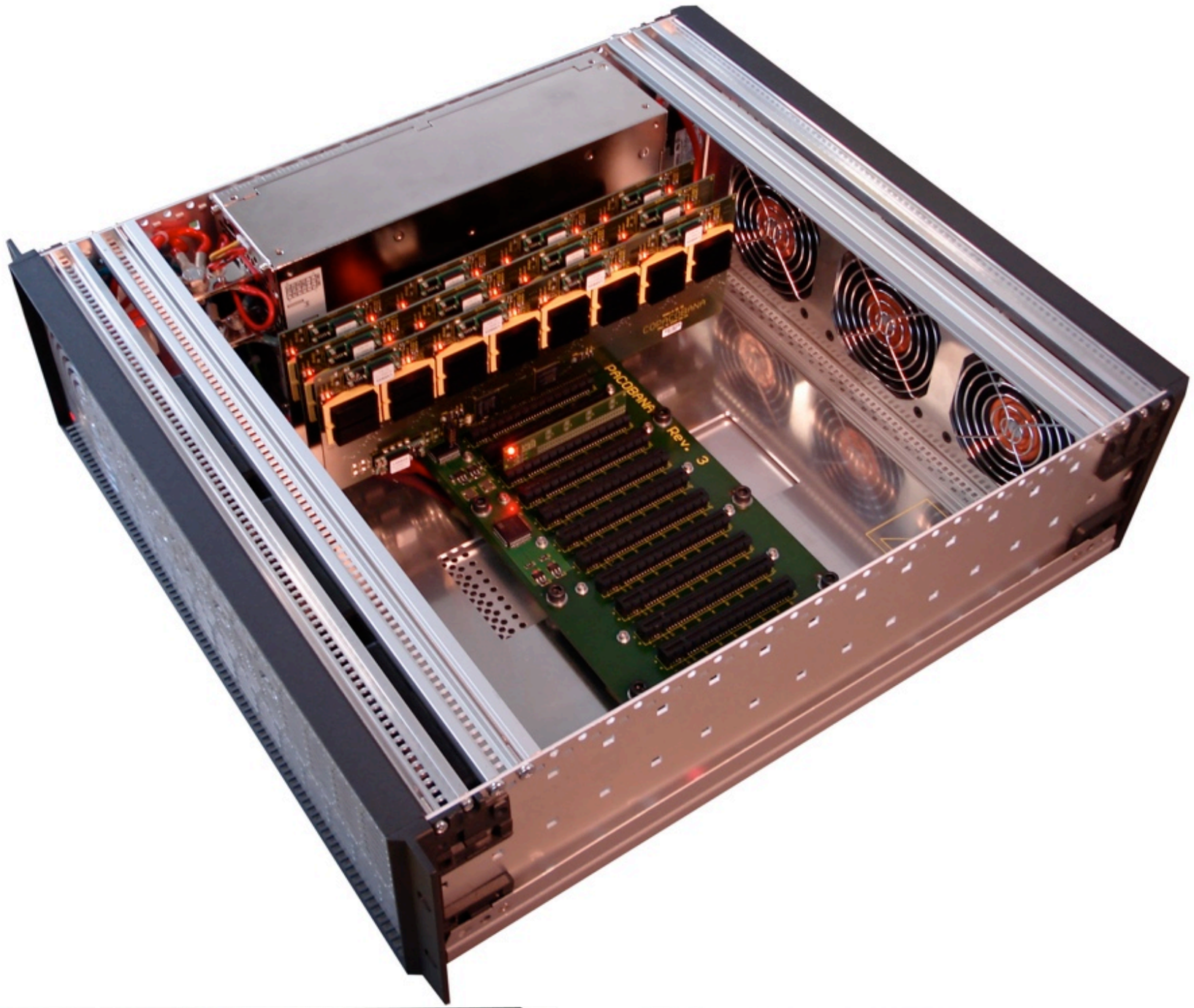


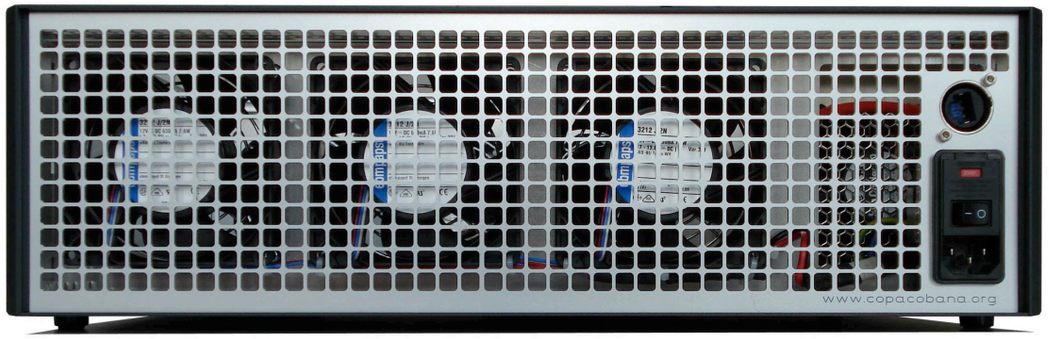
(REV 0) COPACOBANA Virtex-4



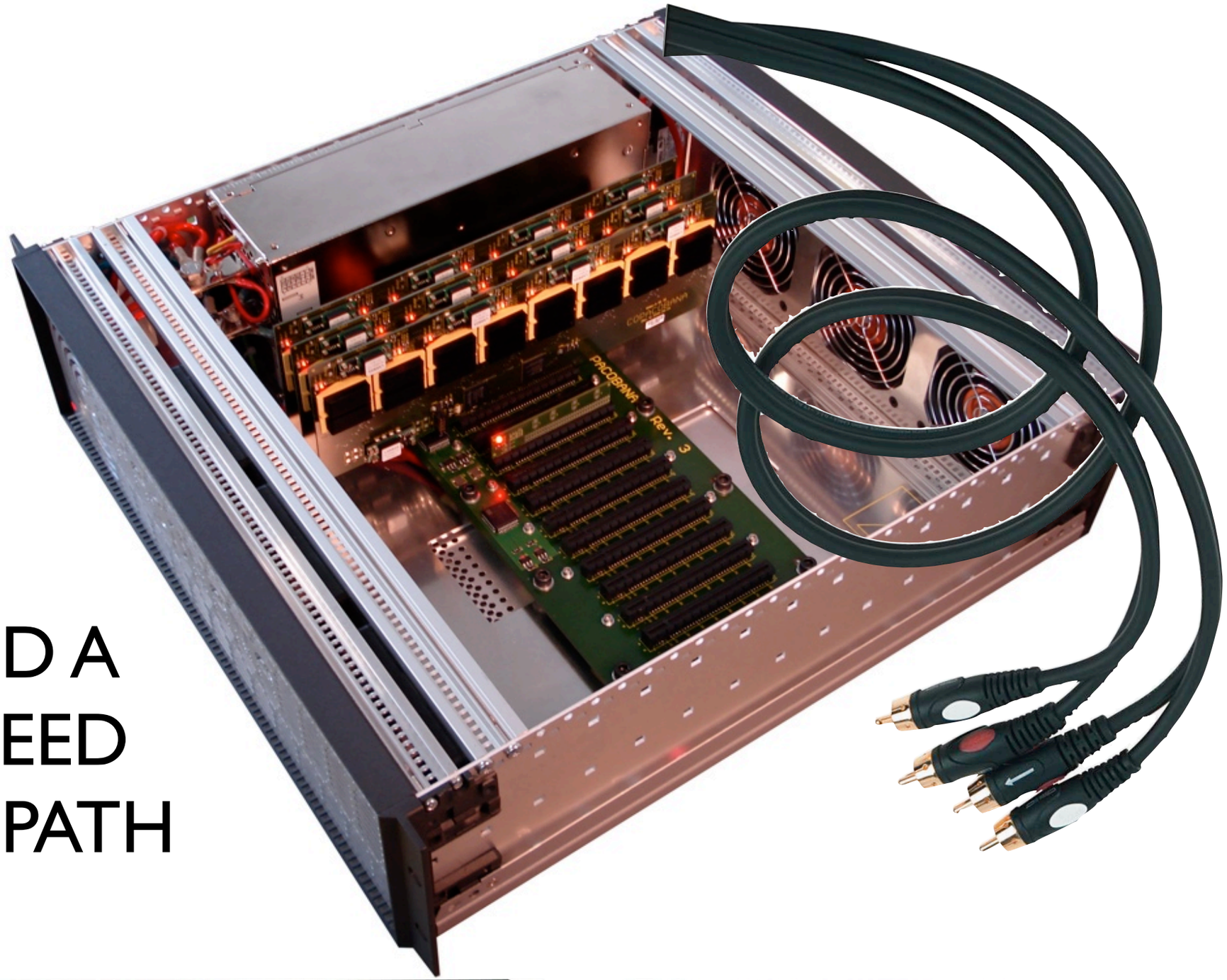


(REV 0) COPACOBANA Virtex-4

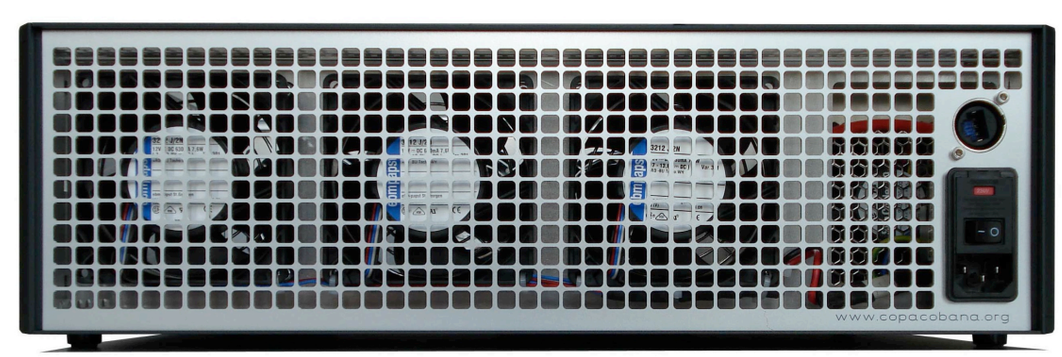




(REV 0) COPACOBANA Virtex-4



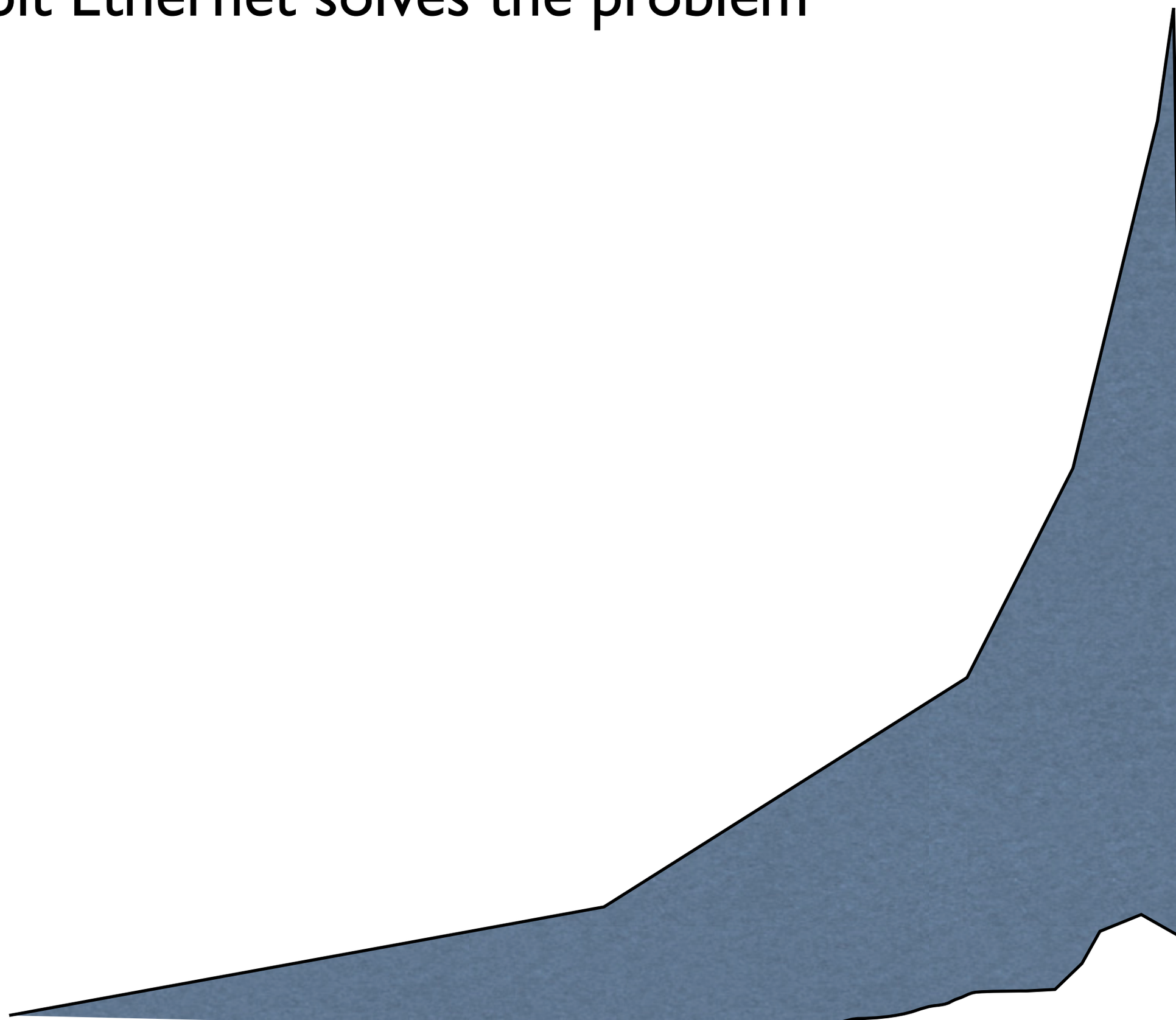
WE NEED A HIGH SPEED DATA I/O PATH



Free Climbing to Highspeed-I/O

Idea: 1000 Gbit Ethernet solves the problem

Idea: 1000 Gbit Ethernet solves the problem



Idea: 1000 Gbit Ethernet solves the problem

PHY

Idea: 1000 Gbit Ethernet solves the problem

MAC

PHY

Idea: 1000 Gbit Ethernet solves the problem

Protokollstack

MAC

PHY

Idea: 1000 Gbit Ethernet solves the problem

Interface API

Protokollstack

MAC

PHY

Idea: 1000 Gbit Ethernet solves the problem

Interface API

Protokollstack

MAC

PHY

Free Climbing to Highspeed-I/O

Idea: 1000 Gbit Ethernet solves the problem

costs for selfimplemented TCP/IP > machine costs

Interface API

Protokollstack

MAC

PHY

Free Climbing to Highspeed-I/O

Idea: 1000 Gbit Ethernet solves the problem

costs for selfimplemented TCP/IP > machine costs

costs properitary of TCP/IP > machine costs

Interface API

Protokollstack

MAC

PHY

Free Climbing to Highspeed-I/O

Idea: 1000 Gbit Ethernet solves the problem

costs for selfimplemented TCP/IP > machine costs

costs properitary of TCP/IP > machine costs

Interface API

freeware TCP/IP ~10Mbit

Protokollstack

MAC

PHY

Free Climbing to Highspeed-I/O

Idea: 1000 Gbit Ethernet solves the problem

costs for selfimplemented TCP/IP > machine costs

costs properitary of TCP/IP > machine costs

Interface API

freeware TCP/IP ~10Mbit

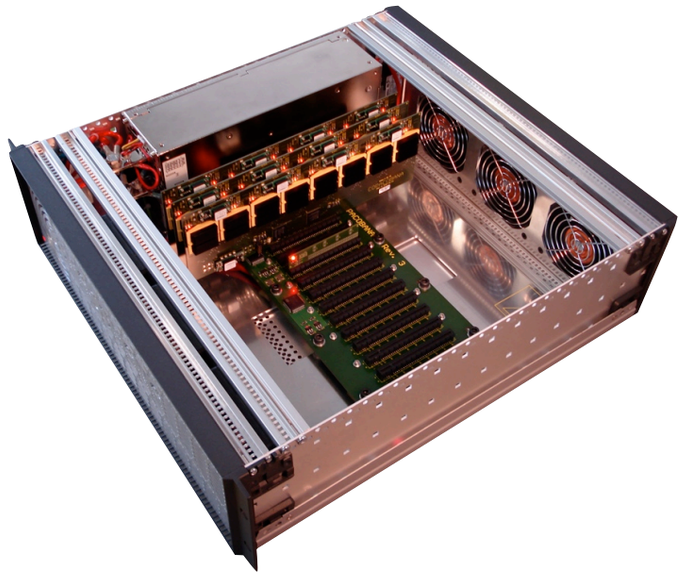
Protokollstack

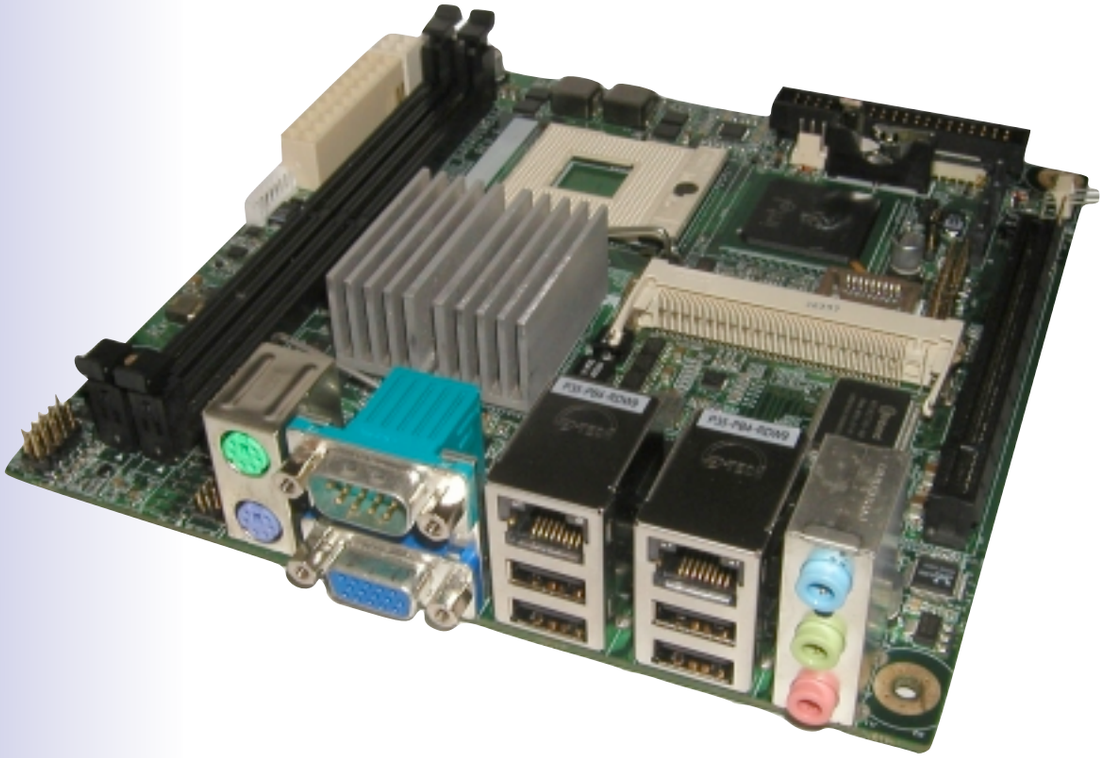
MAC

PHY

Prototype worked but no adequate solution

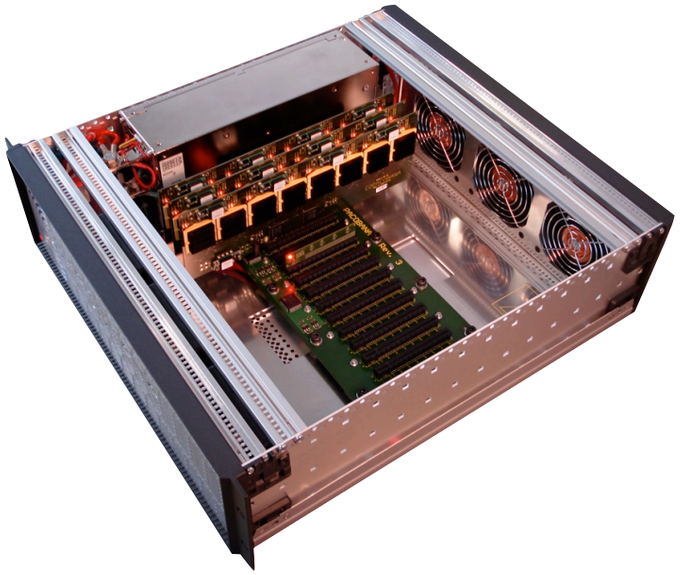
Idea: PC have working TCP / IP Stacks with good performance

