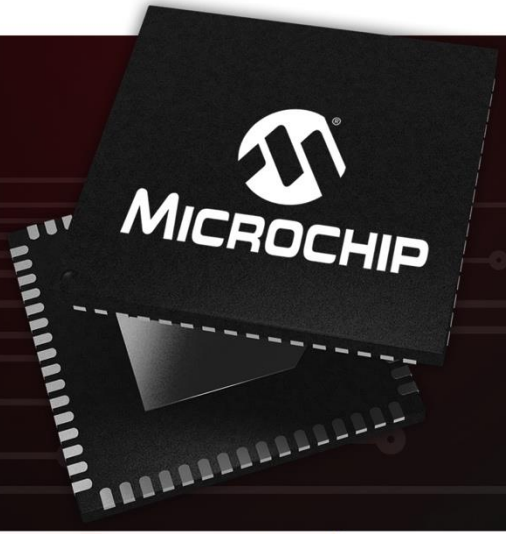
MICROCHIP



A Leading Provider of Microcontroller, Security, Mixed-Signal, Analog & Flash-IP Solutions




Securing the New Golden Age of Computer Architecture

Ted Speers, Head Of Product Arch & Planning

March 13, 2019

About Microchip FPGAs

Number One from Low Earth Orbit to Beyond Pluto

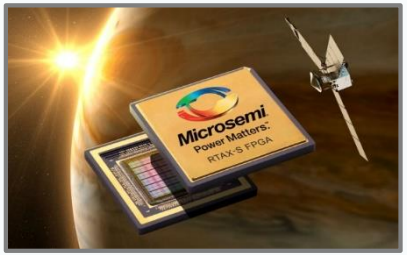
Rosetta
Orbits and Lands on Comet 2014

Legacy RT FPGAs

Pluto New Horizons
Pluto Images 2015

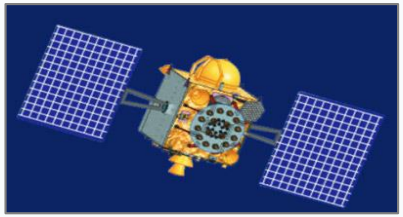
RTSX32SU, RTSX72SU

JUNO
Entered Jupiter Orbit 2016



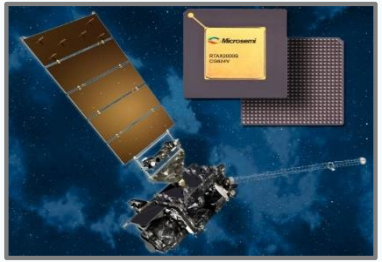
RTSX32SU, RTAX250S, RTAX2000S

IRNSS
7 Satellites Launched 2013-2016



RTAX2000S

GOES-R
Climate Satellite Launched 2016



RTSX72SU, RTAX2000S

Iridium Next
First 10 Satellites Launched 2017

RTSX32SU, RTAX250S, RTAX1000S, RT3PE3000L

Number One Above 30000 Feet

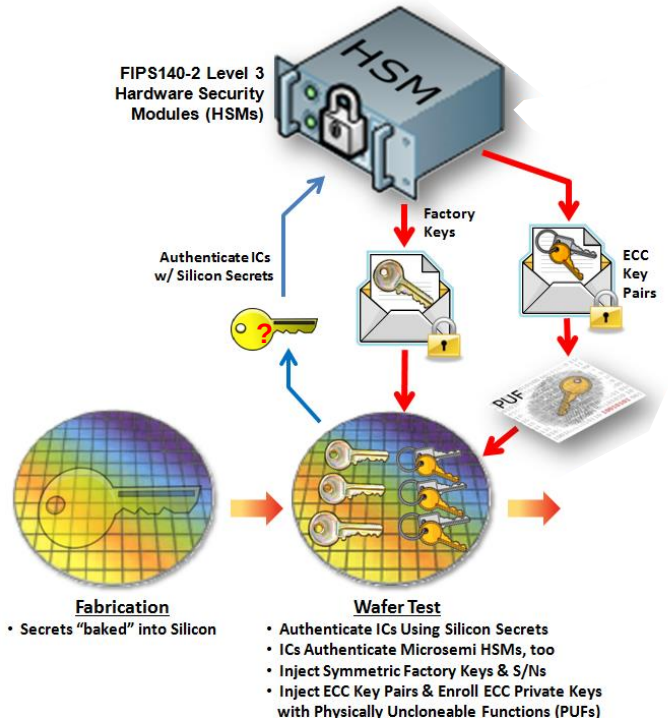
Airbus A380
- APA, A500K, SX-A, AX FPGAs
- Flight computers, cockpit displays, engine controls, power distribution, . . .

Boeing 787 Dreamliner
- APA, A3P, AX FPGAs
- Flight computers, cockpit displays, engine controls, braking, power distribution, cabin pressure, flight surface actuation . . .

Boeing 777-300ER
- A3P, Igloo2 FPGAs
- Flight computers, power distribution, engine controls, electronic control networks, flight surface actuation. . .

Airbus A350 XWB
- APA, A3P FPGAs
- Flight computers, cockpit displays, braking, engine controls, power distribution, cabin pressure, flight surface actuation . . .

Comprehensive Womb-to-Tomb Security Architecture



Award Winning PolarFire FPGA as an SoC platform

Lowest Power
- Low static power technology
- Power optimized transceivers
- Up to 50% lower than SRAM FPGAs

Proven Security
- Defense-grade security
- DPA safe Crypto coprocessor
- Built-in anti-tamper

Exceptional Reliability
- SEU immune configuration
- Block RAM with ECC
- Extended temperatures

