

seL4[®]

What, Why, Who and Where?

June Andronick



Photo by Alessandro Erbetta on Unsplash



Photo by Alessandro Erbetta on Unsplash



Photo by Ante Hamersmit on Unsplash



Photo by Gregory DALLEAU on Unsplash



“Ask Me Anything”

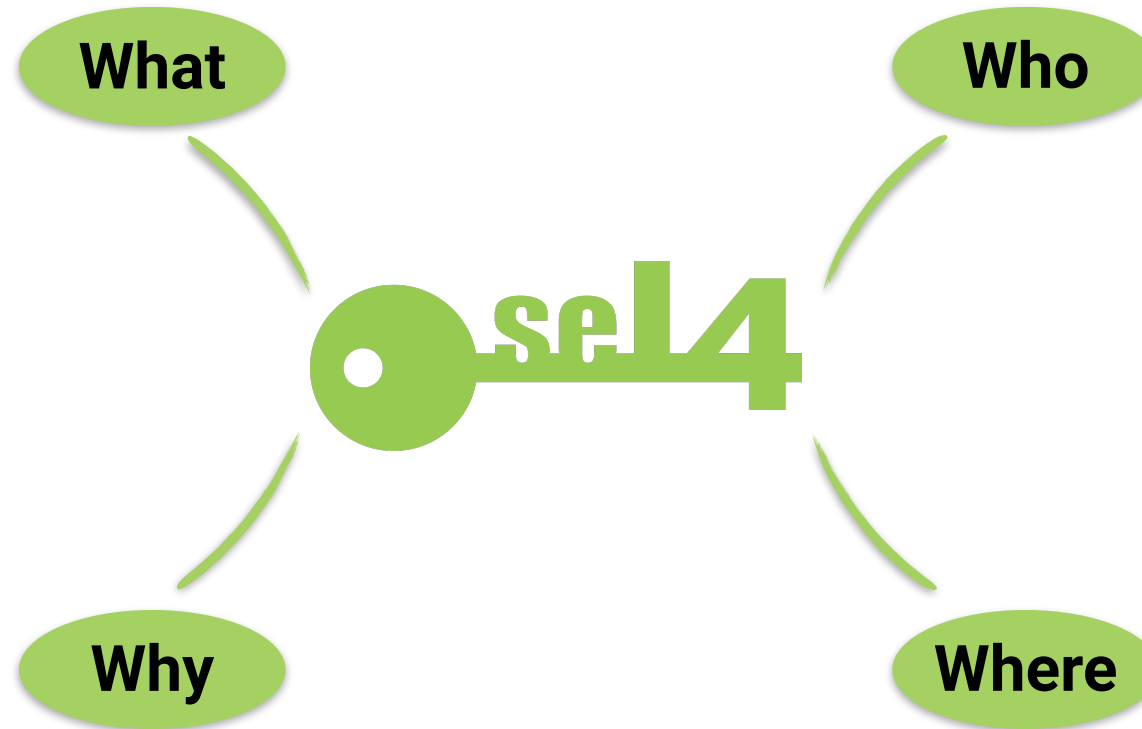
**AMA session
with seL4 experts**

on Day 3



**Safe, Secure, Reliable
Software Products**





What



seL4 is an open source, high-assurance, high-performance operating system microkernel

Available on GitHub
under GPLv2 license

Most comprehensive
mathematical proofs of
correctness and security

Fastest
microkernel

Piece of software that
runs at the heart of any
system and controls all
accesses to resources



seL4 Foundation

Become a Member

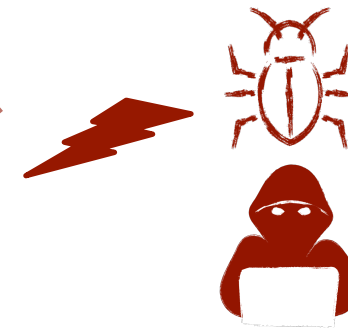
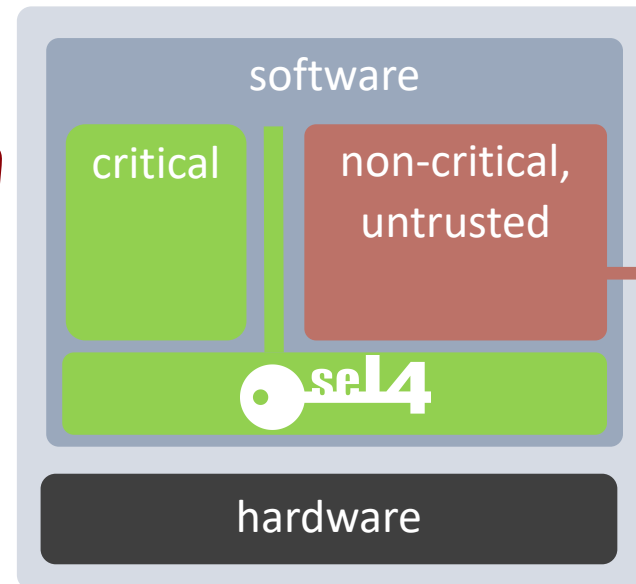