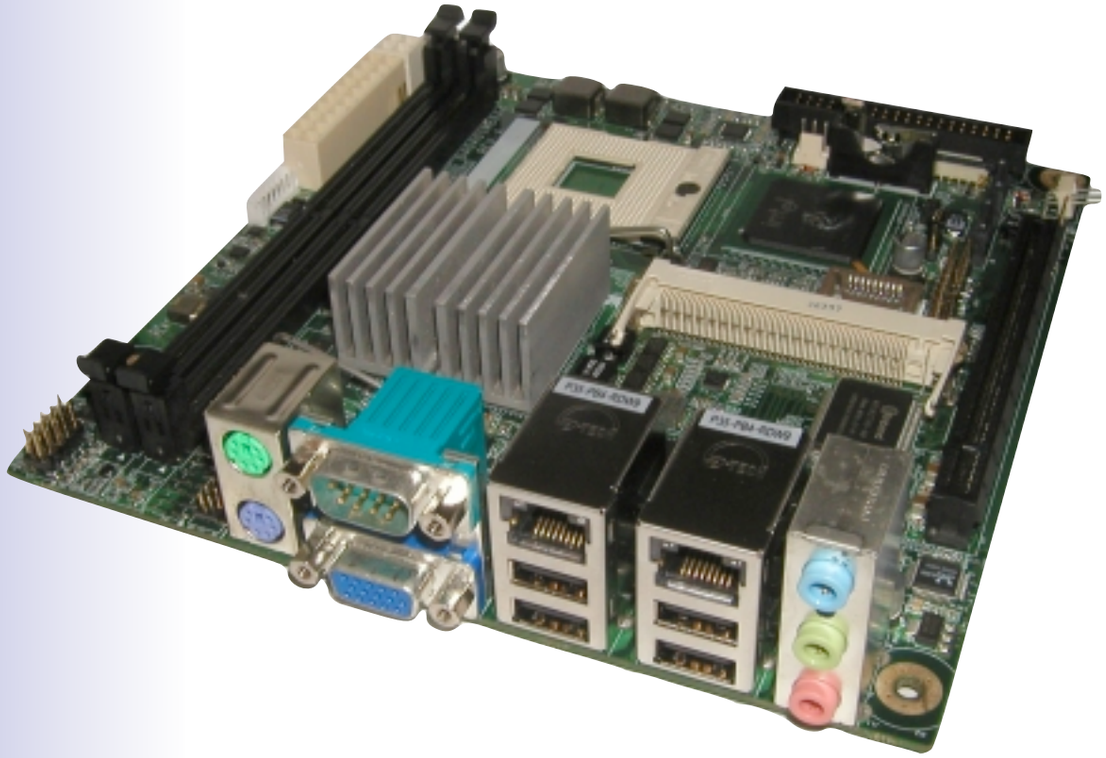




Idea: PC have working TCP / IP Stacks with good performance

SATA

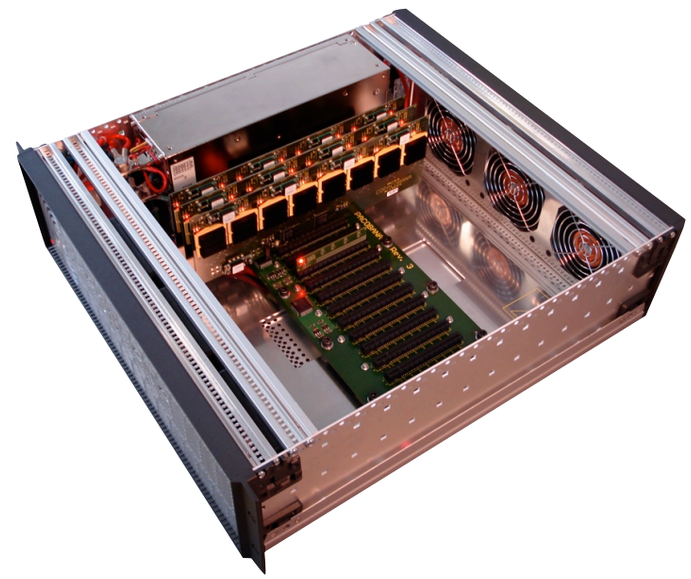


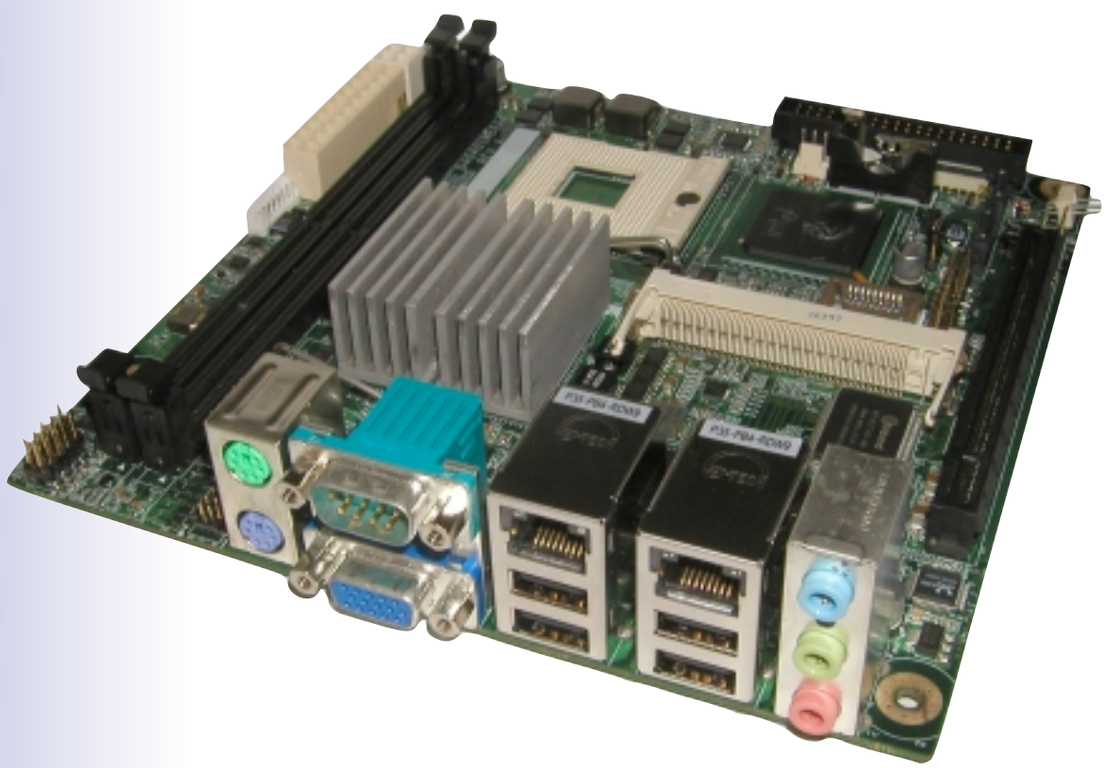


Idea: PC have working TCP / IP Stacks with good performance

SATA

PCI



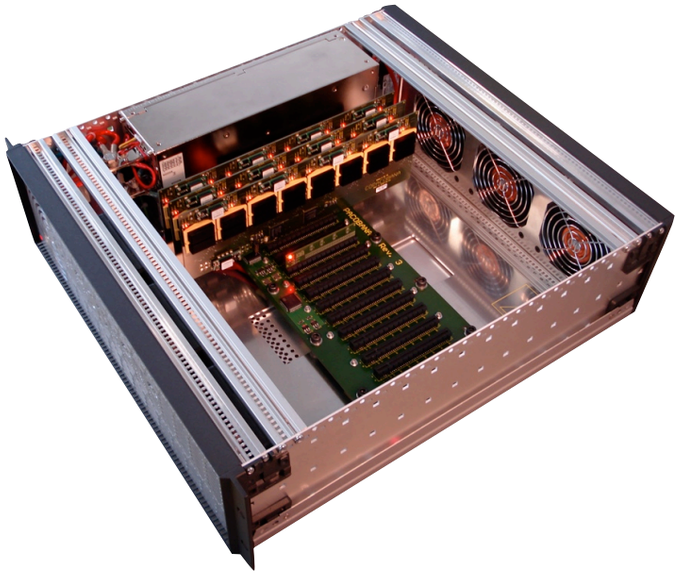


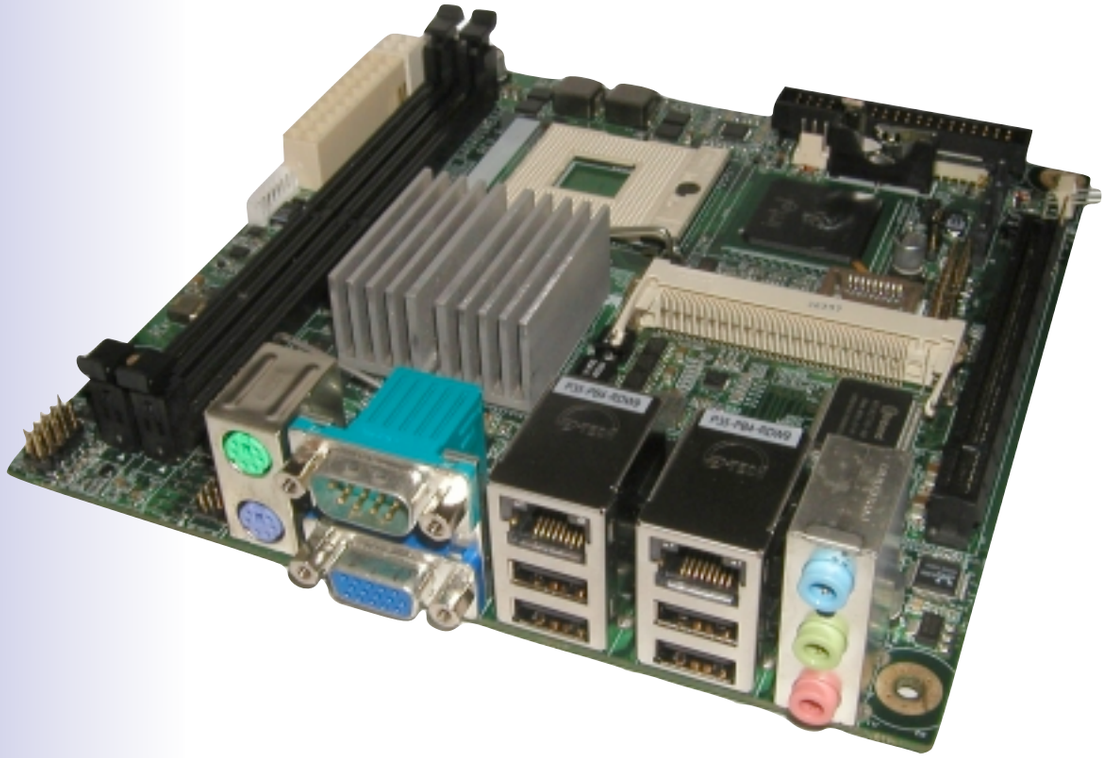
Idea: PC have working TCP / IP Stacks with good performance

SATA

PCI

USB





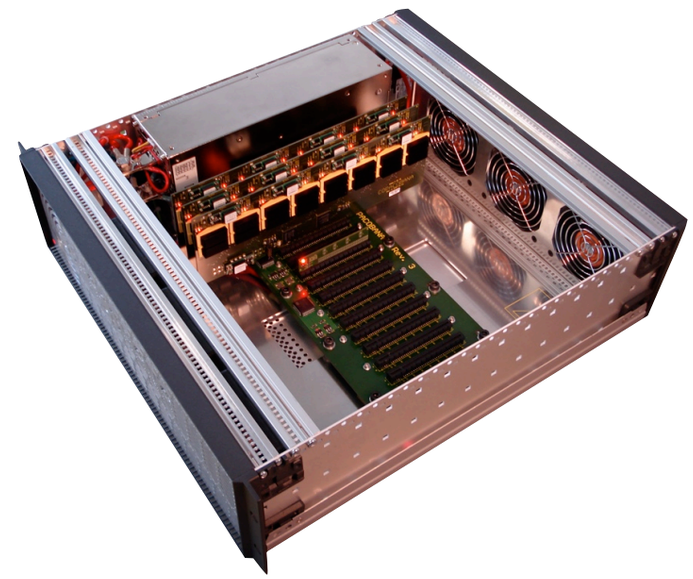
Idea: PC have working TCP / IP Stacks with good performance