10G Bridging & Aggregation

Video & Image Processing

Portable Equipment

Signal Processing

Control Plane

Hardware Acceleration

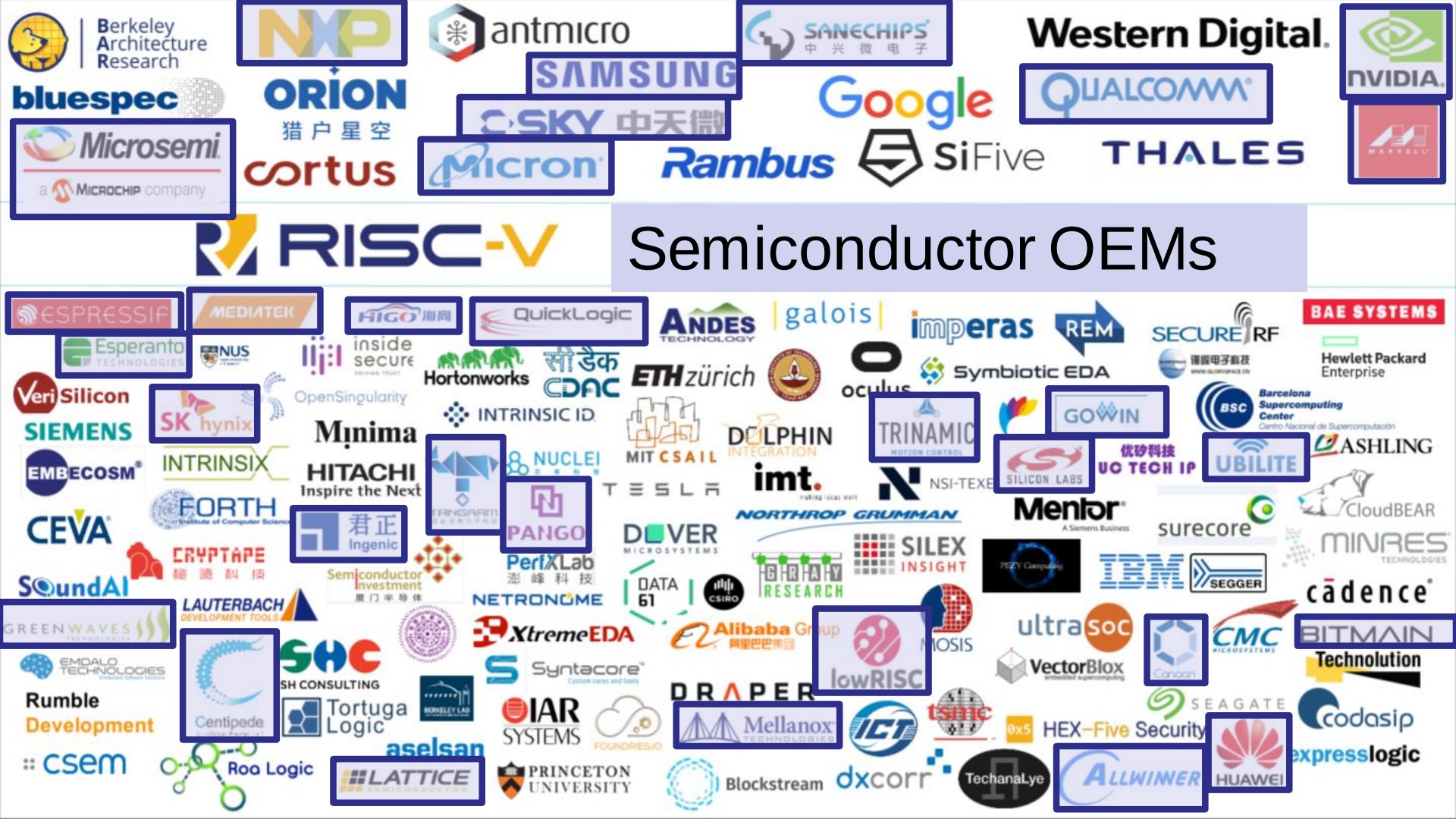
Low Power Optics

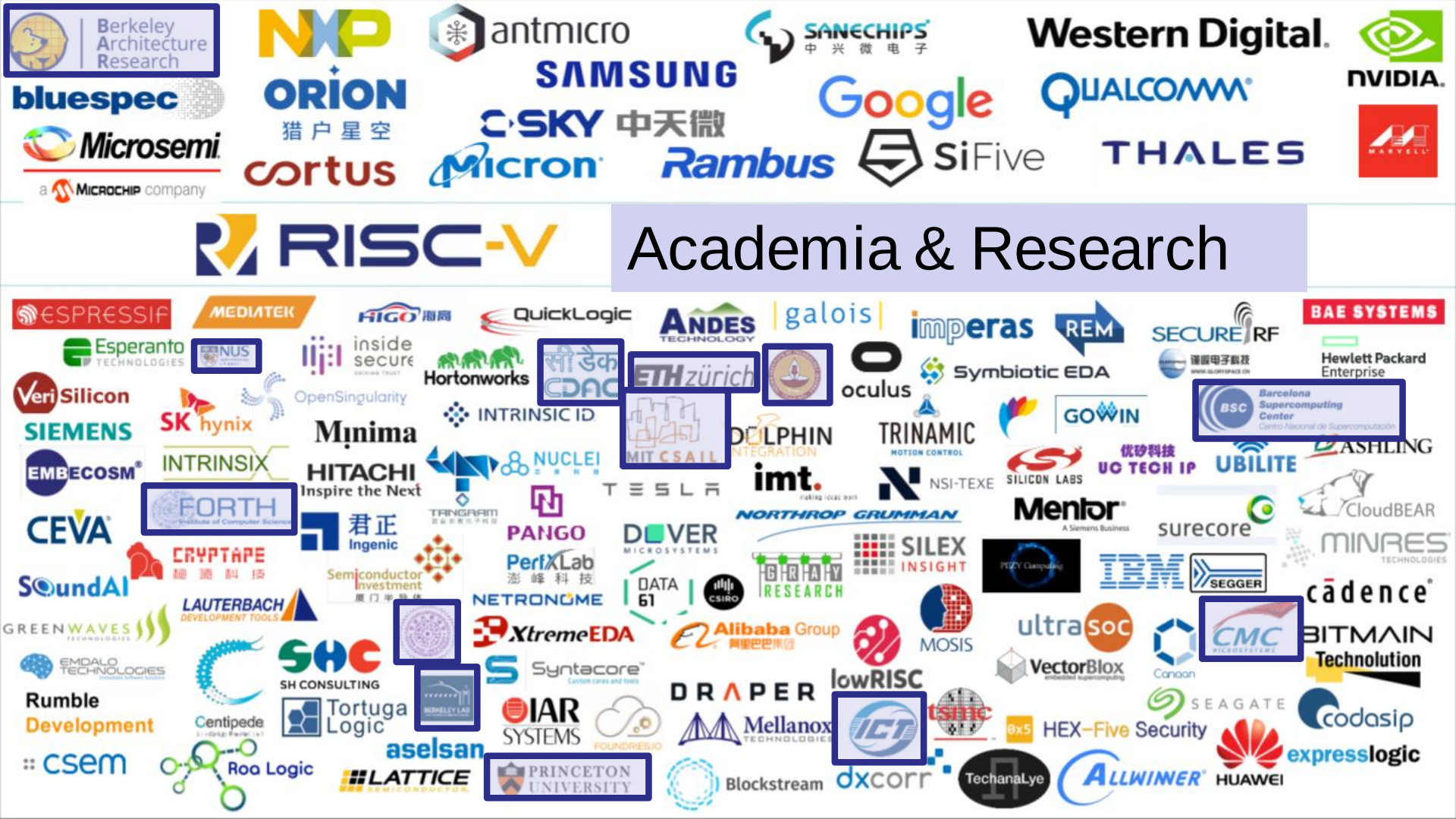
Who joins the RISC-V Foundation?


Berkeley Architecture Research
NXP
antmicro
SANECHIPS 中兴微电子
Western Digital.
NVIDIA.
bluespec
ORION 猎户星空
SAMSUNG
Google
QUALCOMM
C-SKY 中天微
Microsemi a MICROCHIP company
cortus
Micron
Rambus
SiFive
THALES
RISC-V
Foundation: 200+ Members
ESPRESSIF
MEDIATEK
HiGo 海高
QuickLogic
ANDES TECHNOLOGY
galois
imperas
REM
SECURE RF
BAE SYSTEMS
Esperanto TECHNOLOGIES
NUS
inside secure
Hortonworks
सी डैक CDAC
ETH zürich
oculus
Symbiotic EDA
Hewlett Packard Enterprise
VeriSilicon
OpenSingularity
INTRINSIC ID
GOWIN
Barcelona Supercomputing Center
SIEMENS
SK hynix
Minima
MIT CSAIL
DOLPHIN INTEGRATION
TRINAMIC MOTION CONTROL
ASHLING
EMBECOSM
INTRINSIX
HITACHI Inspire the Next
NUCLEI
TESLA
imt.
NSI-TEXE
SILICON LABS
优矽科技 UC TECH IP
UBILITE
CloudBEAR
FORTH Institute of Computer Science
TANGRAM
PANGO
NORTHROP GRUMMAN
Mentor A Siemens Business
surecore
CEVA
君正 Ingenic
DOVER MICROSYSTEMS
SILEX INSIGHT
MINRES TECHNOLOGIES
CRYPTAPE 楠菱科技
Semiconductor Investment 厦门半导体
PerfXLab 澎峰科技
GRAY RESEARCH
PEZY Computing
IBM
SEGGER
SoundAI
DATA 61
CSIRO
cadence
LAUTERBACH DEVELOPMENT TOOLS
NETRONOME
GREENWAVES TECHNOLOGIES
XtremeEDA
Alibaba Group 阿里巴巴集团
MOSIS
ultraSoc
CMC MICROSYSTEMS
BITMAIN Technolution
EMDALO TECHNOLOGIES
SHC SH CONSULTING
Syntacore
VectorBlox
Canaan
Rumble Development
lowRISC
DRAPER
SEAGATE
Centipede
Tortuga Logic
IAR SYSTEMS
FOUNDRIES.IO
Mellanox TECHNOLOGIES
ICT
tsmc
0x5
HEX-Five Security
codasip
csem
Roa Logic
aselsan
LATTICE SEMICONDUCTOR
PRINCETON UNIVERSITY
Blockstream
dxcorr
TechanaLye
ALLWINNER
HUAWEI
expresslogic

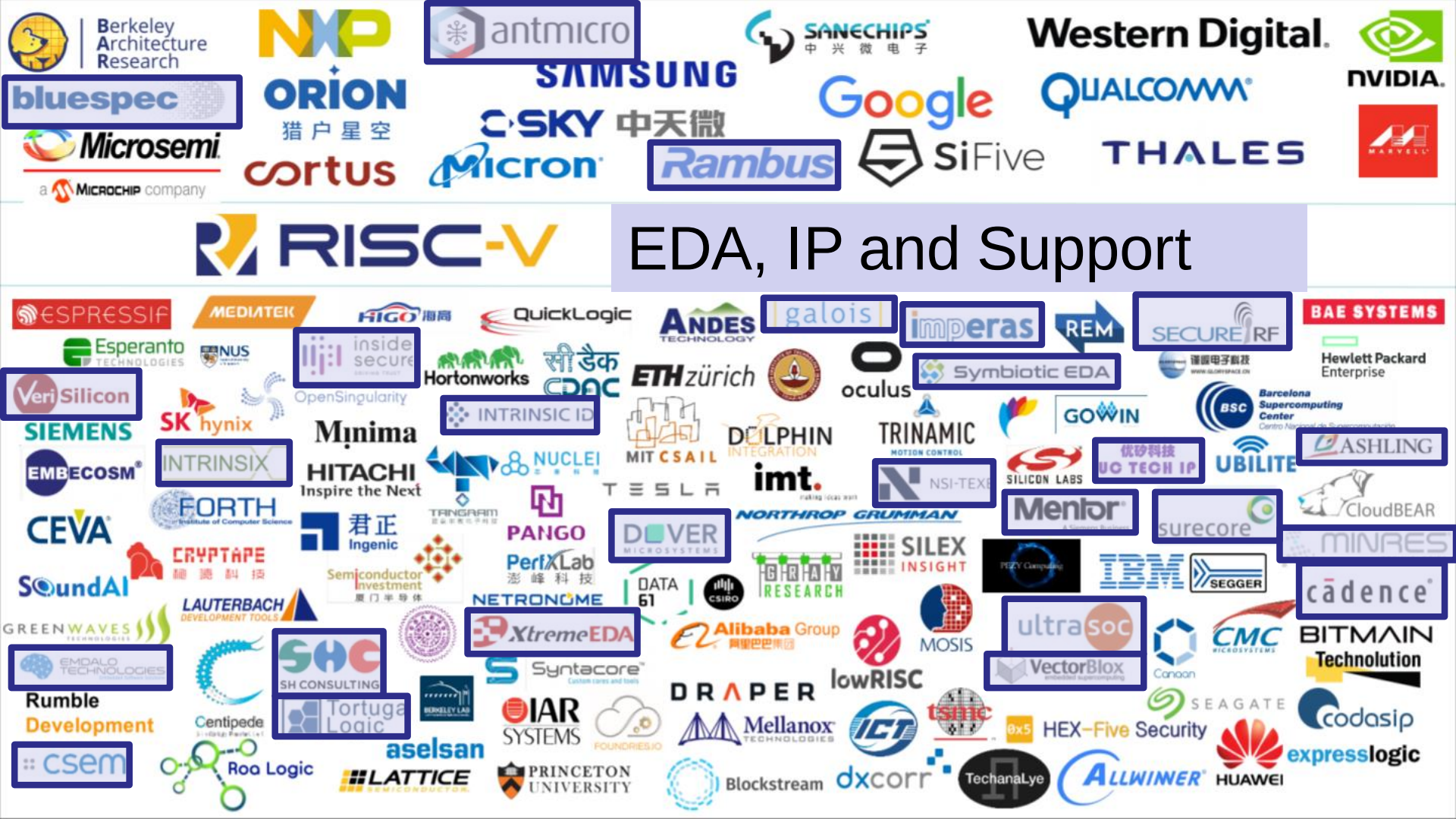

Berkeley Architecture Research
NXP
antmicro
SANECHIPS 中兴微电子
Western Digital
NVIDIA
bluespec
ORION 猎户星空
SAMSUNG
Google
QUALCOMM
Microsemi a Microchip company
C-SKY 中天微
cortus
Micron
Rambus
SiFive
THALES
MARVELL
RISC-V
Board of Directors
ESPRESSIF
MEDIATEK
HiGo 海高
QuickLogic
ANDES TECHNOLOGY
galois
imperas
REM
SECURE RF
BAE SYSTEMS
Esperanto TECHNOLOGIES
NUS
inside secure
Hortonworks
सी डैक CDAC
ETH zürich
oculus
Symbiotic EDA
Hewlett Packard Enterprise
VeriSilicon
OpenSingularity
INTRINSIC ID
GOWIN
BSC Barcelona Supercomputing Center
SIEMENS
SK hynix
Minima
MIT CSAIL
DOLPHIN INTEGRATION
TRINAMIC MOTION CONTROL
ASHLING
EMBECOSM
INTRINSIX
HITACHI Inspire the Next
NUCLEI
TESLA
imt.
NSI-TEXE
SILICON LABS
优矽科技 UC TECH IP
UBILITE
CloudBEAR
FORTH Institute of Computer Science
TANGRAM
PANGO
NORTHROP GRUMMAN
Mentor A Siemens Business
surecore
CEVA
君正 Ingenic
DOVER MICROSYSTEMS
SILEX INSIGHT
MINRES TECHNOLOGIES
CRYPTAPE 楠菱科技
Semiconductor Investment 厦门半导体
PerfXLab 澎峰科技
GRAHAY RESEARCH
IBM
SEGGER
SoundAI
DATA 61
CSIRO
cadence
LAUTERBACH DEVELOPMENT TOOLS
NETRONOME
ultraSoC
CMC MICROSYSTEMS
BITMAIN Technolution
GREENWAVES TECHNOLOGIES
XtremeEDA
Alibaba Group 阿里巴巴集团
MOSIS
Canaan
EMDALO TECHNOLOGIES
SHC SH CONSULTING
Syntacore
VectorBlox
lowRISC
Rumble Development
DRAPER
SEAGATE
codasip
Centipede
Tortuga Logic
IAR SYSTEMS
FOUNDRIES.IO
Mellanox TECHNOLOGIES
ICT
tsmc
0x5 HEX-Five Security
csem
aselsan
Roa Logic
LATTICE SEMICONDUCTOR
PRINCETON UNIVERSITY
Blockstream
dxcorr
TechanaLye
ALLWINNER
HUAWEI
expresslogic