**10% off your
1st year!**



Licence

<https://sel4.systems/Legal/>



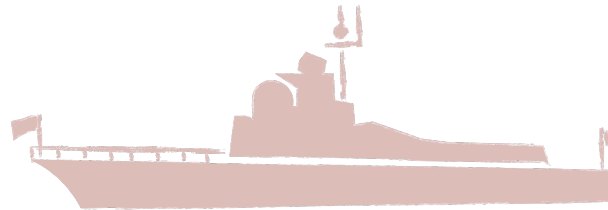
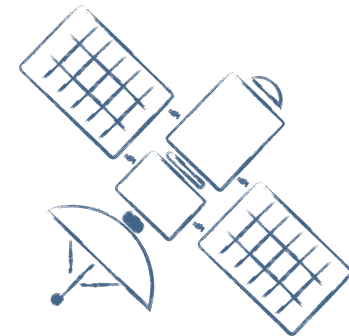
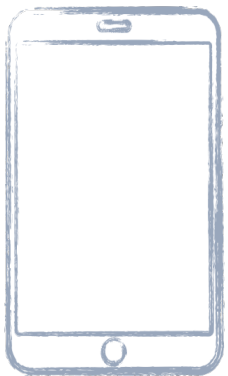
What



seL4 is an open source, high-assurance, high-performance operating system microkernel



seL4 is the most trustworthy foundation for safety- and security-critical systems



What



History

- ▶ 70's and 80's : First microkernel: minimality but bad performance
- ▶ 90's: L4 kernel: Microkernels can have high performance
- ▶ 2004: Start of the L4.verified project (in the group that is now called Trustworthy Systems or TS)
- ▶ **29th July 2009:** 0 sorries: first formally verified kernel (correctness)
- ▶ 2012-2013: Further proofs: Security, Binary Correctness, and more
- ▶ 2012-2017: DARPA HACMS: seL4 protects unmanned helicopter against cyber-attacks
- ▶ **29th July 2014:** Freedom day: seL4 becomes Open Source
- ▶ 7th April 2020: Launch of the seL4 Foundation (founding members incl. Dornerworks & UNSW)
- ▶ 2021: seL4 becomes an Ecosystem (TS at UNSW; Proofcraft; Kry10 and more)