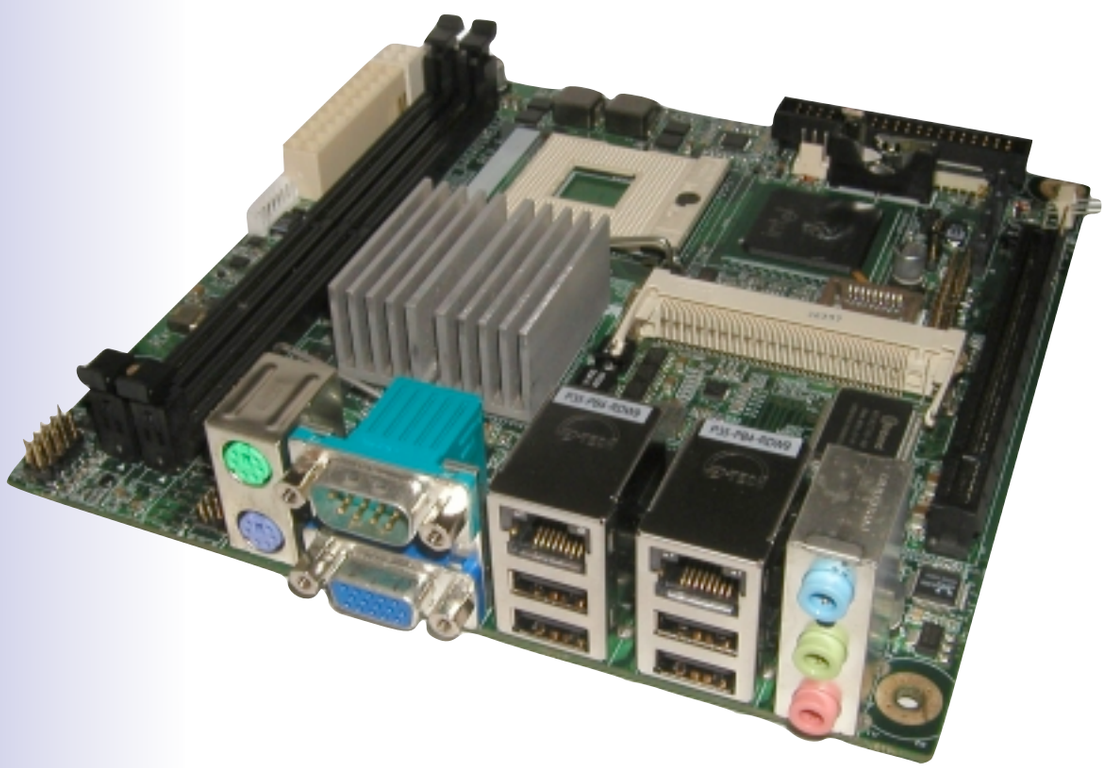
SATA

PCI

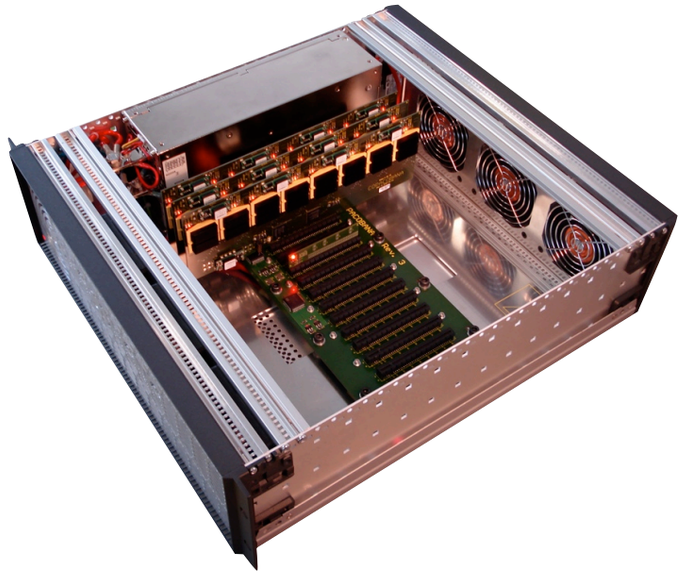
USB

FireWire





Idea: PC have working TCP / IP Stacks with good performance



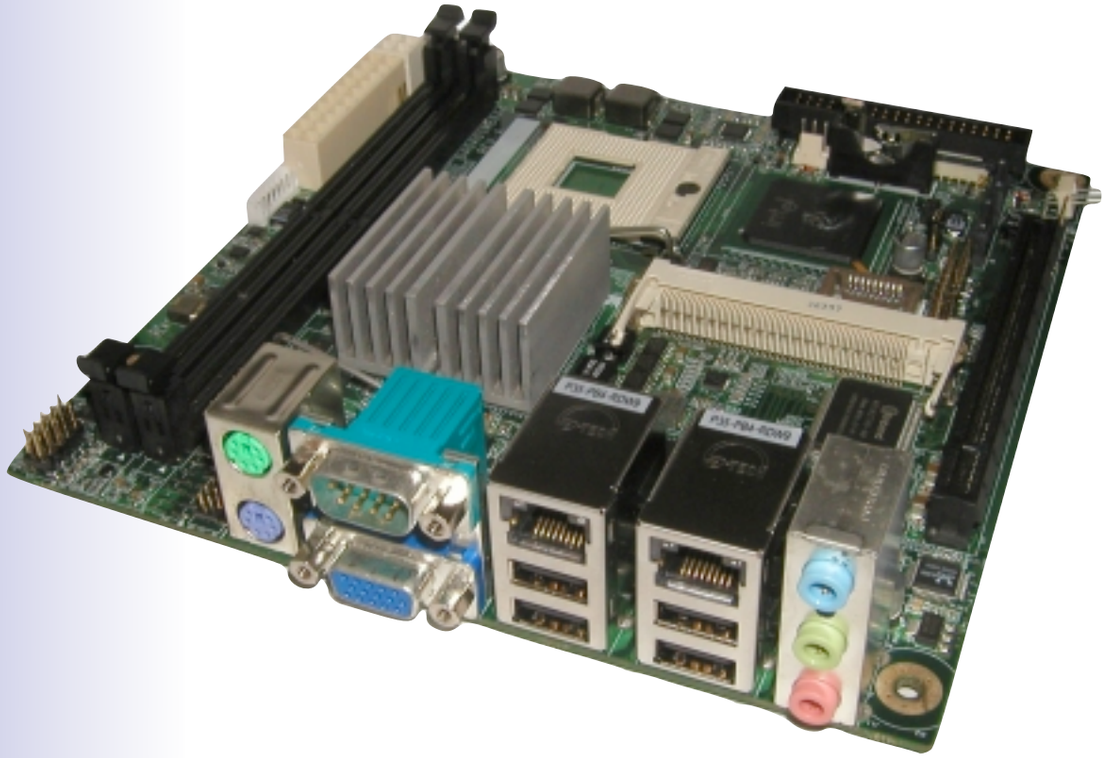
SATA

PCI

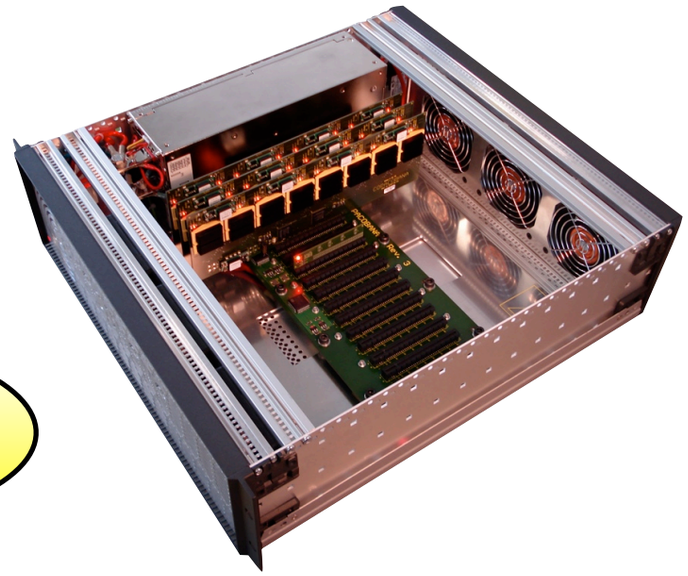
USB

FireWire

Ethernet



Idea: PC have working TCP / IP Stacks with good performance



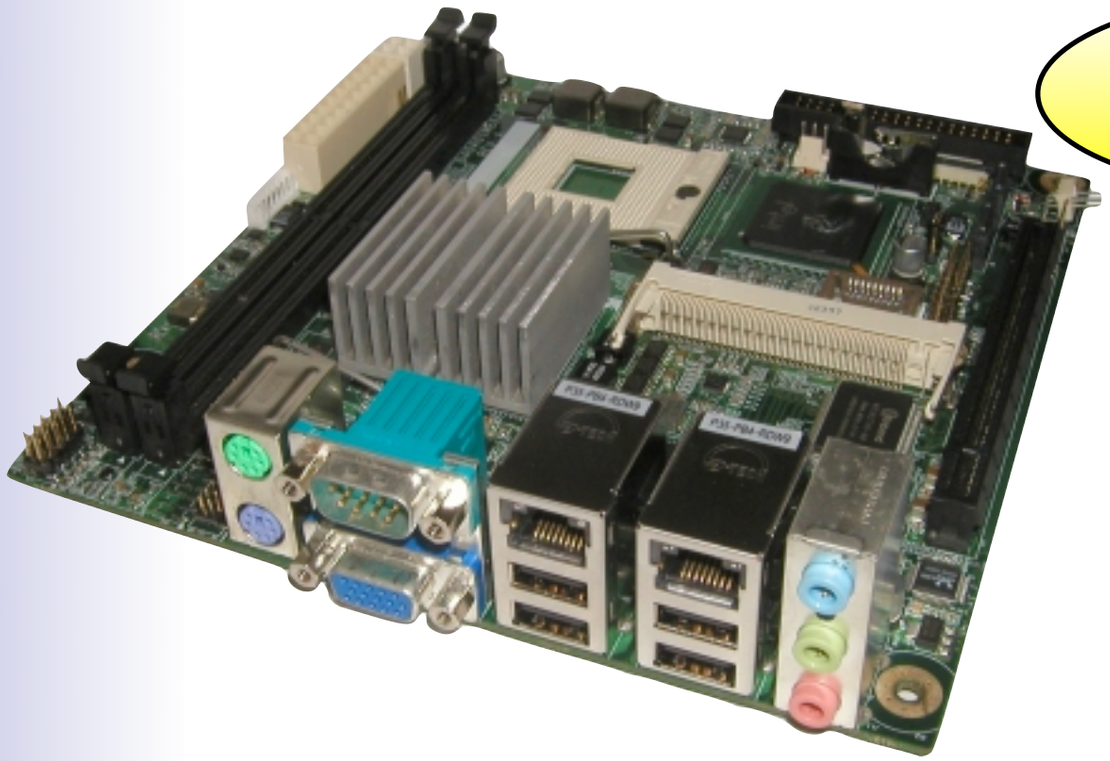
SATA

PCI

USB

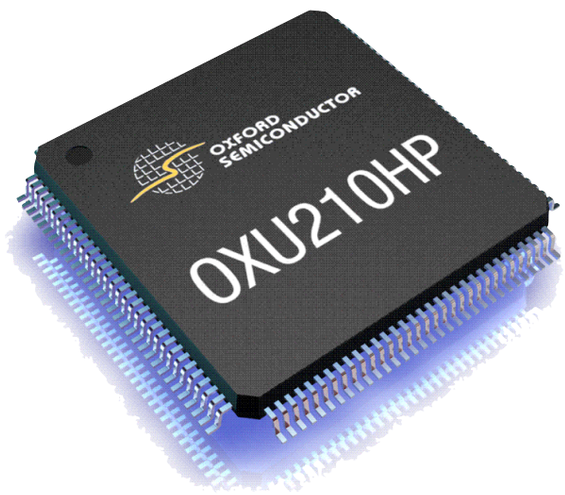
FireWire

Ethernet



Idea: USB 2.0 (480Mbit) is a commonly used interface

Prototype A



- offen used chip
- good spec
- good silicon
- poor drivers
- worst licening policy ever
- poor undocumented api

Idea: USB 2.0 (480Mbit) is a commonly used interface

Prototype A

- offen used chip
- good spec
- good silicon
- poor drivers
- worst licening poli
- poor undocum

firm died and was bought no adequate solution

Idea: USB 2.0 (480Mbit) is a commonly used interface

Prototype B

- offen used chip
- good spec
- good silicon
- multiple drivers
- documented api

FTDI Chip
Document No.: FT_000060
FT4232H QUAD HIGH SPEED USB TO MULTIPURPOSE UART/MPSSE IC
Datasheet Version 2.05
Clearance No.: FTDI#78

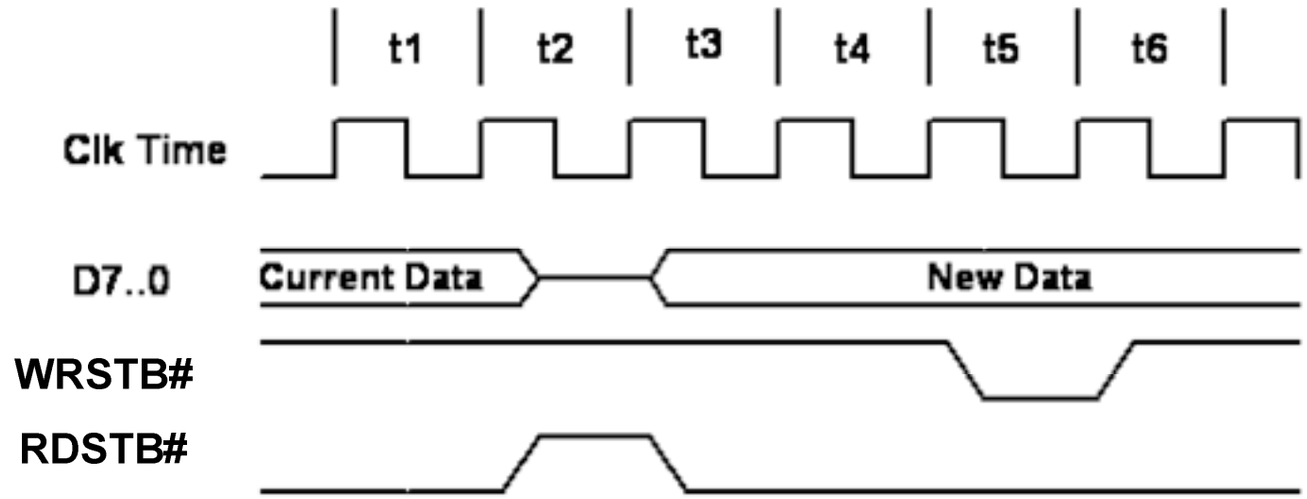


Figure 4.5 Synchronous Bit-Bang Mode Timing Interface Example

It should be noted that the FT4232H does not output the WRSTB# or RDSTB# signals when configured in bit-bang mode. Figure 4.5. and Table 4.2 show these signals for **illustration** purposes only.

NAME	Description
t1	Current pin state is read
t2	RDSTB# is set inactive and data on the paralle I/O pins is read and sent to the USB host.
t3	RDSTB# is set active again, and any pins that are output will change to their new data
t4	1 clock cycle to allow for data setup
t5	WRSTB# goes active. This indicates that the host PC has written new data to the I/O parallel data
t6	WRSTB# goes inactive

Table 4.2 Synchronous Bit-Bang Mode Timing Interface Example Timings