RISC-V IP Providers

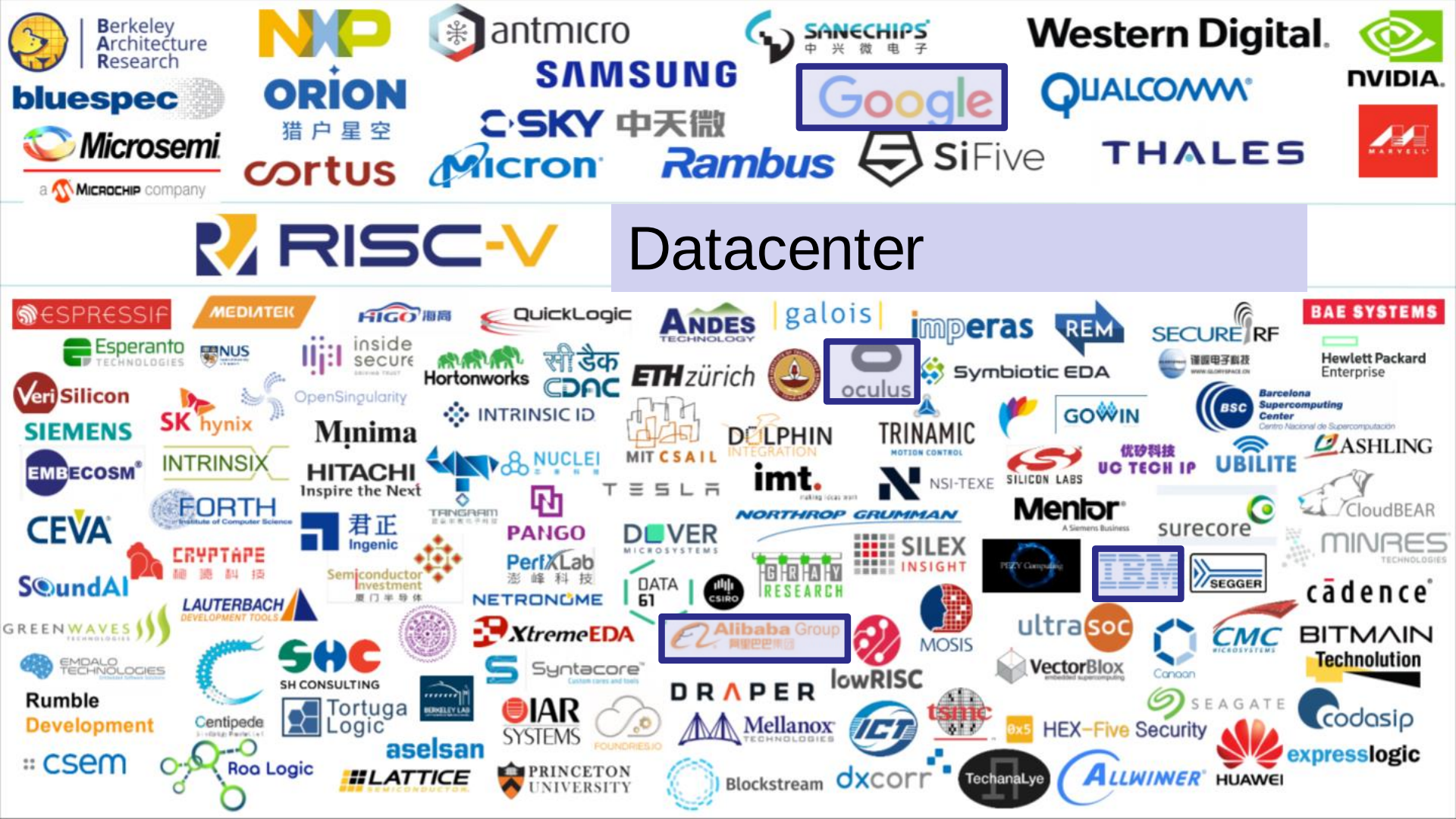

Berkeley Architecture Research
NXP
antmicro
SANECHIPS 中兴微电子
Western Digital
NVIDIA
SAMSUNG
bluespec
ORION 猎户星空
Google
QUALCOMM
SKY 中天微
Microsemi a Microchip company
cortus
Micron
Rambus
SiFive
THALES
MARVELL
RISC-V
Semiconductor OEMs
ESPRESSIF
MEDIATEK
HiGo 海高
QuickLogic
ANDES TECHNOLOGY
galois
imperas
REM
SECURE RF
BAE SYSTEMS
Esperanto TECHNOLOGIES
NUS
inside secure
Hortonworks
सी डैक CDAC
ETH zürich
oculus
Symbiotic EDA
Hewlett Packard Enterprise
VeriSilicon
SIEMENS
SK hynix
OpenSingularity
INTRINSIC ID
Minima
TRINAMIC MOTION CONTROL
GOWIN
BSC Barcelona Supercomputing Center Centro Nacional de Supercomputación
EMBECOSM
INTRINSIX
HITACHI Inspire the Next
MIT CSAIL
DOLPHIN INTEGRATION
SILICON LABS
优矽科技 UC TECH IP
UBILITE
ASHLING
NUCLEI
TESLA
imt.
NSI-TEXE
FORTH Institute of Computer Science
PANGO
Mentor A Siemens Business
surecore
CloudBEAR
CEVA
君正 Ingenic
DOVER MICROSYSTEMS
NORTHROP GRUMMAN
SILEX INSIGHT
IBM
SEGGER
MINRES TECHNOLOGIES
CRYPTAPE 楠菱科技
PerfXLab 澎峰科技
GRAY RESEARCH
SoundAI
Semiconductor Investment 厦门半导体
DATA 61
CSIRO
NETRONOME
cadence
GREENWAVES TECHNOLOGY
LAUTERBACH DEVELOPMENT TOOLS
XtremeEDA
Alibaba Group 阿里巴巴集团
lowRISC
MOSIS
ultraSoC
VectorBlox
CMC MICROSYSTEMS
BITMAN
Technolution
EMDALO TECHNOLOGIES
SHC SH CONSULTING
Syntacore
Rumble Development
Centipede
Tortuga Logic
BERKELEY LAB
DRAPER
IAR SYSTEMS
FOUNDRIES.IO
Mellanox TECHNOLOGIES
ICT
tsmc
0x5
HEX-Five Security
SEAGATE
codasip
csem
Roa Logic
aselsan
LATTICE SEMICONDUCTOR
PRINCETON UNIVERSITY
Blockstream
dxcorr
TechanaLye
ALLWINNER
HUAWEI
expresslogic


Berkeley Architecture Research
NXP
antmicro
SANECHIPS 中兴微电子
Western Digital
NVIDIA
SAMSUNG
bluespec
ORION 猎户星空
Google
QUALCOMM
C-SKY 中天微
Microsemi
a MICROCHIP company
cortus
Micron
Rambus
SiFive
THALES
RISC-V
Academia & Research
ESPRESSIF
MEDIATEK
HiGO 海高
QuickLogic
ANDES TECHNOLOGY
galois
imperas
REM
SECURE RF
BAE SYSTEMS
Esperanto TECHNOLOGIES
NUS
inside secure
Hortonworks
CDAC
ETH zürich
oculus
Symbiotic EDA
Hewlett Packard Enterprise
VeriSilicon
OpenSingularity
INTRINSIC ID
MIT CSAIL
GOWIN
Barcelona Supercomputing Center
SIEMENS
SK hynix
Minima
DOLPHIN INTEGRATION
TRINAMIC MOTION CONTROL
ASHLING
EMBECOSM
INTRINSIX
HITACHI Inspire the Next
NUCLEI
TANGRAM
TESLA
imt.
NSI-TEXE
SILICON LABS
UC TECH IP
UBILITE
FORTH
CloudBEAR
CEVA
君正 Ingenic
PANGO
DOVER MICROSYSTEMS
NORTHROP GRUMMAN
Mentor A Siemens Business
surecore
MINRES TECHNOLOGIES
CRYPTAPE
PerfXLab 澎峰科技
SILEX INSIGHT
IBM
SEGGER
SoundAI
Semiconductor Investment
DATA 61
CSIRO
GRAY RESEARCH
cadence
LAUTERBACH DEVELOPMENT TOOLS
NETRONOME
GREENWAVES TECHNOLOGIES
XtremeEDA
Alibaba Group
MOSIS
ultraSoC
CMC MICROSYSTEMS
BITMAIN
Technolution
EMDALO TECHNOLOGIES
SHC
SH CONSULTING
Syntacore
VectorBlox
Canaan
Rumble Development
Centipede
Tortuga Logic
BERKELEY LAB
DRAPER
lowRISC
SEAGATE
IAR SYSTEMS
FOUNDRIESJO
Mellanox TECHNOLOGIES
ICT
tsmc
0x5
HEX-Five Security
codasip
csem
Roa Logic
aselsan
LATTICE SEMICONDUCTOR
PRINCETON UNIVERSITY
Blockstream
dxcorr
TechanaLye
ALLWINNER
HUAWEI
expresslogic