What



**Safe, Secure, Reliable
Software Products**



What



**Safe, Secure, Reliable
Software Products**

Components/OS



What

Tools, Frameworks & Languages

<https://sel4.systems/tools.html>

Development Kits & Component Frameworks

Microkit

CAMkES

sDDF

seL4 Dev Kit

BriefCase

Operating Systems

LionsOS

KOS

ScultOS

Virtualisation

CAMkES
VMM
Library

Microkit
VMM
Library

VM
Composer

Language support



C/C++



Rust



Pancake



MicroPython



Erlang/Elixir

What

Tools, Frameworks & Languages

<https://sel4.systems/tools.html>

Development Kits & Component Frameworks

Microkit

CAMkES

sDDF

seL4 Dev Kit

BriefCase

Operating Systems

LionsOS

KOS

ScultOS

Virtualisation

CAMkES
VMM
Library

Microkit
VMM
Library

VM
Composer

Language support

C

C/C++

R

Rust

P

Pancake

Python

MicroPython

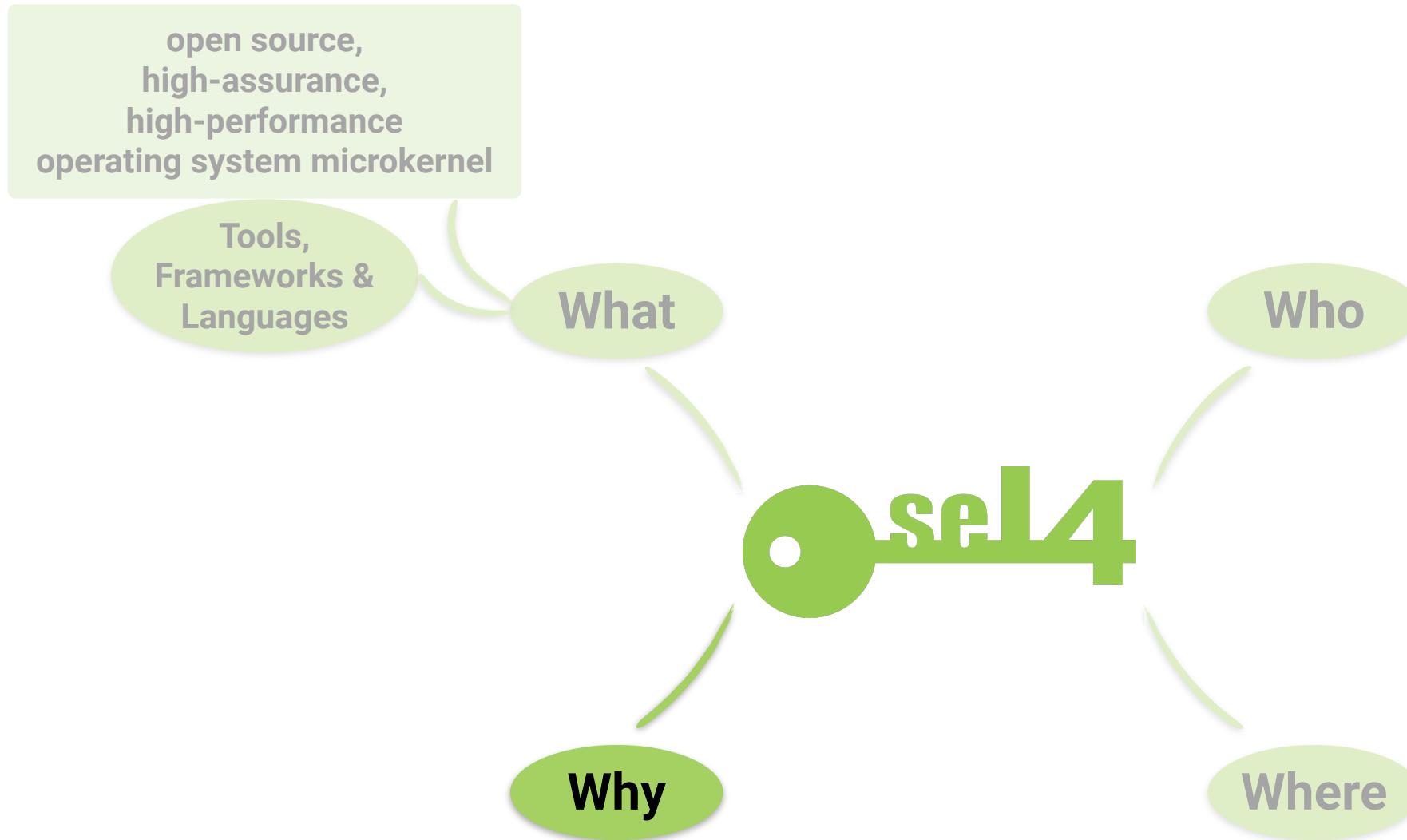
E

Erland/Elixir

Commercial

Open Source

Provided by the seL4 Foundation



Why



Verification

seL4 is the only kernel with inspectable proofs of deep properties down to the implementation



Features

- ✓ General purpose
- ✓ Cyber-retrofit
- ✓ Capability-based
- ✓ Lightweight



Awards

seL4, an award-winning technology

- ✓ 2023: DARPA Game Changer Award for HACMS
- ✓ 2022: ACM Software System Award
- ✓ 2019: ACM SIGOPS Hall of Fame Award
- ✓ 2011: MIT Technology Review's TR10 Award
- ✓ 2009: SOSP Best Paper Award



Performance

seL4 is 2 to 10 times faster than other comparable systems

Why



Verification

seL4 is the only kernel with inspectable proofs of deep properties down to the implementation