WRSTB# = this output indicates when new data has been written to the I/O pins from the Host PC (via the USB interface).

RDSTB# = this output rising edge indicates when data has been read from the I/O pins and sent to the Host PC (via the USB interface).

Free Climbing to Highspeed-I/O

FTDI Chip
Document No.: FT_000060
FT4232H QUAD HIGH SPEED USB TO MULTIPURPOSE UART/MPSSE IC
Datasheet Version 2.05
Clearance No.: FTDI#78

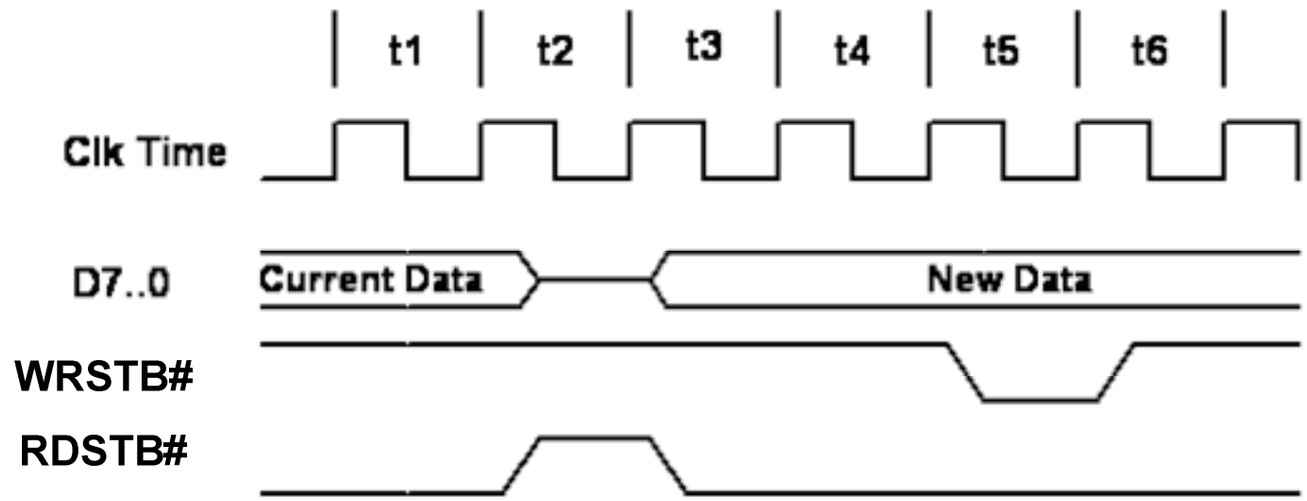


Figure 4.5 Synchronous Bit-Bang Mode Timing Interface Example

no flow control
no sync / ack
no clock

It should be noted that the FT4232H does not output the WRSTB# or RDSTB# signals when configured in bit-bang mode. Figure 4.5. and Table 4.2 show these signals for **illustration** purposes only.

NAME	Description
t1	Current pin state is read
t2	RDSTB# is set inactive and data on the paralle I/O pins is read and sent to the USB host.
t3	RDSTB# is set active again, and any pins that are output will change to their new data
t4	1 clock cycle to allow for data setup
t5	WRSTB# goes active. This indicates that the host PC has written new data to the I/O parallel data
t6	WRSTB# goes inactive

Table 4.2 Synchronous Bit-Bang Mode Timing Interface Example Timings

WRSTB# = this output indicates when new data has been written to the I/O pins from the Host PC (via the USB interface).

RDSTB# = this output rising edge indicates when data has been read from the I/O pins and sent to the Host PC (via the USB interface).

Free Climbing to Highspeed-I/O

FTDI Chip

Document No.: FT_000060
FT4232H QUAD HIGH SPEED USB TO MULTIPURPOSE UART/MPSSE IC
Datasheet Version 2.05
Clearance No.: FTDI#78

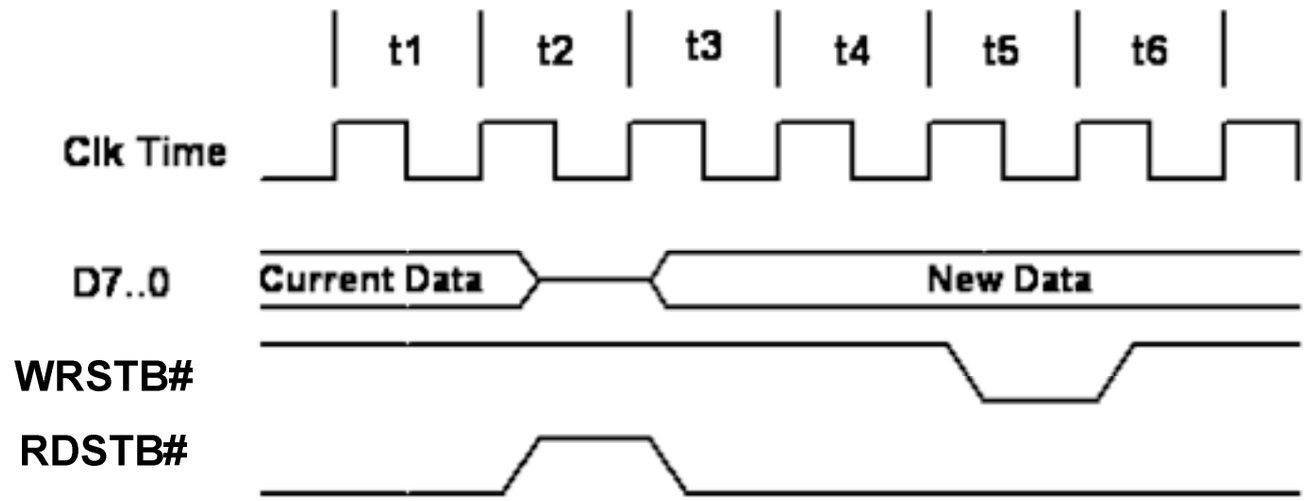


Figure 4.5 Synchronous Bit-Bang Mode Timing Interface Example

It should be noted that the FT4232H does not output the WRSTB# or RDSTB# signals when configured in bit-bang mode. Figure 4.5. and Table 4.2 show these signals for **illustration** purposes only.