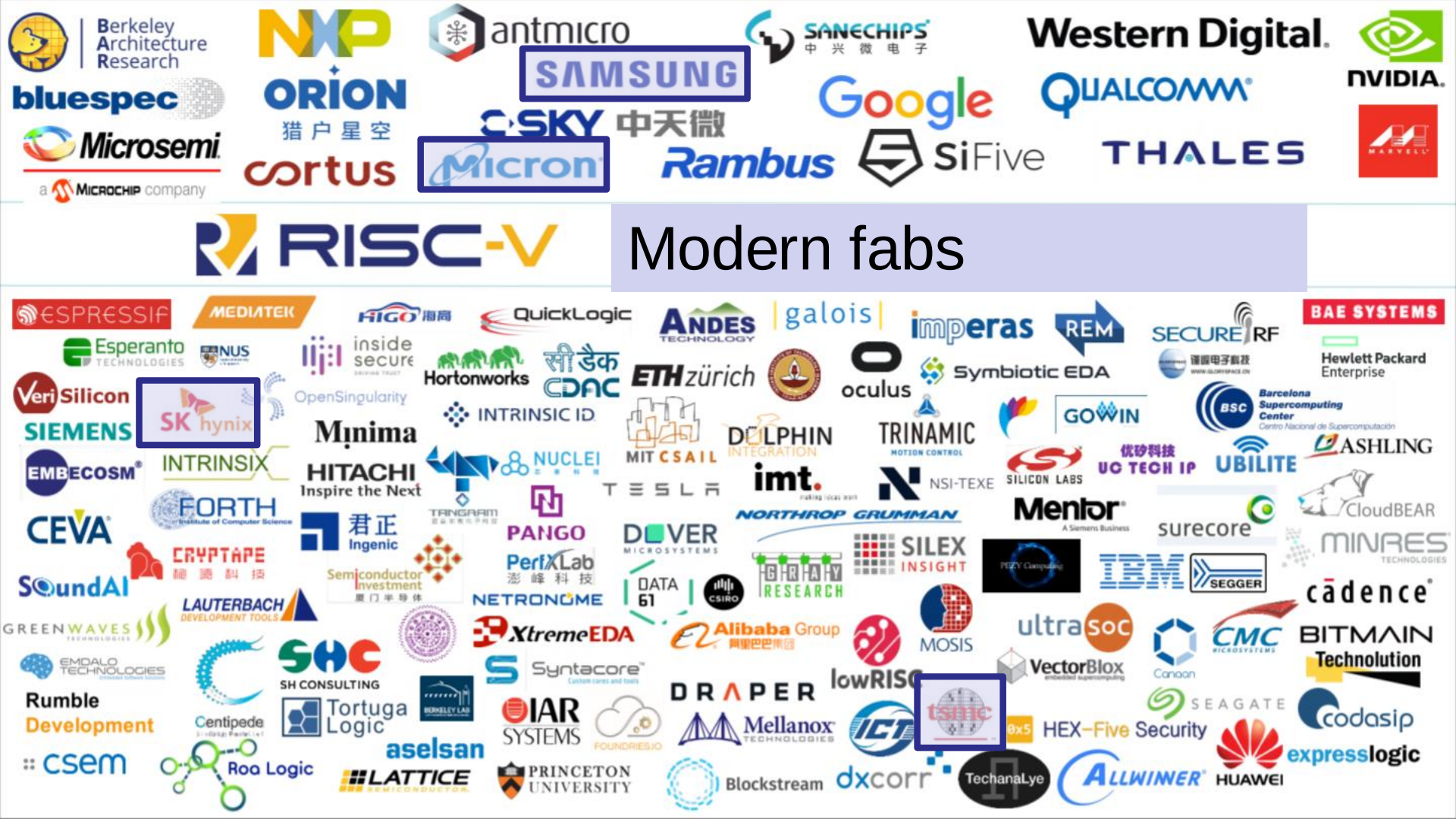

Berkeley Architecture Research
NXP
antmicro
SANECHIPS 中兴微电子
Western Digital
NVIDIA
SAMSUNG
bluespec
ORION 猎户星空
Google
QUALCOMM
C-SKY 中天微
Microsemi a MICROCHIP company
cortus
Micron
Rambus
SiFive
THALES
RISC-V
System OEMs
ESPRESSIF
MEDIATEK
HiGo 海思
QuickLogic
ANDES TECHNOLOGY
galois
imperas
REM
SECURE RF
BAE SYSTEMS
Esperanto TECHNOLOGIES
NUS
inside secure
Hortonworks
सी डैक CDAC
ETH zürich
oculus
Symbiotic EDA
Hewlett Packard Enterprise
VeriSilicon
OpenSingularity
INTRINSIC ID
GOWIN
BSC Barcelona Supercomputing Center
SIEMENS
SK hynix
Minima
DOLPHIN INTEGRATION
TRINAMIC MOTION CONTROL
ASHLING
EMBECOSM
INTRINSIX
HITACHI Inspire the Next
NUCLEI
MIT CSAIL
SILICON LABS
优矽科技 UC TECH IP
UBILITE
TESLA
imt.
NSI-TEXE
FORTH
TANGRAM
NORTHROP GRUMMAN
Mentor A Siemens Business
surecore
CloudBEAR
CEVA
PANGO
君正 Ingenic
DOVER MICROSYSTEMS
SILEX INSIGHT
MINRES TECHNOLOGIES
CRYPTAPE 楠菁科技
PerfXLab 芯峰科技
GRAY RESEARCH
IBM
SEGGER
SoundAI
Semiconductor Investment 厦门半导体
DATA 61
CSIRO
cadence
LAUTERBACH DEVELOPMENT TOOLS
NETRONOME
GREENWAVES TECHNOLOGIES
XtremeEDA
Alibaba Group 阿里巴巴集团
MOSIS
ultraSoC
CMC MICROSYSTEMS
BITMAIN Technolution
EMDALO TECHNOLOGIES
SHC SH CONSULTING
Syntacore
VectorBlox
Canaan
Rumble Development
Centipede
Tortuga Logic
BERKELEY LAB
DRAPER
lowRISC
SEAGATE
codasip
IAR SYSTEMS
FOUNDRIES.IO
Mellanox TECHNOLOGIES
ICT
tsmc
0x5
HEX-Five Security
aselsan
csem
Roa Logic
LATTICE SEMICONDUCTOR
PRINCETON UNIVERSITY
Blockstream
dxcorr
TechanaLye
ALLWINNER
HUAWEI
expresslogic


Berkeley Architecture Research
NXP
antmicro
SANECHIPS 中兴微电子
Western Digital.
NVIDIA.
bluespec
ORION 猎户星空
SAMSUNG
Google
QUALCOMM
Microsemi a MICROCHIP company
CSKY 中天微
cortus
Micron
Rambus
SiFive
THALES
RISC-V
EDA, IP and Support
ESPRESSIF
MEDIATEK
HiGO 海高
QuickLogic
ANDES TECHNOLOGY
galois
imperas
REM
SECURE RF
BAE SYSTEMS
Esperanto TECHNOLOGIES
NUS
inside secure
Hortonworks
सी डैक CDAC
ETH zürich
oculus
Symbiotic EDA
Hewlett Packard Enterprise
VeriSilicon
OpenSingularity
INTRINSIC ID
GOWIN
Barcelona Supercomputing Center
SIEMENS
SK hynix
Minima
MIT CSAIL
DOLPHIN INTEGRATION
TRINAMIC MOTION CONTROL
ASHLING
EMBECOSM
INTRINSIX
HITACHI Inspire the Next
NUCLEI
TESLA
imt.
NSI-TEXE
SILICON LABS
UC TECH IP
UBILITE
FORTH
TANGRAM
PANGO
Mentor
surecore
CloudBEAR
CEVA
君正 Ingenic
DOVER MICROSYSTEMS
NORTHROP GRUMMAN
MINRES
CRYPTAPE 楠菁科技
Semiconductor Investment 厦门半导体
PerfXLab 澎峰科技
SILEX INSIGHT
IBM
SEGGER
SoundAI
DATA 61
CSIRO
GRAY RESEARCH
cadence
LAUTERBACH DEVELOPMENT TOOLS
NETRONOME
ultraSoC
GREENWAVES TECHNOLOGIES
XtremeEDA
Alibaba Group 阿里巴巴集团
MOSIS
CMC MICROSYSTEMS
BITMAIN
Technolution
EMDALO TECHNOLOGIES
SHC SH CONSULTING
Syntacore
VectorBlox
Canaan
Rumble Development
lowRISC
DRAPER
Centipede
Tortuga Logic
IAR SYSTEMS
SEAGATE
codasip
Mellanox TECHNOLOGIES
ICT
tsmc
0x5 HEX-Five Security
csem
Roa Logic
aselsan
LATTICE SEMICONDUCTOR
PRINCETON UNIVERSITY
Blockstream
dxcorr
TechanaLye
ALLWINNER
HUAWEI
expresslogic


Berkeley Architecture Research
NXP
antmicro
SANECHIPS 中兴微电子
Western Digital
NVIDIA
bluespec
ORION 猎户星空
SAMSUNG
Google
QUALCOMM
Microsemi a MICROCHIP company
C-SKY 中天微
cortus
Micron
Rambus
SiFive
THALES
RISC-V
Debug, OS and Tools
ESPRESSIF
MEDIATEK
HiGo 海高
QuickLogic
ANDES TECHNOLOGY
galois
imperas
REM
SECURE RF
BAE SYSTEMS
Esperanto TECHNOLOGIES
NUS
inside secure
Hortonworks
सी डैक CDAC
ETH zürich
oculus
Symbiotic EDA
Hewlett Packard Enterprise
VeriSilicon
OpenSingularity
INTRINSIC ID
GOWIN
Barcelona Supercomputing Center
SIEMENS
SK hynix
Minima
MIT CSAIL
DOLPHIN INTEGRATION
TRINAMIC MOTION CONTROL
ASHLING
EMBECOSM
INTRINSIX
HITACHI Inspire the Next
NUCLEI
TESLA
imt.
NSI-TEXE
SILICON LABS
UC TECH IP
UBILITE
FORTH Institute of Computer Science
TANGRAM
PANGO
NORTHROP GRUMMAN
Mentor A Siemens Business
surecore
CloudBEAR
CEVA
君正 Ingenic
DOVER MICROSYSTEMS
SILEX INSIGHT
MINRES TECHNOLOGIES
CRYPTAPE 楠菱科技
Semiconductor Investment 厦门半导体
PerfXLab 澎峰科技
DATA 61
CSIRO
IBM
SEGGER
SoundAI
NETRONOME
cadence
LAUTERBACH DEVELOPMENT TOOLS
GREENWAVES TECHNOLOGIES
XtremeEDA
Alibaba Group
MOSIS
ultraSoc
CMC MICROSYSTEMS
BITMAN Technolution
EMDALO TECHNOLOGIES
SHC SH CONSULTING
Syntacore
VectorBlox
Canaan
Rumble Development
Tortuga Logic
lowRISC
DRAPER
SEAGATE
codasip
Centipede
IAR SYSTEMS
Mellanox TECHNOLOGIES
ICT
tsmc
0x5 HEX-Five Security
csem
Roa Logic
aselsan
PRINCETON UNIVERSITY
Blockstream
dxcorr
TechanaLye
ALLWINNER
HUAWEI
expresslogic
LATTICE SEMICONDUCTOR


Berkeley Architecture Research
NXP
antmicro
SANECHIPS 中兴微电子
Western Digital.
NVIDIA.
bluespec
ORION 猎户星空
SAMSUNG
Google
QUALCOMM
Microsemi
a MICROCHIP company
C-SKY 中天微
cortus
Micron
Rambus
SiFive
THALES
RISC-V
Datacenter
ESPRESSIF
MEDIATEK
HiGo 海高
QuickLogic
ANDES TECHNOLOGY
galois
imperas
REM
SECURE RF
BAE SYSTEMS
Esperanto TECHNOLOGIES
NUS
inside secure
Hortonworks
सी डैक CDAC
ETH zürich
oculus
Symbiotic EDA
Hewlett Packard Enterprise
VeriSilicon
OpenSingularity
INTRINSIC ID
GOWIN
Barcelona Supercomputing Center
SIEMENS
SK hynix
Minima
MIT CSAIL
DOLPHIN INTEGRATION
TRINAMIC MOTION CONTROL
ASHLING
EMBECOSM
INTRINSIX
HITACHI Inspire the Next
NUCLEI
TESLA
imt.
NSI-TEXE
SILICON LABS
优矽科技 UC TECH IP
UBILITE
FORTH
TANGRAM
PANGO
NORTHROP GRUMMAN
Mentor A Siemens Business
surecore
CloudBEAR
CEVA
君正 Ingenic
DOVER MICROSYSTEMS
SILEX INSIGHT
MINRES TECHNOLOGIES
CRYPTAPE
PerfXLab 澎峰科技
GRAY RESEARCH
PEZY Computing
IBM
SEGGER
SoundAI
Semiconductor Investment 厦门半导体
DATA 61
CSIRO
NETRONOME
cadence
LAUTERBACH DEVELOPMENT TOOLS
GREENWAVES TECHNOLOGIES
XtremeEDA
Alibaba Group 阿里巴巴集团
MOSIS
ultraSoC
CMC MICROSYSTEMS
BITMAIN Technolution
EMDALO TECHNOLOGIES
SHC SH CONSULTING
Syntacore
lowRISC
VectorBlox
Canaan
Rumble Development
Tortuga Logic
DRAPER
SEAGATE
codasip
Centipede
IAR SYSTEMS
FOUNDRIES.IO
Mellanox TECHNOLOGIES
ICT
tsmc
0x5
HEX-Five Security
csem
Roa Logic
aselsan
LATTICE SEMICONDUCTOR
PRINCETON UNIVERSITY
Blockstream
dxcorr
TechanaLye
ALLWINNER
HUAWEI
expresslogic