NAME	Description
t1	Current pin state is read
t2	RDSTB# is set inactive and data on the paralle I/O pins
t3	RDSTB# is set active again, and any pins that are o
t4	1 clock cycle to allow for data setup
t5	WRSTB# goes active. This indicates that the hos
t6	WRSTB# goes inactive

Table 4.2 Synchronous Bit-Bang Mode Timing Interface Ex

WRSTB# = this output indicates when new data has been w
USB interface).

RDSTB# = this output rising edge indicates when data has been ost
PC (via the USB interface).

no flow control
no sync / ack
no clock

picked the wrong chip

Free Climbing to Highspeed-I/O

FTDI Chip

Document No.: FT_000060
FT4232H QUAD HIGH SPEED USB TO MULTIPURPOSE UART/MPSSE IC
Datasheet Version 2.05
Clearance No.: FTDI#78

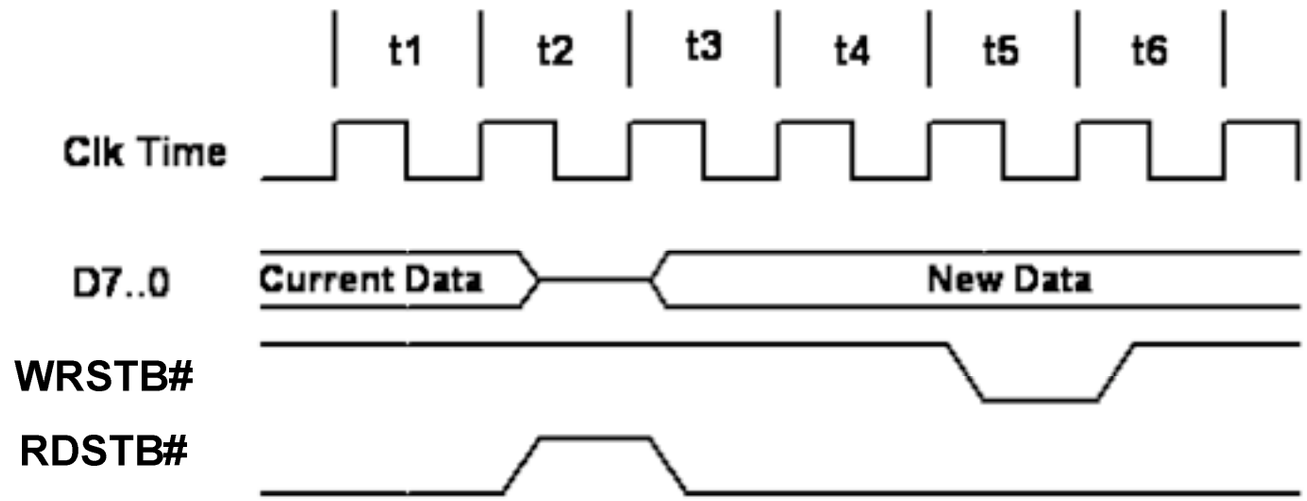


Figure 4.5 Synchronous Bit-Bang Mode Timing Interface Example

It should be noted that the FT4232H does not output the WRSTB# or RDSTB# signals when configured in bit-bang mode. Figure 4.5. and Table 4.2 show these signals for **illustration** purposes only.

NAME	Description
t1	Current pin state is read
t2	RDSTB# is set inactive and data on the paralle I/O pins
t3	RDSTB# is set active again, and any pins that are o
t4	1 clock cycle to allow for data setup
t5	WRSTB# goes active. This indicates that the hos
t6	WRSTB# goes inactive

Table 4.2 Synchronous Bit-Bang Mode Timing Interface Ex

WRSTB# = this output indicates when new data has been w
USB interface).

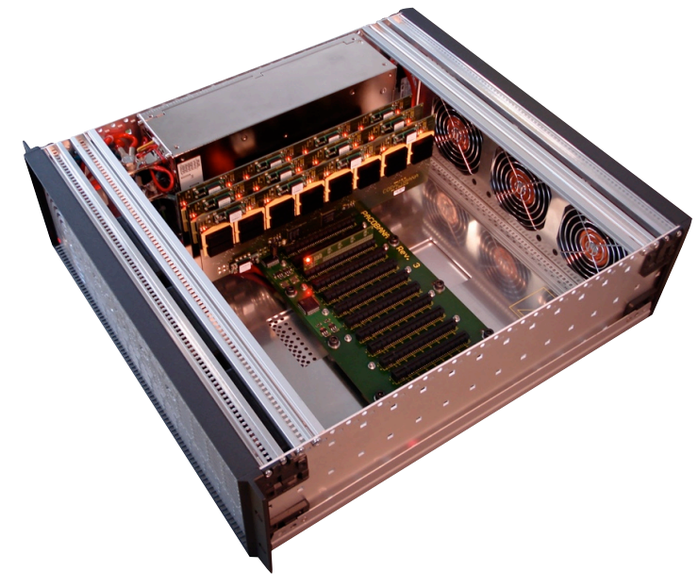
RDSTB# = this output rising edge indicates when data has been ost
PC (via the USB interface).

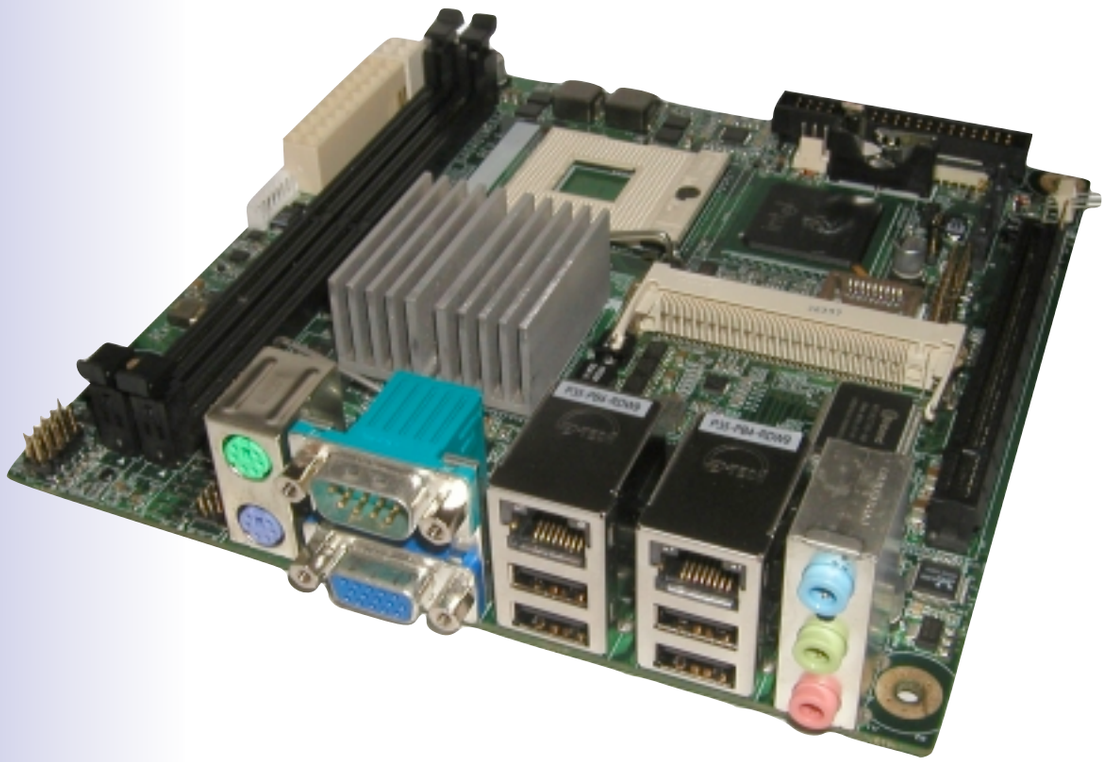
no flow control
no sync / ack
no clock

Solution same Vendor use different a chip

Idea: USB 2.0 (480Mbit) is a commonly used interface

Prototype C





working with good performance

Our Approach

Design goals:

- maximize bandwidth
- availability of memory
- scalability
- cost and performance optimization

moving FPGA computing to a massively parallel architecture

Machine Architecture

Design goal: maximize computational performance

- size of FPGAs
  - Spartan-3 5000
- number of FPGAs
  - at least 128 per machine
- energy per FPGA
  - 7 A, 1.2 V

Design goal: maximize bandwidth

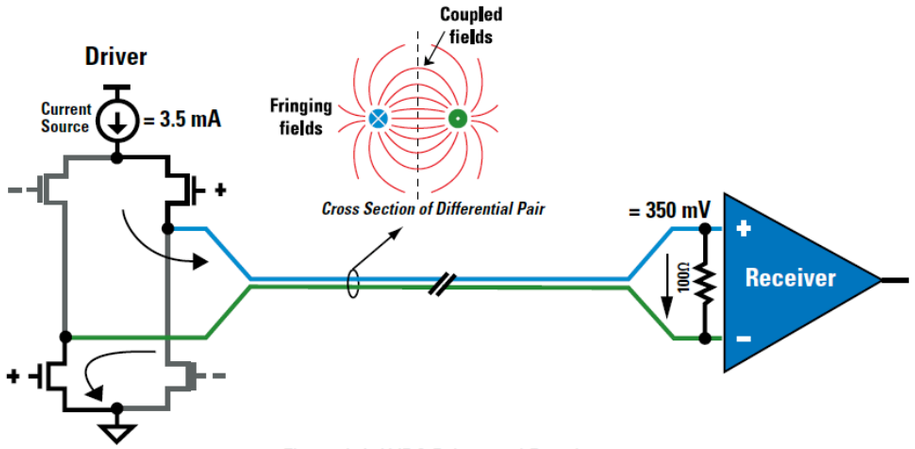
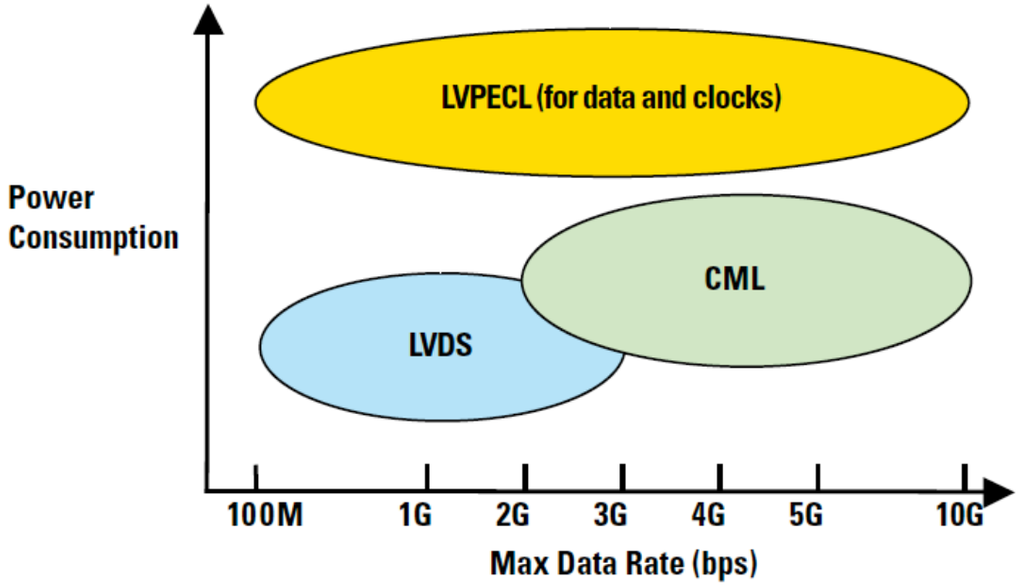


Figure 1-1. LVDS Driver and Receiver

- LVDS
- short and fast lines
- fully impedance-controlled design
- minimum bandwith per differential pair 1Gbit/s



Machine Architecture

Design goal: availability of memory

4 levels of memory

- local memory per FPGA
  - 32 MByte DRAM
- local RAM-Uplink per FPGA
  - 32 GByte Flash (micro SDHC) per FPGA*
- shared memory
  - backplane memory card available
  - 32 GByte DDR3
- hard disk drive*
  - 4 TByte SATAII

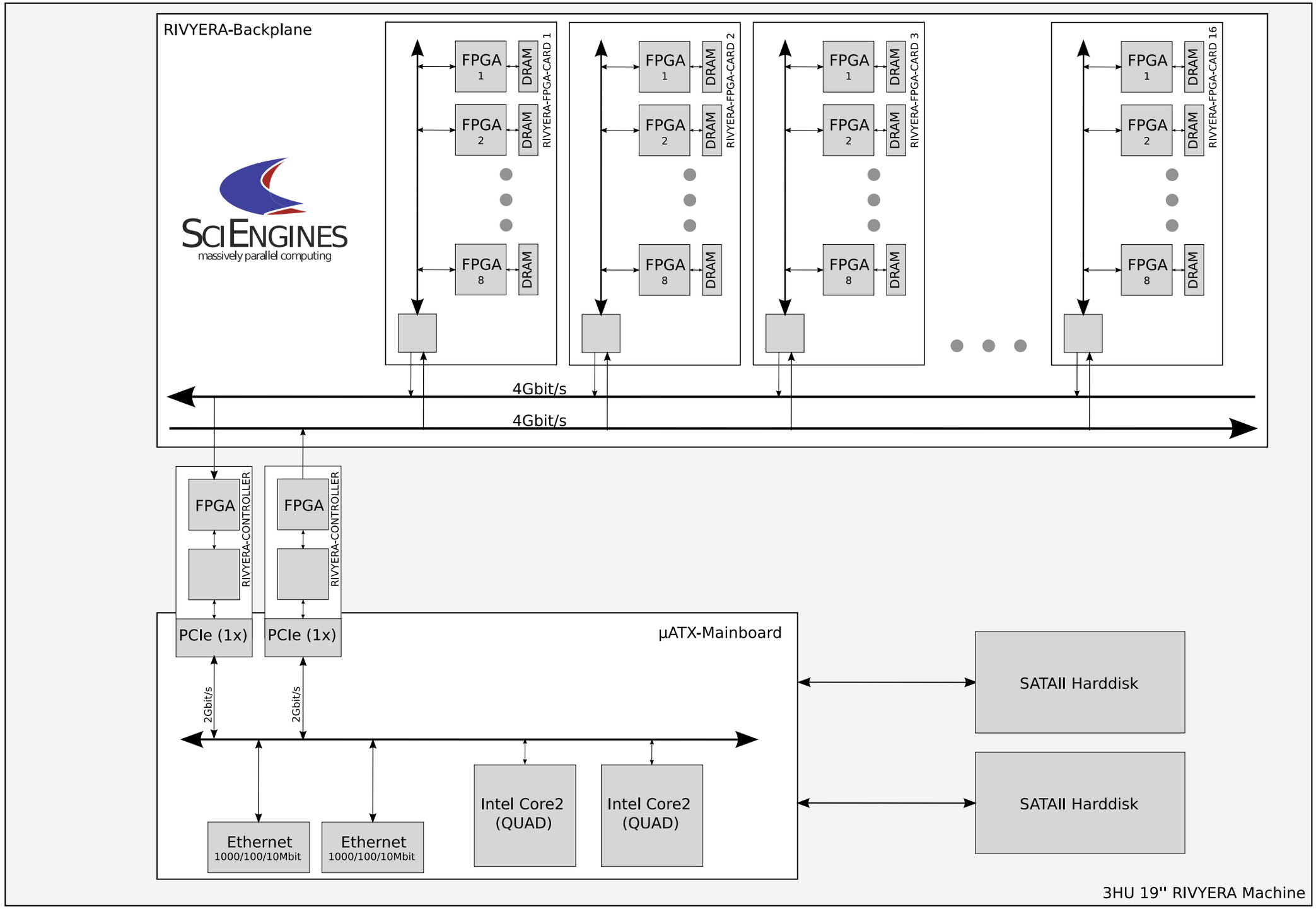
*optional

Design goal: scalability

Fully modular and scalable design

- Scalable thrue uplink
  logically and physically with full backplane bandwidth even beyond machine borders
- 8 FPGAs per FPGA-Card
  Spartan-3 5000, 32 MByte DRAM
- Controller-Card
  PCI-Express / Backplane
- Backplane
  18 identical slots
- Integraded µATX-PC
- Industry 3-HU-Rack-Enclosure

Machine Architecture

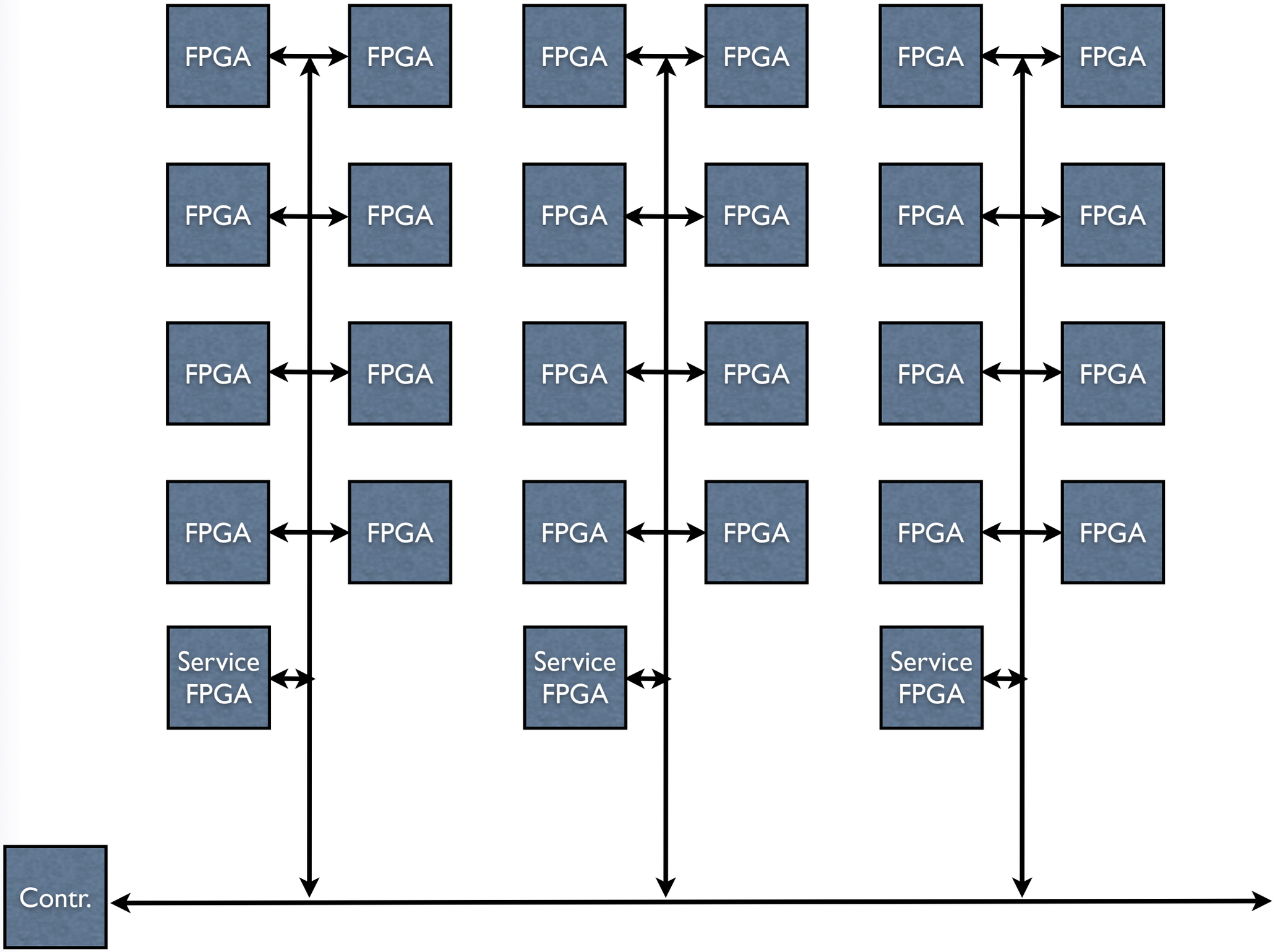


Machine Architecture

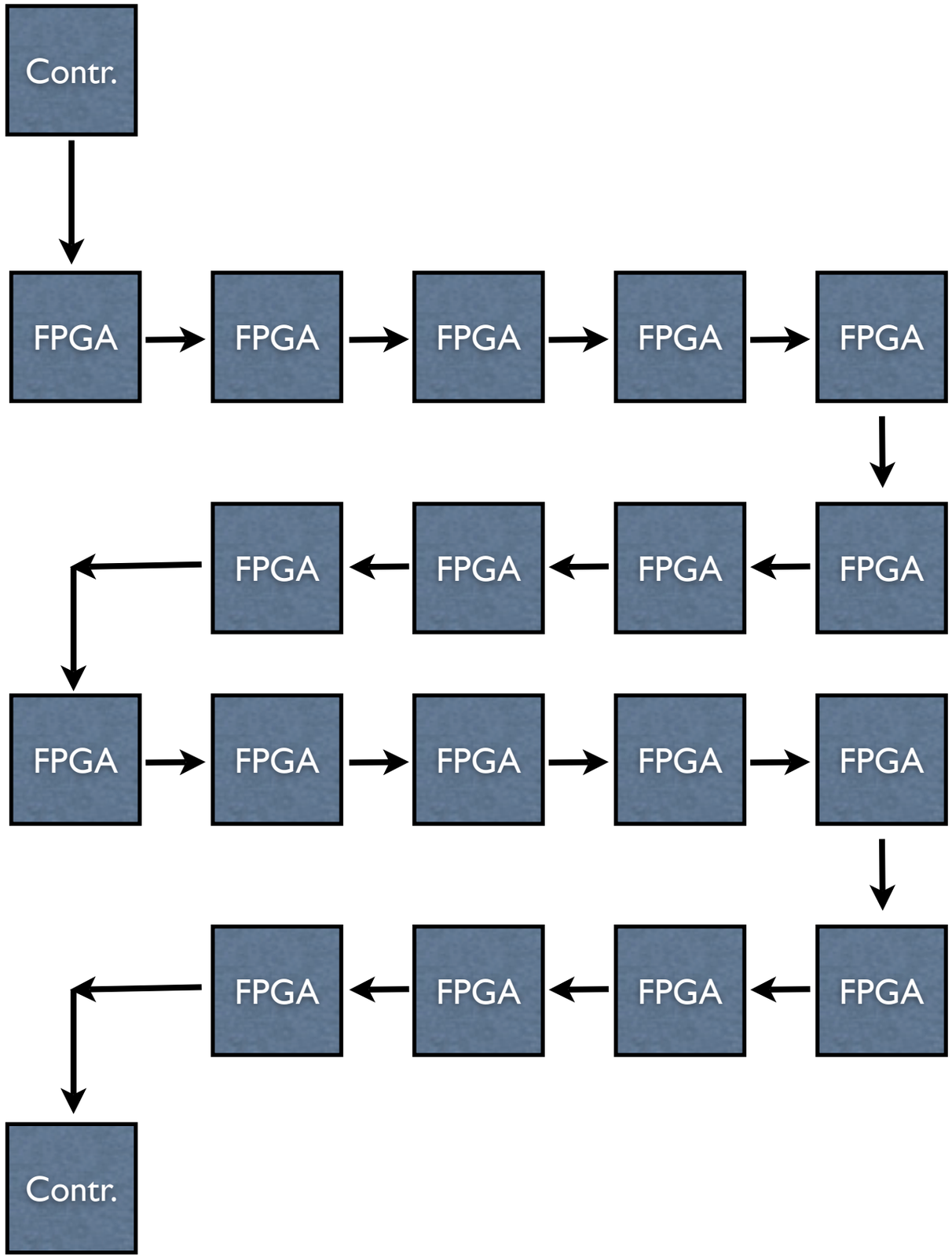
- three independent bus systems
  - JTAG e.g. configuration, debug
  - shared bus e.g. configuration, debug, broadcast
  - point to point 16 lanes, direction configurable
- 4 firmware assisted communication schemes
  - memory mapped I/O
  - lineare systolic array
  - one to many / one to all
  - user*