Modern fabs


Berkeley Architecture Research
NXP
antmicro
SANECHIPS 中兴微电子
Western Digital
NVIDIA
bluespec
ORION 猎户星空
SAMSUNG
Google
QUALCOMM
Microsemi a MICROCHIP company
cortus
C-SKY 中天微
Micron
Rambus
SiFive
THALES
RISC-V
ESPRESSIF
MEDIATEK
HiGo 海高
QuickLogic
ANDES TECHNOLOGY
galois
imperas
REM
SECURE RF
BAE SYSTEMS
Esperanto TECHNOLOGIES
NUS
inside secure
Hortonworks
सी डैक CDAC
ETH zürich
oculus
Symbiotic EDA
Hewlett Packard Enterprise
VeriSilicon
SIEMENS
SK hynix
OpenSingularity
Minima
INTRINSIC ID
MIT CSAIL
DOLPHIN INTEGRATION
TRINAMIC MOTION CONTROL
GOWIN
Barcelona Supercomputing Center
ASHLING
EMBECOSM
INTRINSIX
HITACHI Inspire the Next
NUCLEI
TESLA
imt.
NSI-TEXE
SILICON LABS
优矽科技 UC TECH IP
UBILITE
FORTH
TANGRAM
PANGO
NORTHROP GRUMMAN
Mentor A Siemens Business
surecore
CloudBEAR
CEVA
君正 Ingenic
DOVER MICROSYSTEMS
SILEX INSIGHT
MINRES TECHNOLOGIES
CRYPTAPE 楠菱科技
Semiconductor Investment 厦门半导体
PerfXLab 澎峰科技
GRAY RESEARCH
IBM
SEGGER
SoundAI
DATA 61
CSIRO
cadence
LAUTERBACH DEVELOPMENT TOOLS
NETRONOME
GREENWAVES TECHNOLOGIES
XtremeEDA
Alibaba Group 阿里巴巴集团
MOSIS
ultraSoC
CMC MICROSYSTEMS
BITMAIN Technolution
EMDALO TECHNOLOGIES
SHC SH CONSULTING
Syntacore
lowRISC
VectorBlox
Canaan
Rumble Development
Centipede
Tortuga Logic
DRAPER
SEAGATE
codasip
IAR SYSTEMS
FOUNDRIES.IO
Mellanox TECHNOLOGIES
ICT
tsmc
0x5
HEX-Five Security
csem
Roa Logic
aselsan
LATTICE SEMICONDUCTOR
PRINCETON UNIVERSITY
Blockstream
dxcorr
TechanaLye
ALLWINNER
HUAWEI
expresslogic


Berkeley Architecture Research
NXP
antmicro
SANECHIPS 中兴微电子
Western Digital
NVIDIA
bluespec
ORION 猎户星空
SAMSUNG
Google
QUALCOMM
Microsemi
a MICROCHIP company
C-SKY 中天微
Micron
Rambus
SiFive
THALES
cortus
RISC-V
Emerging Applications
ESPRESSIF
MEDIATEK
HiGo 海高
QuickLogic
ANDES TECHNOLOGY
galois
imperas
REM
SECURE RF
BAE SYSTEMS
Esperanto TECHNOLOGIES
NUS
inside secure
Hortonworks
सी डैक CDAC
ETH zürich
oculus
Symbiotic EDA
Hewlett Packard Enterprise
VeriSilicon
OpenSingularity
INTRINSIC ID
GOWIN
Barcelona Supercomputing Center
SIEMENS
SK hynix
Minima
MIT CSAIL
DOLPHIN
TRINAMIC MOTION CONTROL
ASHLING
EMBECOSM
INTRINSIX
HITACHI Inspire the Next
NUCLEI
TESLA
imt.
NSI-TEXE
SILICON LABS
UC TECH IP
UBILITE
FORTH Institute of Computer Science
TANGRAM
NORTHROP GRUMMAN
Mentor A Siemens Business
surecore
CloudBEAR
CEVA
君正 Ingenic
PANGO
DOVER MICROSYSTEMS
CRYPTAPE
Semiconductor Investment
PerfXLab 澎峰科技
SILEX INSIGHT
IBM
SEGGER
MINRES TECHNOLOGIES
SoundAI
DATA 61
CSIRO
GRAY RESEARCH
cadence
LAUTERBACH DEVELOPMENT TOOLS
NETRONOME
GREENWAVES TECHNOLOGIES
XtremeEDA
Alibaba Group
MOSIS
ultraSoC
CMC MICROSYSTEMS
BITMAIN
EMDALO TECHNOLOGIES
SHC
SH CONSULTING
Syntacore
VectorBlox
Canaan
Technolution
Rumble Development
Centipede
Tortuga Logic
DRAPER
lowRISC
SEAGATE
codasip
IAR SYSTEMS
Mellanox TECHNOLOGIES
ICT
tsmc
0x5
HEX-Five Security
csem
Roa Logic
aselsan
LATTICE SEMICONDUCTOR
PRINCETON UNIVERSITY
Blockstream
dxcorr
TechanaLye
ALLWINNER
HUAWEI
expresslogic

The New Golden Age of Computer Architecture

2017 Turing Award Lecture

A New Golden Age for Computer Architecture:

Domain-Specific Hardware/Software Co-Design, Enhanced Security, Open Instruction Sets, and Agile Chip Development

John Hennessy and David Patterson
Stanford and UC Berkeley

June 4, 2018

https://www.youtube.com/watch?v=3LVeEjsn8Ts

1

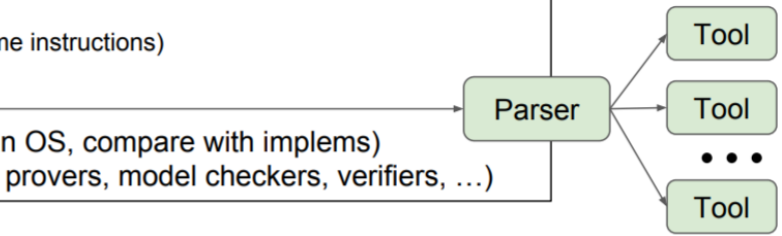
Building a secure world from the ground up

Activity of Note: Formal Spec

What is an ISA Formal Spec?

A specification of the semantics of each instruction in the ISA, and of code execution:

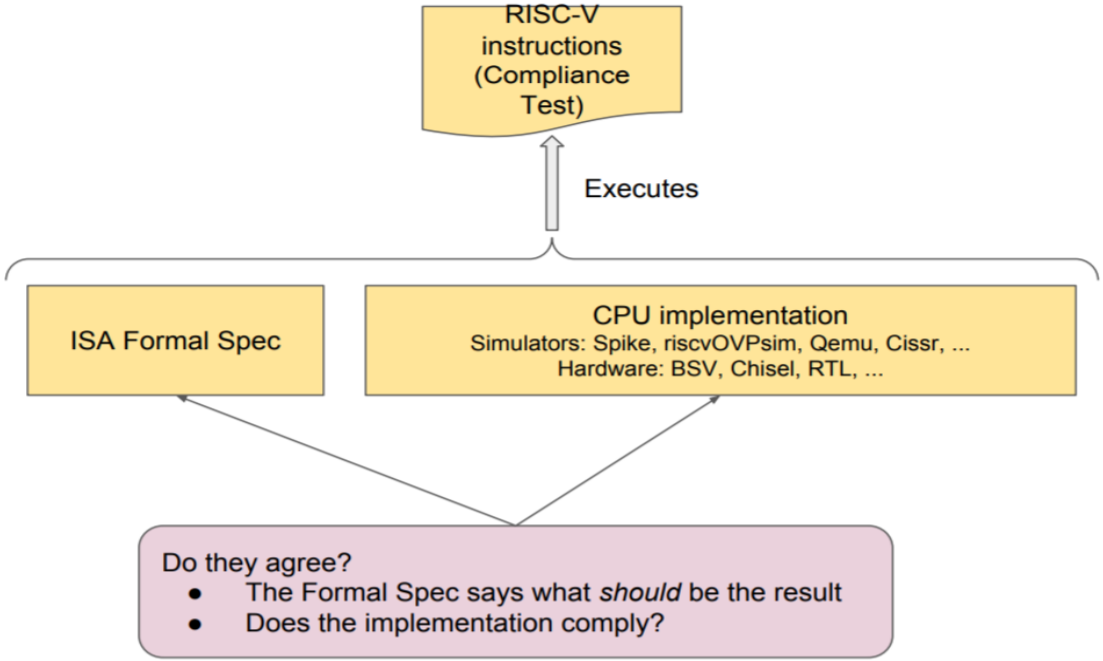
- Simple, clear and understandable to the human reader
  - Not cluttered with implementation considerations; no micro-architectural detail
  - Accessible to the practicing engineer: implementers of hardware, simulators, compilers, OSs, libraries of concurrent data structures, ...
- Precise and complete
  - (including allowed non-determinism of some instructions)
- Machine readable
- Executable (run RISC-V programs, boot an OS, compare with implems)
- Usable with various formal tools (theorem provers, model checkers, verifiers, …)



English-language text specs, and instruction-set simulators (like Spike, riscvOVPSim, Qemu, Cissr, etc.) can be regarded as specs, but they typically do not meet many of these goals.

Activity of Note: Formal Spec

Of What Use is an ISA Formal Spec? Major use case: Compliance Testing



Activity of Note: Formal Spec

There are six efforts within TG Formal ISA, all quite advanced

(in free and open source repositories)

- **riscv-semantics**: Adam Chlipala group at MIT
  - In Haskell, connecting to Coq formal tools in particular.

  https://github.com/mit-plv/riscv-semantics
- **SAIL-RISCV**: Prashanth Mundkur and Peter Sewell group at U. Cambridge and SRI International
  - In SAIL DSL (domain specific language), which has also been used to model production ARMv8 (and others)
  - Has most experience in addressing concurrency.

  https://github.com/rems-project/sail-riscv
- **riscv-formal:** Clifford Wolf
  - In Verilog

  https://github.com/cliffordwolf/riscv-formal
- **GRIFT**: ("Galois RISC-V ISA Formal Tools") Ben Selfridge group at Galois
  - In Haskell

  https://github.com/GaloisInc/grift
- **Kami**: Murali Vijayaraghavan group at SiFive
  - In "Kami", a DSL in Coq for HW description.

  (hoping to publish soon)
- **Forvis**: ("Formal RISC-V ISA spec") Rishiyur Nikhil et. al. at Bluespec
  - In "Extremely Elementary" Haskell for extreme readability.

  https://github.com/rsnikhil/Forvis_RISCV-ISA-Spec[10]

RISC-V Members Through a Security Filter

Defense Companies

BAE SYSTEMS

THALES

NORTHROP GRUMMAN

aselsan

Chip Companies

NXP

wRISC

NVIDIA

HIP

Micron

Application Denied

Security IP

inside secure

INTRINSIC ID

Rambus
Cryptography Research

SECURE RF
Securing the Internet of Things®

DOVER MICROSYSTEMS

s and Tools

Tortuga Logic

DATA 61

CSIRO

Blockstream

bluespec

galois

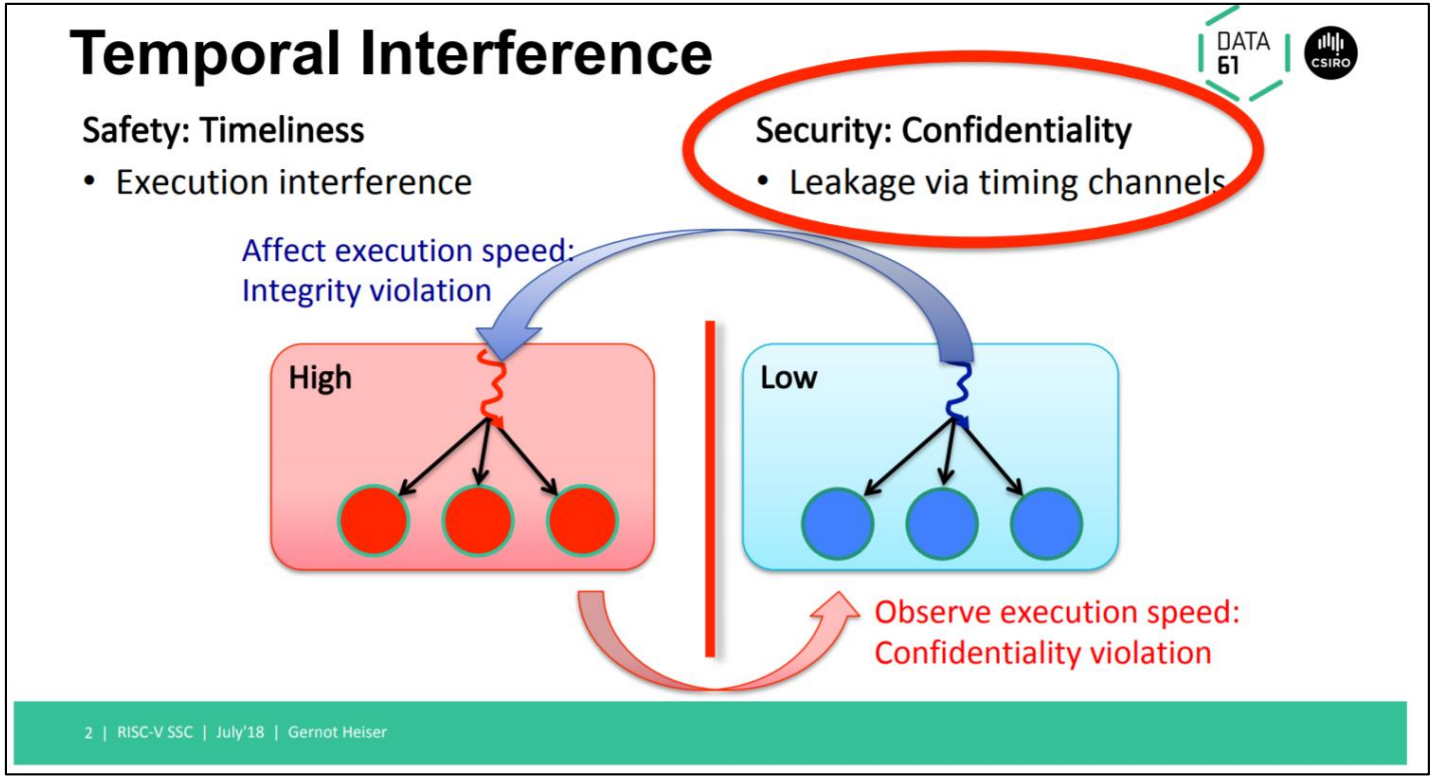
INTRINSIX

Activity of Note: Security Standing Committee

Security Steering Committee Main Goals

- Promote RISC-V as an ideal vehicle for the security community
- Liaise with other internal RISC-V committees and with external security committees
- Create an information repository on new attack trends, threats and countermeasures
- Identify top 10 open challenges in security for the RISC-V community to address
- Propose security committees (Marketing or Technical) to tackle specific security topics
- Recruit security talent to the RISC-V ecosystem (e.g., into committees)
- Develop consensus around best security practices for IoT devices and embedded systems

Speaker Program: Gernot Heiser, Data61



Timing Channels

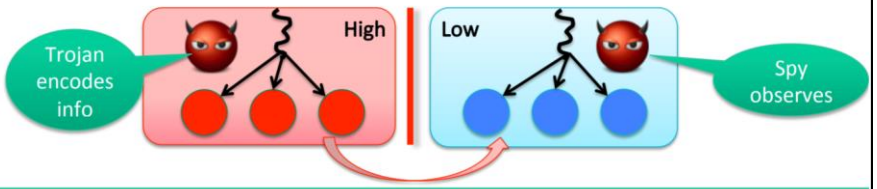
Covert Channel

Definition:

- Information flow that bypasses the system's security policy

Note:

- CC exploits mechanisms not intended for information transmission



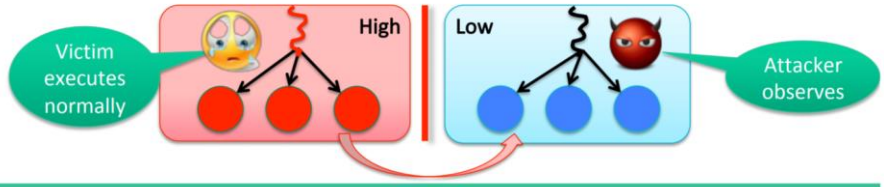
Side Channel

Definition:

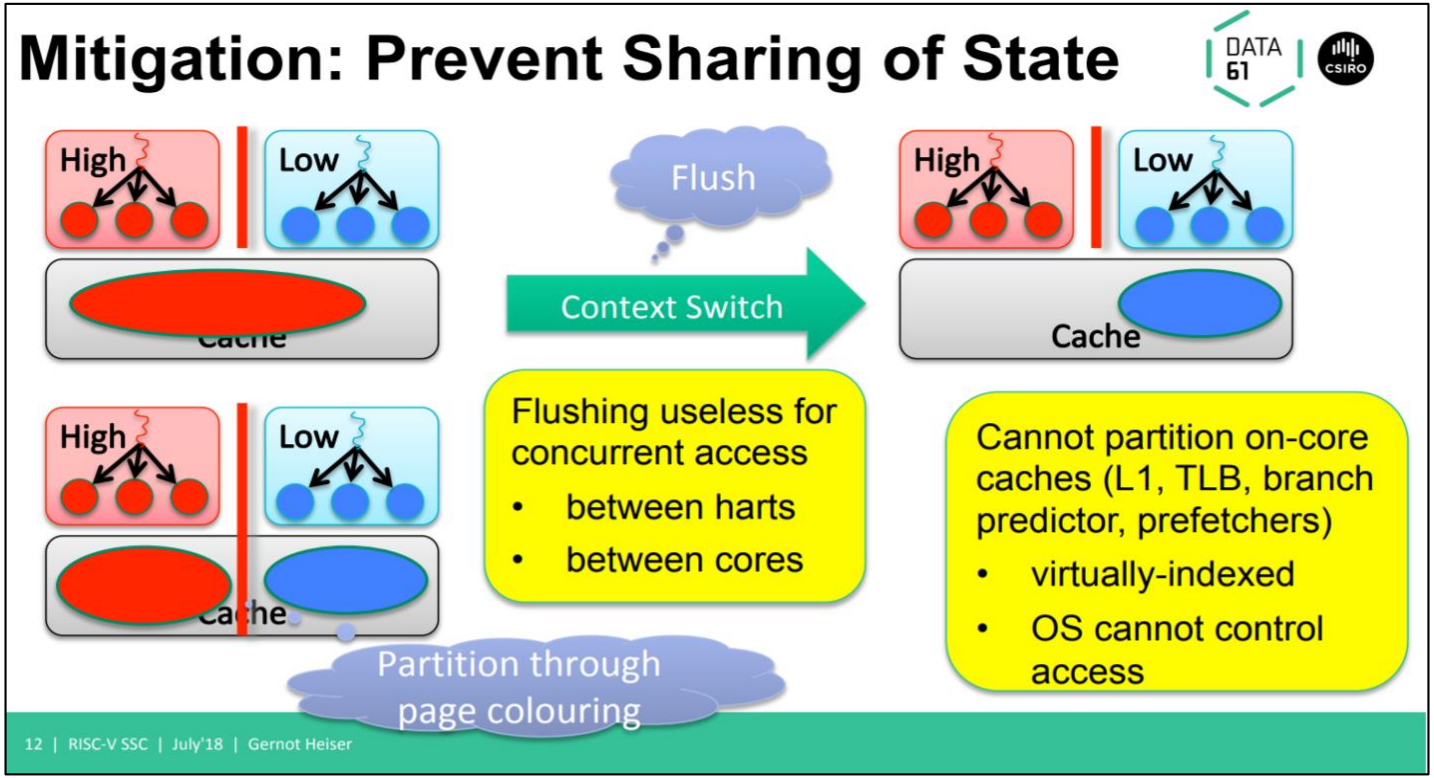
- Covert channel that can be exploited without insider help

Note:

- Attacker probes for traces left by the execution of an innocent victim



Mitigating Timing Attacks



New Hardware-Software Contract!

Need New Hardware-Software Contract!