* not recomended

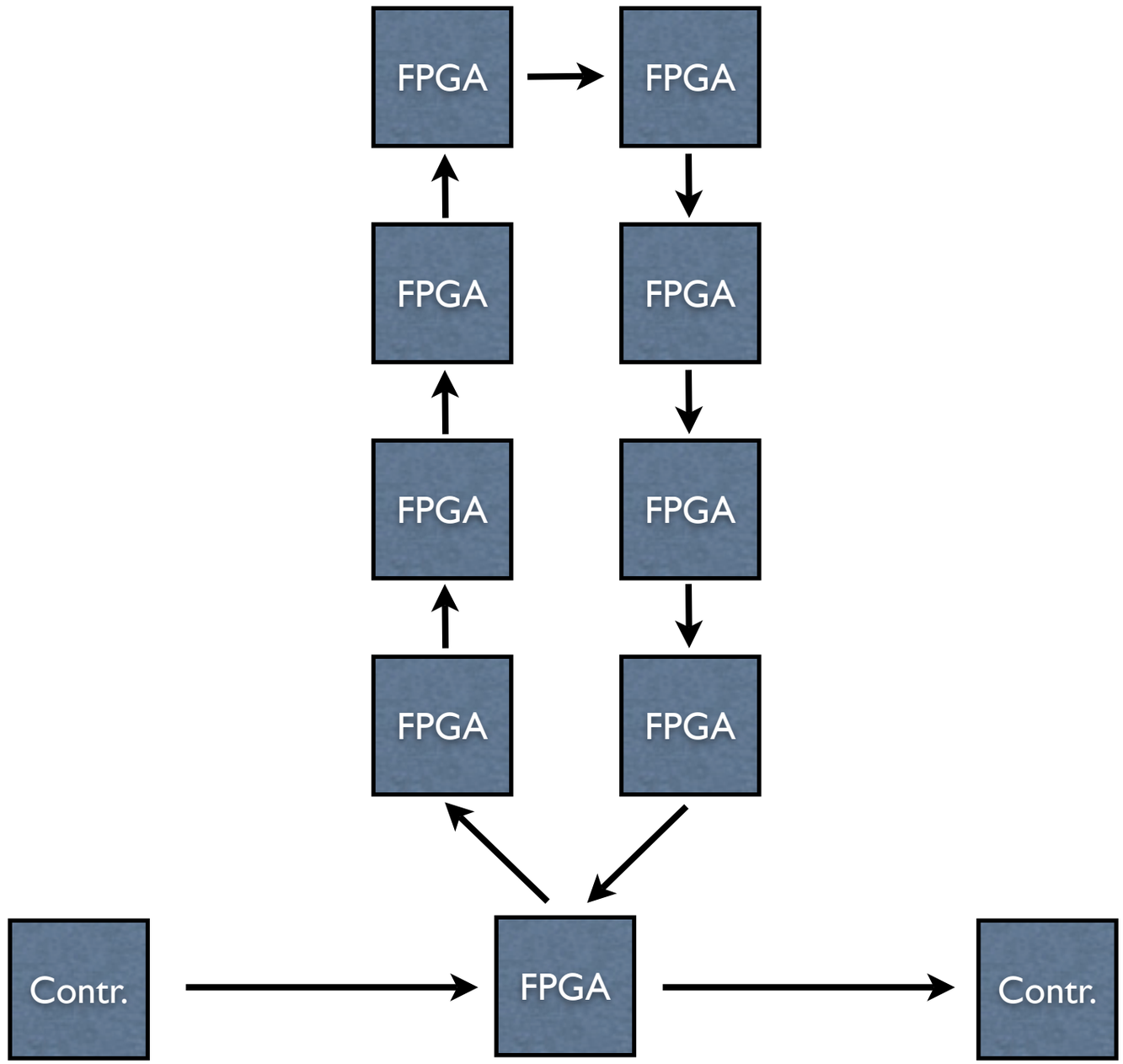
Machine Architecture



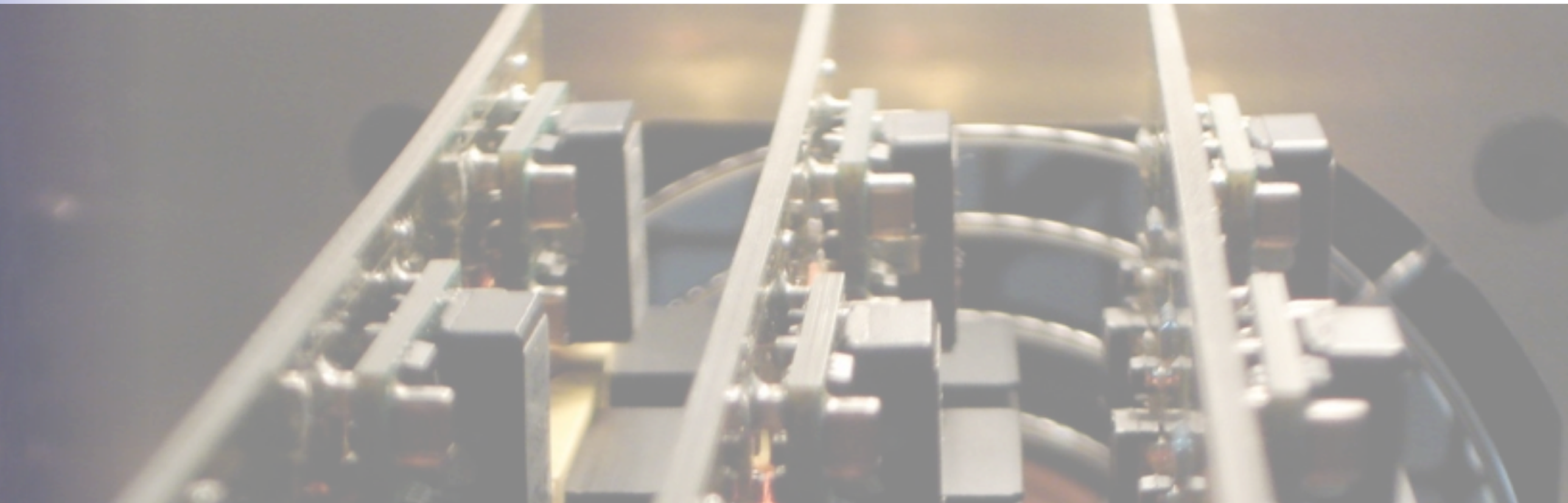
Machine Architecture



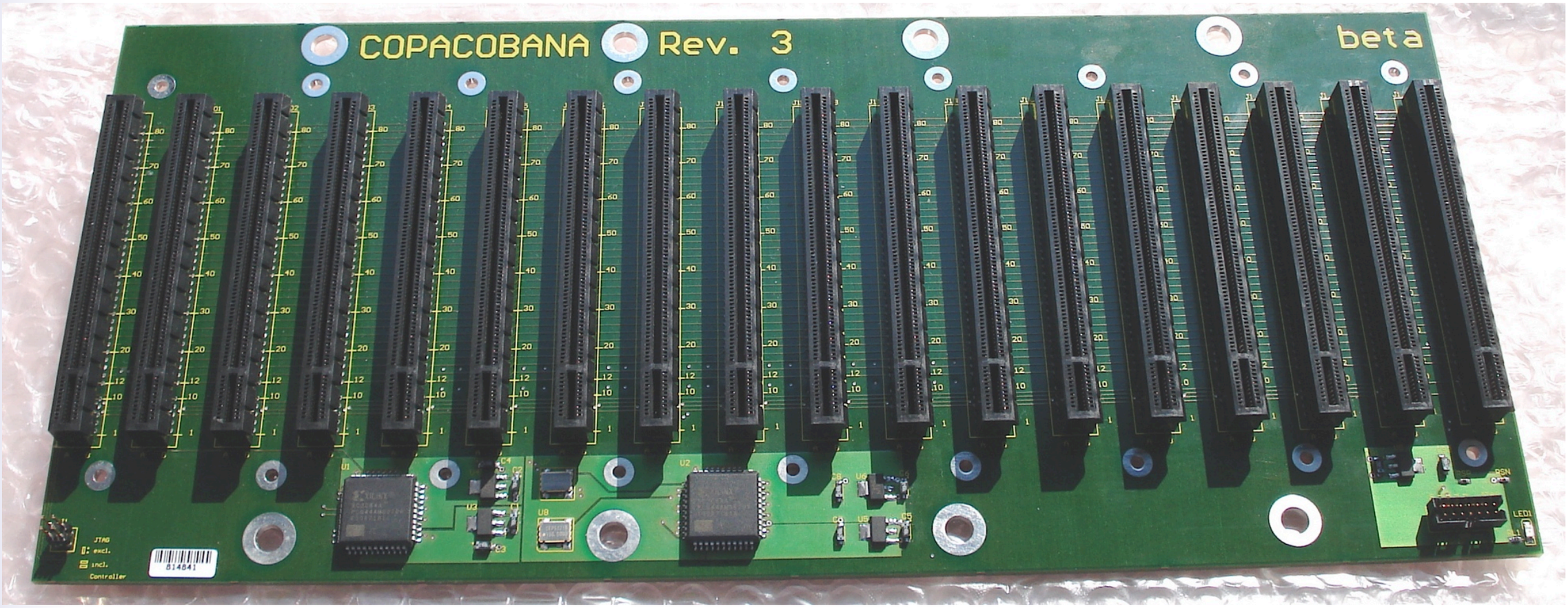
Machine Architecture



- About us
- Motivation
- Todays Approaches
- Our Approach
- Performance Evaluation
- **Conclusion and Comments**