- The ISA is a purely functional contract
  - sufficient to ensure functional correctness
  - abstracts away time
  - insufficient for ensuring either timing safety or security
- For security need an abstraction of microarchitectural state
  - essential for letting OS provide time protection

Remember: Timing channels can be closed *iff* all shared hardware state can be partitioned or flushed

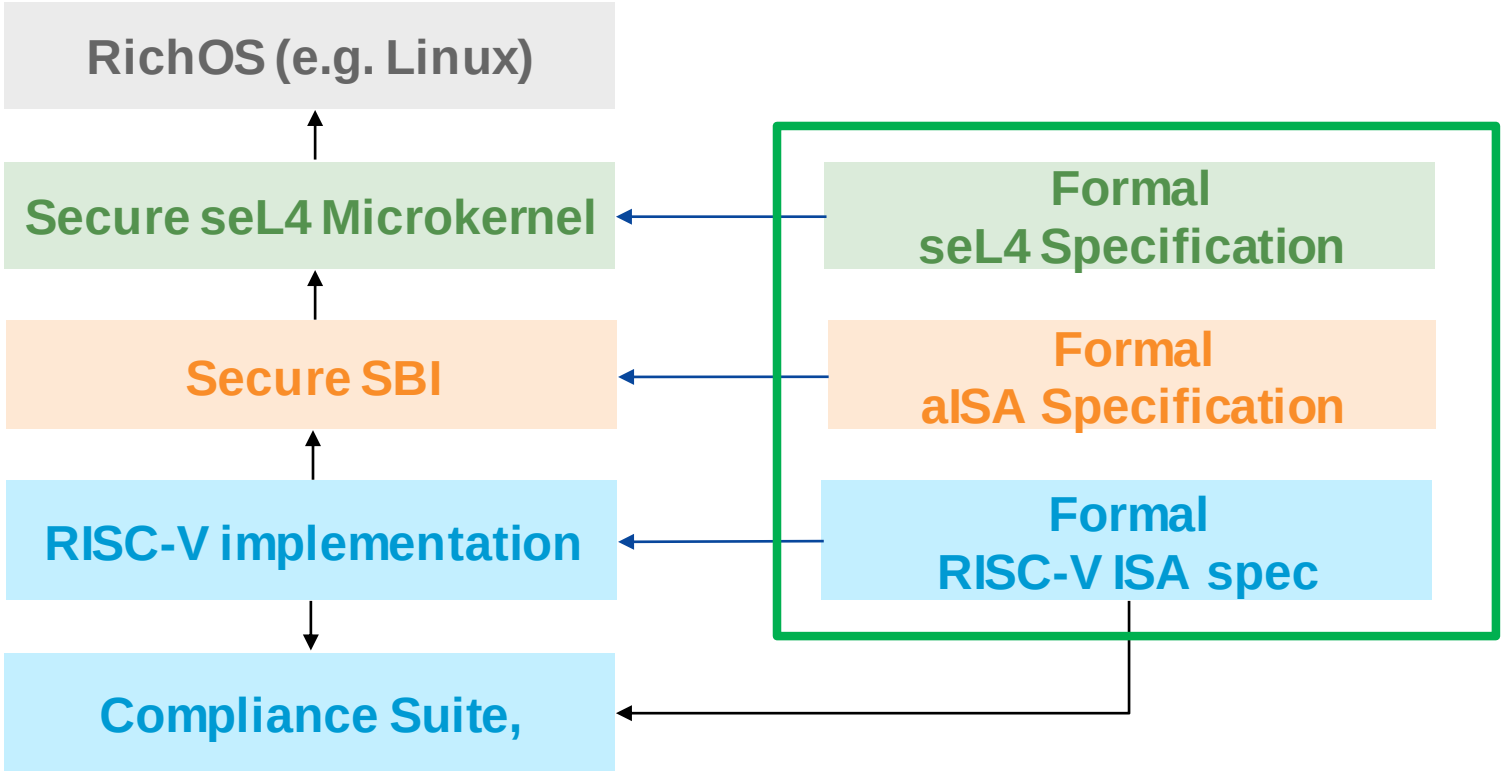
Augmented ISA

New Hardware-Software Contract: AISA

Augmented ISA must provide abstractions that support time protection:

1. Identify partitionable state and how to partition
   - Generally physically-addressed caches, memory interfaces
   - Mostly there, just make it part of the contract
2. Identify existence of non-partitionable state and how it can be flushed
   - Can probably lump all on-core state into single abstraction
   - A single flush-on-core-state operation may be sufficient

Putting it all Together: The RISC-V Security Stack

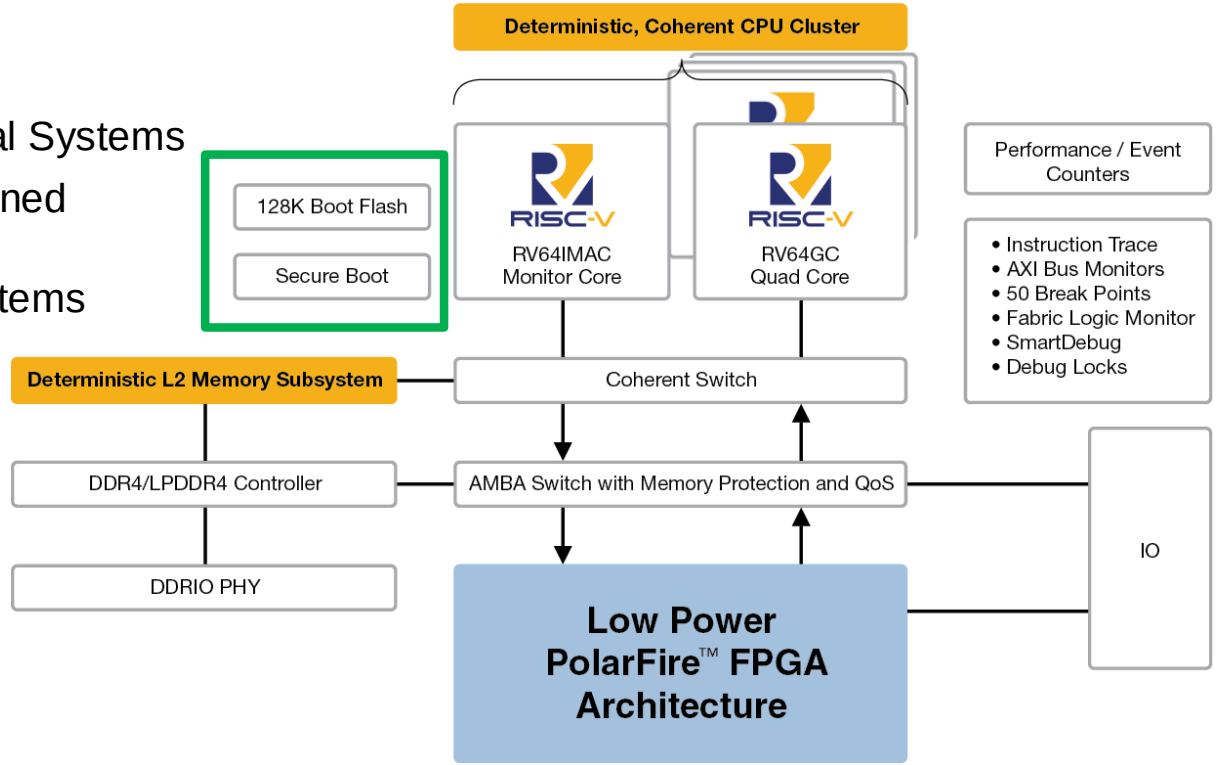


Start creating a secure future today with Microchip and RISC-V

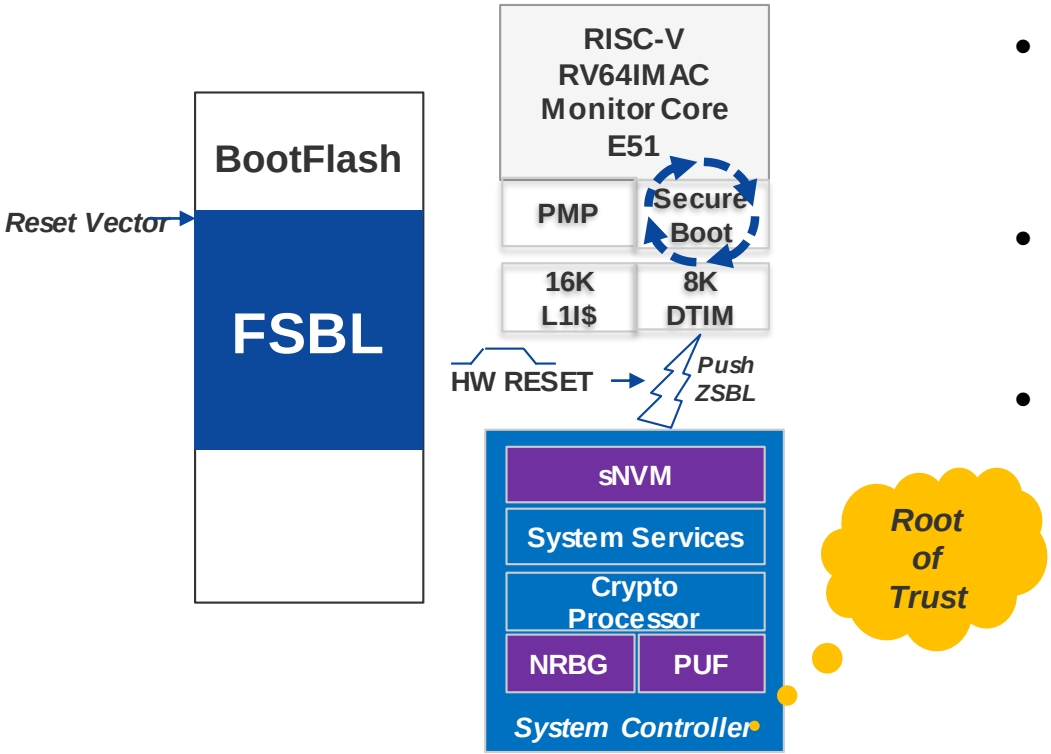
PolarFire SoC RISC-V-based SoC FPGA

Freedom to Innovate in

- Linux and Real-Time
- High-Reliability Safety Critical Systems
- Thermal and Power Constrained Systems
- Securely Connected IoT Systems

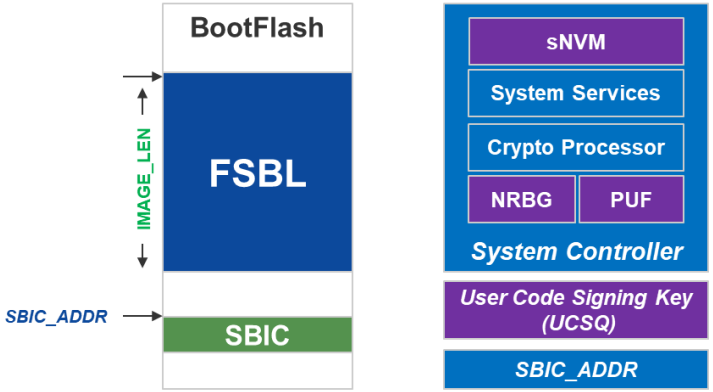


Secure Boot



- **Guards against sophisticated methods of attack whereby a malicious external agent tampers with the boot image stored in bootflash (e.g Linux FSBL)**
- **Authenticates the image in bootflash before transferring execution control to the OS boot loader pointed to by reset vector**
- **FPGA system controller (root of trust) manages the authentication process and certifies boot image using crypto functionality built into the FPGA backbone**
  - Push “zero state boot loader” (ZSBL) upon detecting HW reset.
  - Release monitor core from reset and executes authentication on FSBL image pointed to by reset vector.
  - If authentication is successful, transfer execution control back to FSBL, otherwise abort.