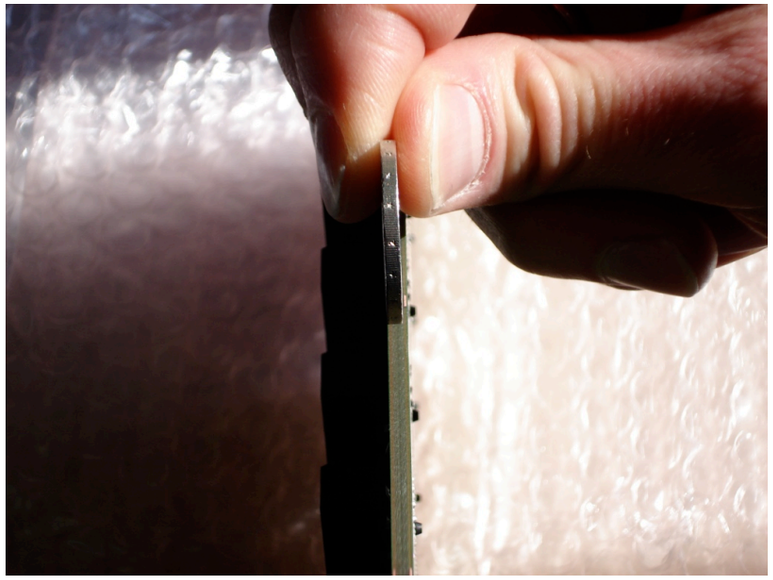


Prototype Backplane

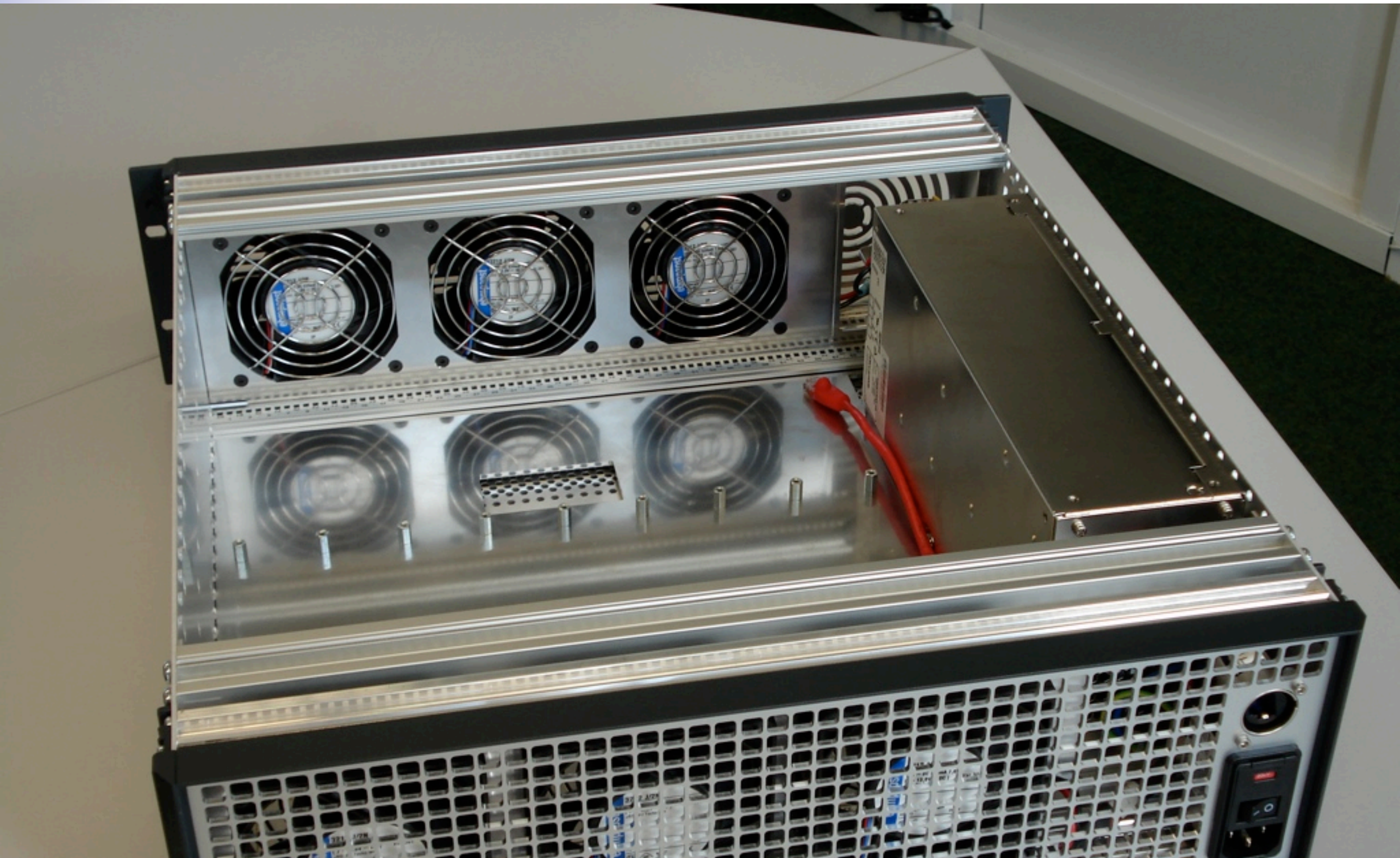


4.25 mm

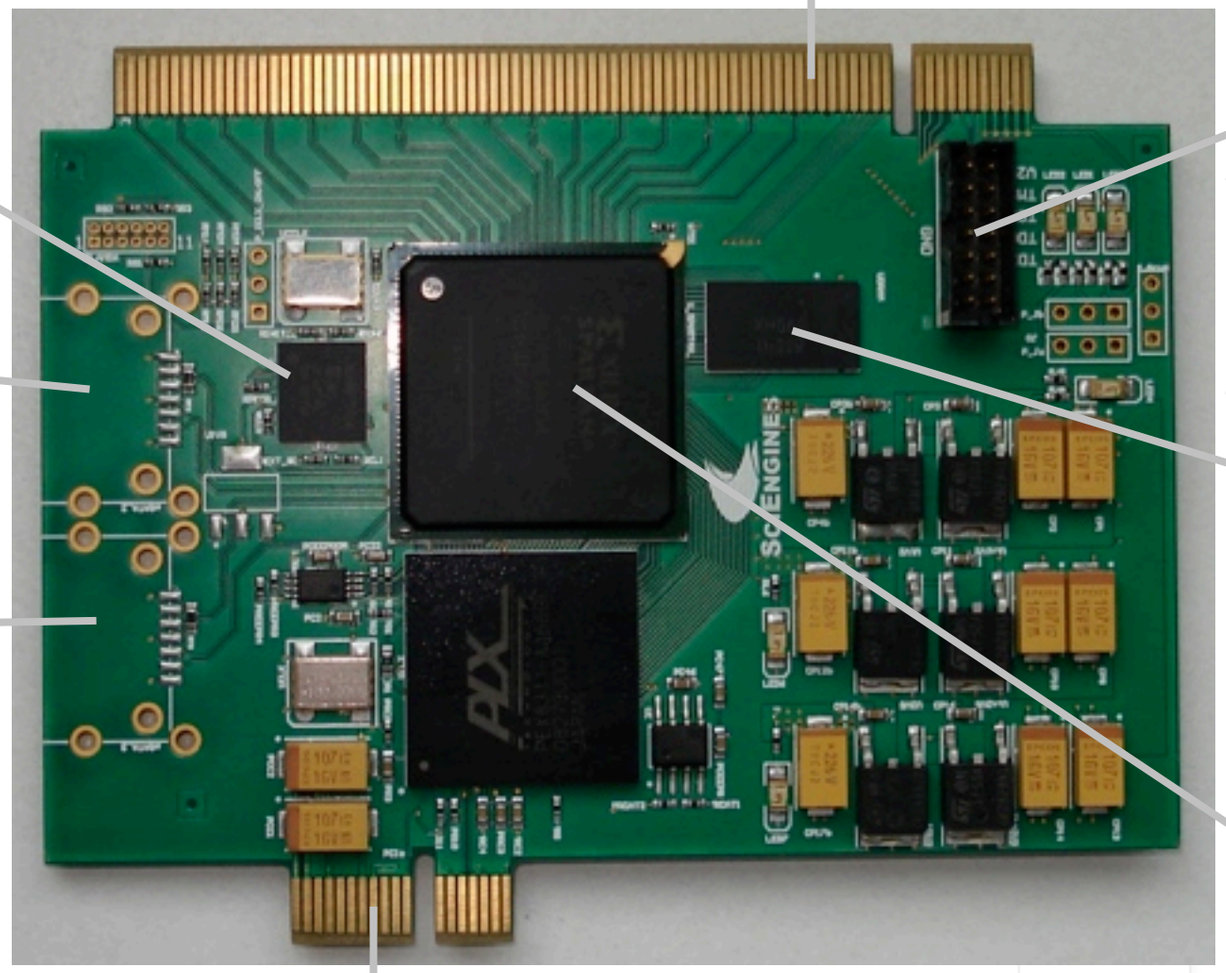
8 Layers



Prototype Enclosure



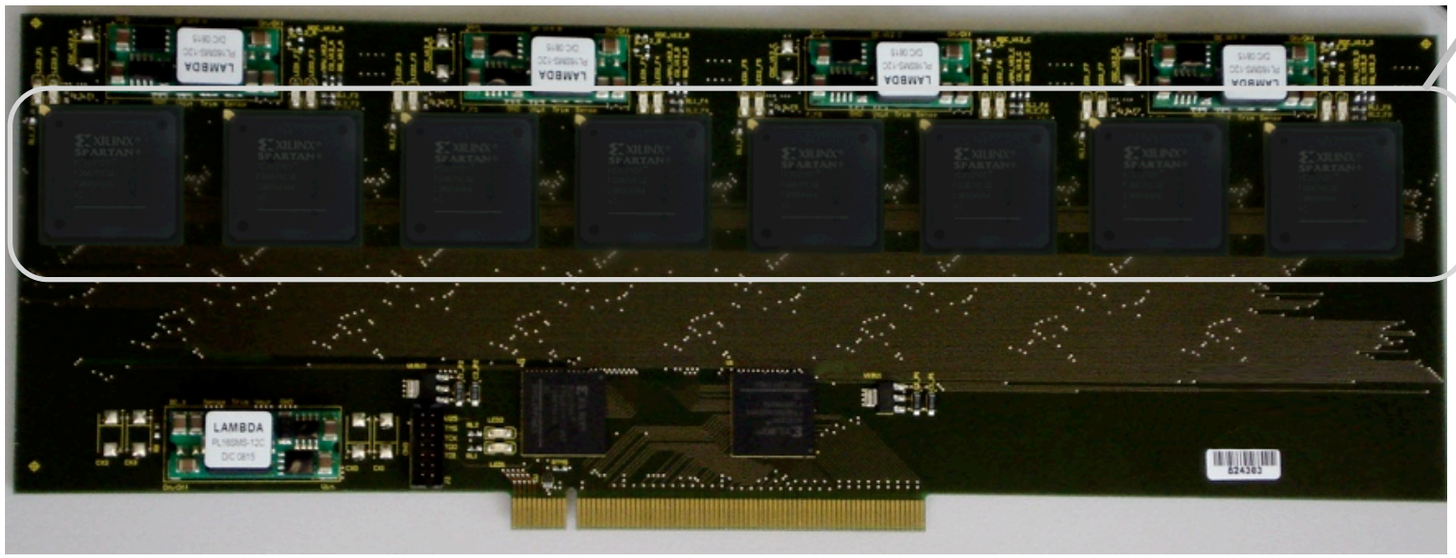
Prototype Controller



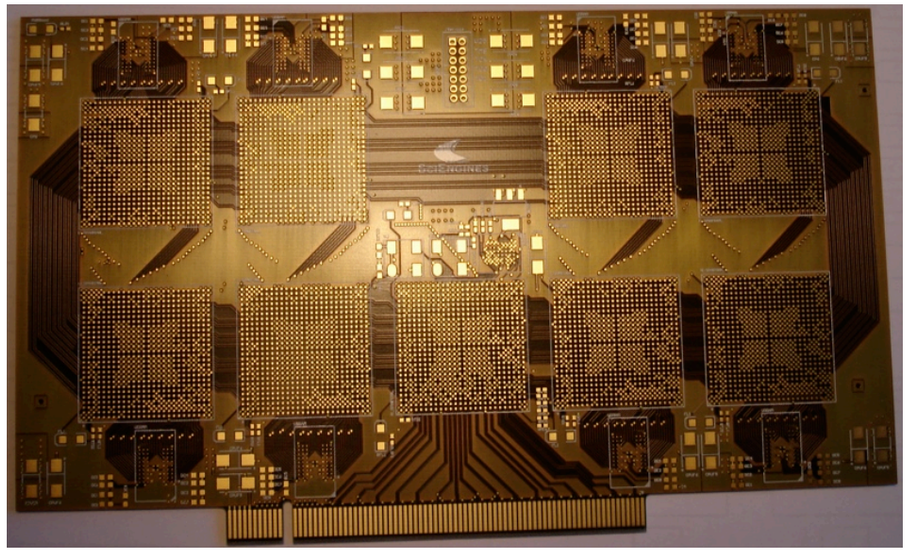
Sneak Preview: FPGA-Card

functional non cost optimized prototype without DRAM

8 x Spartan-3 5000

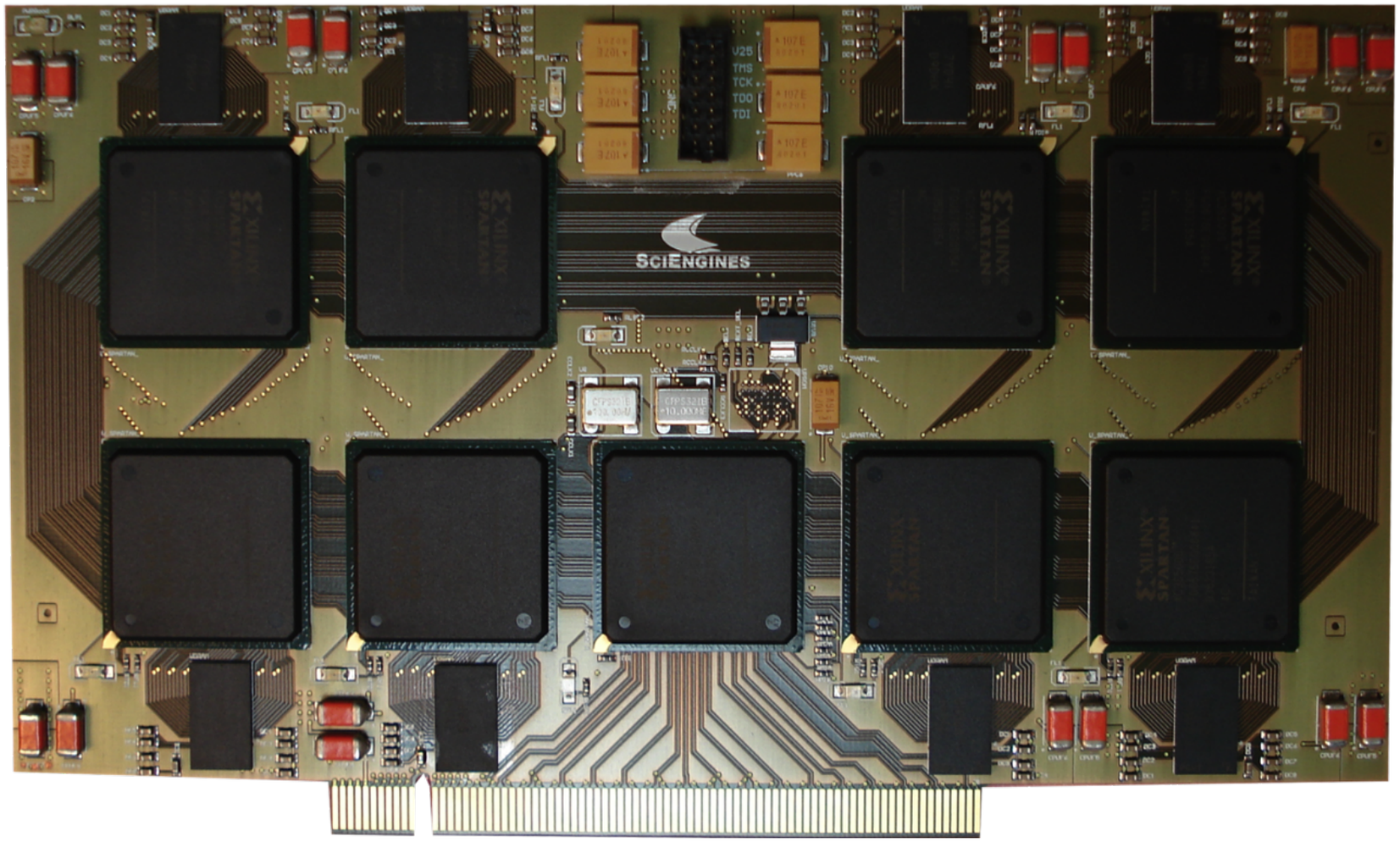


pre production series rev. 2
PCB

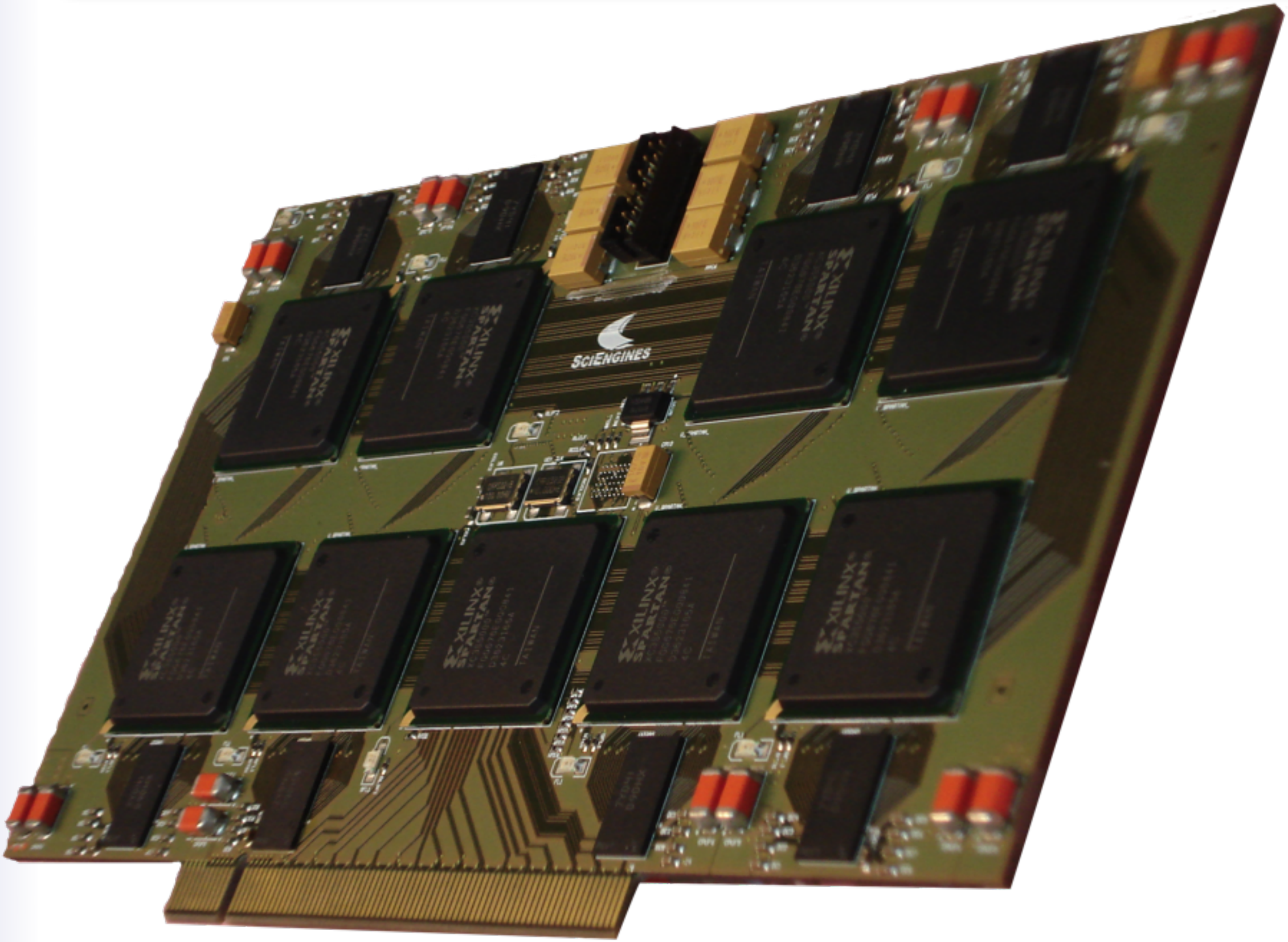


- half the physical length
- same height
- twice the bus bandwidth

Sneak Preview: FPGA-Card



Sneak Preview: FPGA-Card



COPACOBANA RIVYERA

Green Super Computing

Thank You !

QUESTIONS ?

Contact:

Gerd Pfeiffer
Geschäftsführer CEO

Jost Bissel
Chief Software Architect CSA

Stefan Baumgart
Chief Hardware Engineer CHE

info@sciengines.com
www.sciengines.com