Authentication Framework



Value	Description
IMAGE_ADDR	Address of FSBL in SOC Memory map
IMAGE_LEN	Size of FSBL in Bytes
$BOOT\_VEC_0$	Boot Vector in FSBL Monitor Core
$BOOT\_VEC_{1-4}$	Boot Vectors for User Cores
H	FSBL Image Hash (SHA512-256)
CODESIG	SBIC Digital Signature (ECDSA)

- **ZSBL bootloader authenticates FSBL image in bootflash which contains:**
  - Actual FSBL image
  - SBIC data structure generated during bootflash programming and stored @ SBIC_ADDR
- **Authenticity of SBIC is verified by FPGA system controller using ECDSA:**
  - UCSQ is a public key programmed on the device by the user
  - Corresponds to UCSK private key used to sign the SBIC during programming

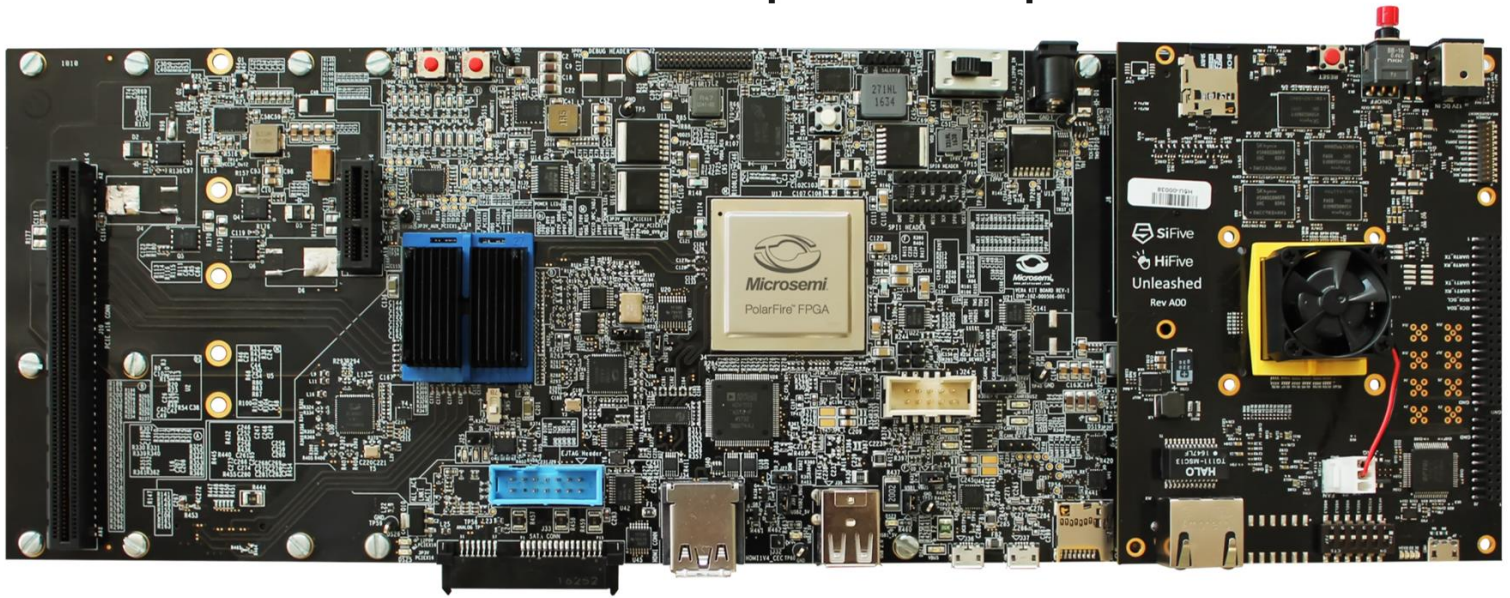
$$CODESIG = ECDSA_{SIGN}\ (UCSK,\ IMAGE\_ADDR \mid IMAGE\_LEN \mid BOOTVEC_{0\text{-}4} \mid H)$$

$$ECDSA_{VERIFY}\ (UCSQ,\ IMAGE\_ADDR \mid IMAGE\_LEN \mid BOOTVEC_{0\text{-}4} \mid H,\ CODESIG)$$

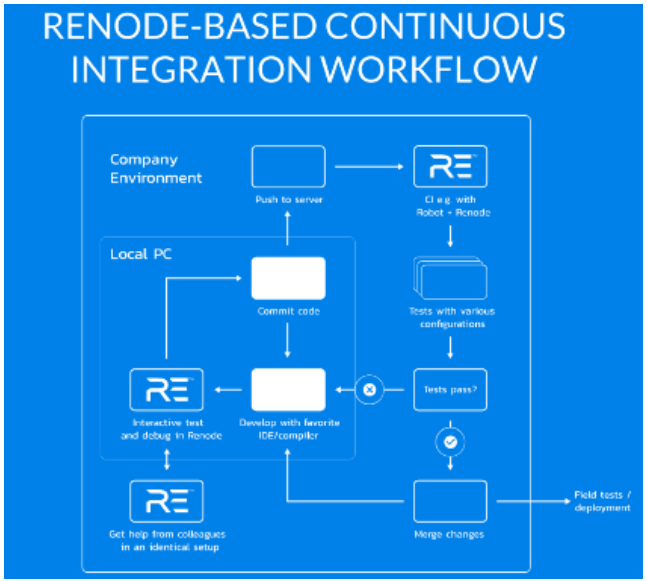
Elliptic Curve Digital Signature Algorithm (ECDSA)

Freedom to Begin Hardware Development

PolarFire SoC Embedded Experts Development Platform



Freedom to Start Software Development



RENODE™

- Free Rapid Software Development and Debug Capabilities without Hardware
- Complete PolarFire SoC Processor
- Subsystem Model

antmicro

Building Out the Mi-V RISC-V Ecosystem

MICROCHIP

SiFive

SoftConsole

RISC-V

0x5 HEX-Five

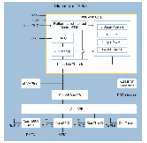
Zephyr

antmicro

Libero System-on-Chip

Mi-V

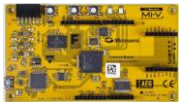
DIGITAL CORE TECHNOLOGIES QUALITY BY DESIGN



EmCraft systems

APACHE mynewt

aries embedded Intelligence for Industry



BuildRoot Making Embedded Linux Easy

expresslogic

freeRTOS

PHYTEC

Micrium Embedded Software

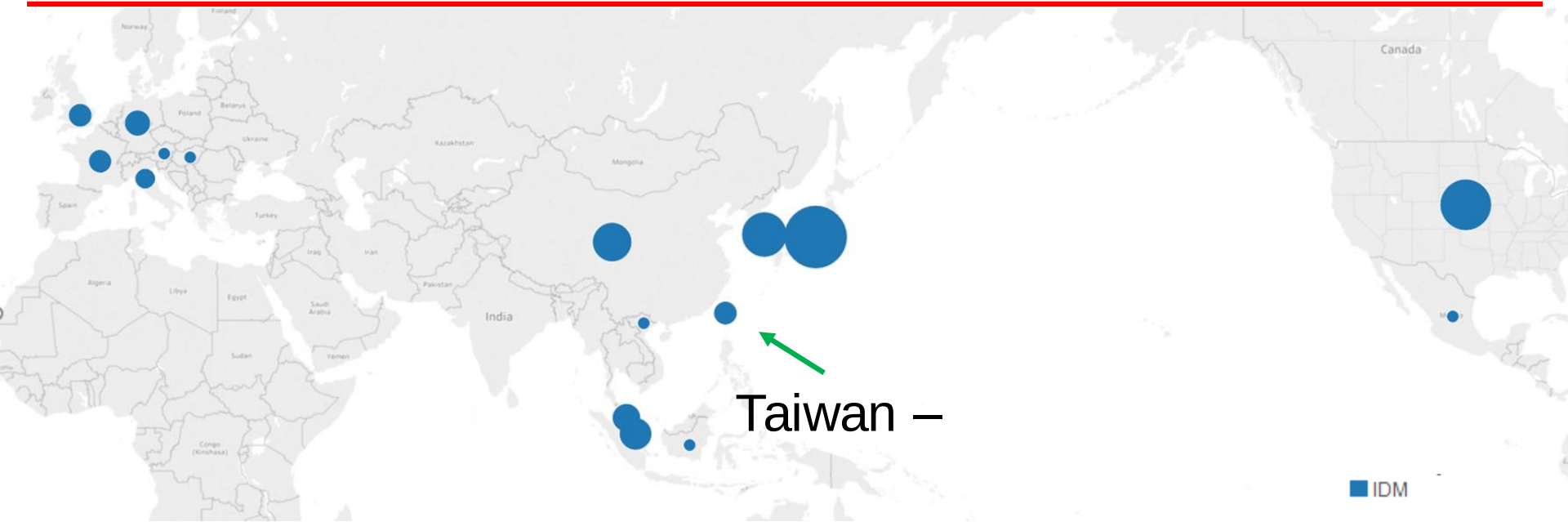
ultraSoC

µC/OS The Real-Time Operating System

imperas

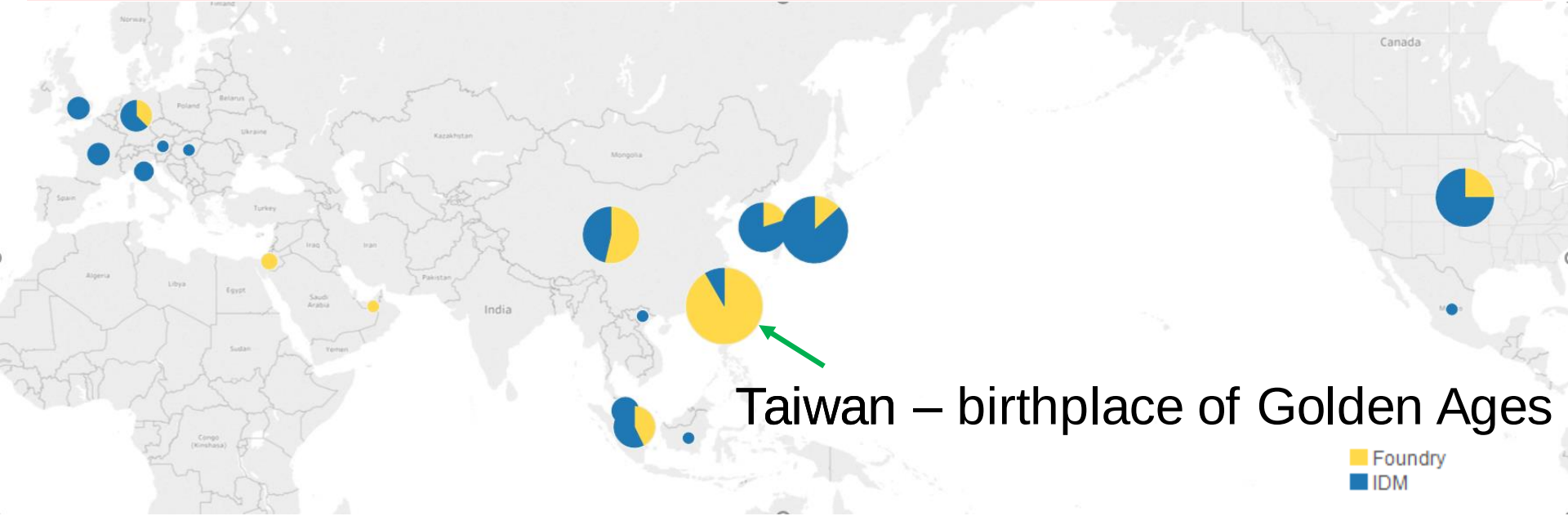
DORNERWORKS

Where IDMs have Fabs



https://en.wikipedia.org/wiki/List_of_semiconductor_fabrication_plants

Where foundries have their fabs



https://en.wikipedia.org/wiki/List_of_semiconductor_fabrication_plants

Thank You