Facts

- ✓ 0 violations of verified properties since proof completed in 2009
- ✓ Continually maintained and updated; No code change without proof validation
- ✓ Beyond top certification requirements (CC EAL7, ISO26262 ASIL-D, DO-178C A)



Why



Verification

seL4 is the only kernel with inspectable proofs of deep properties down to the implementation

Implications

- ✓ No buffer overflows
- ✓ No null pointer dereferences
- ✓ No pointer errors
- ✓ No memory leaks
- ✓ No arithmetic overflows or exceptions
- ✓ No undefined behaviour

Assumptions

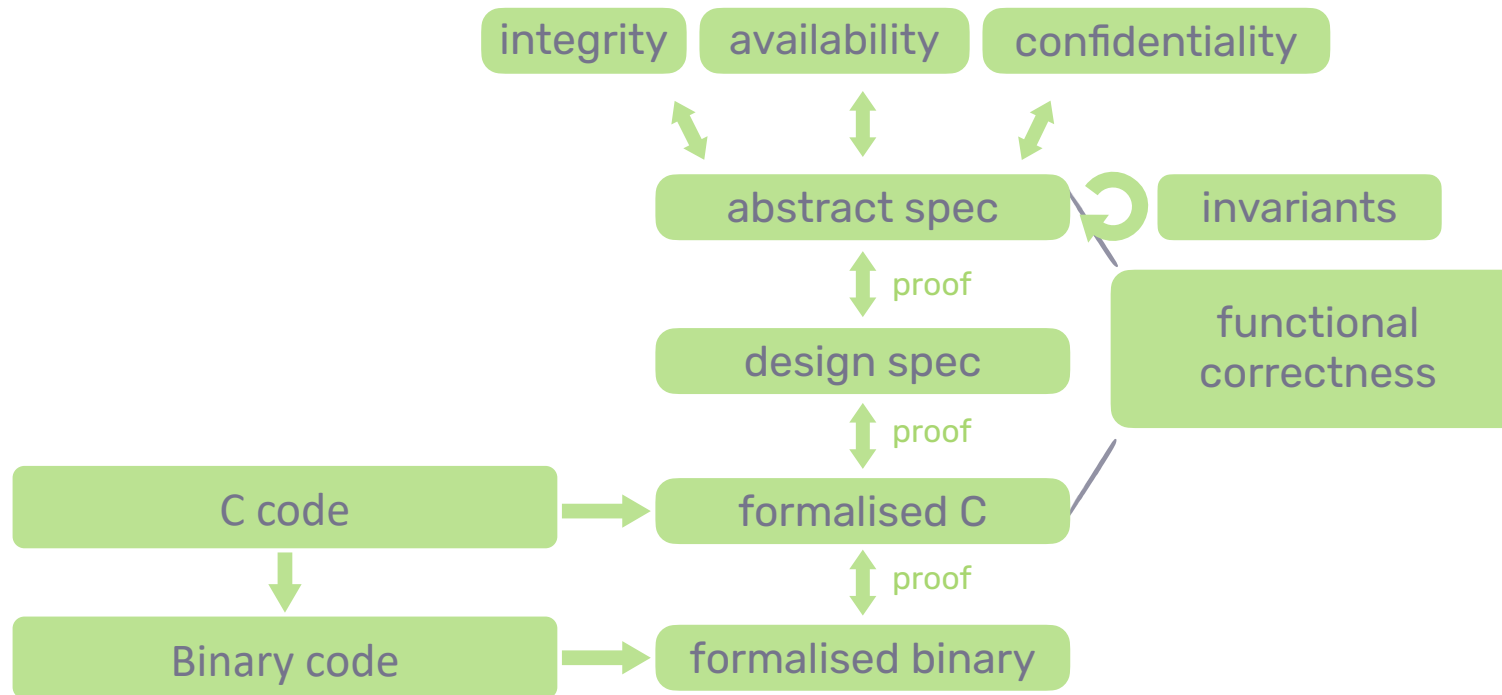
- ✓ Assembly
- ✓ Hardware
- ✓ Hardware management
- ✓ Boot code
- ✓ Virtual memory
- ✓ DMA
- ✓ Information side-channels

Why



Verification

seL4 is the only kernel with inspectable proofs of deep properties down to the implementation



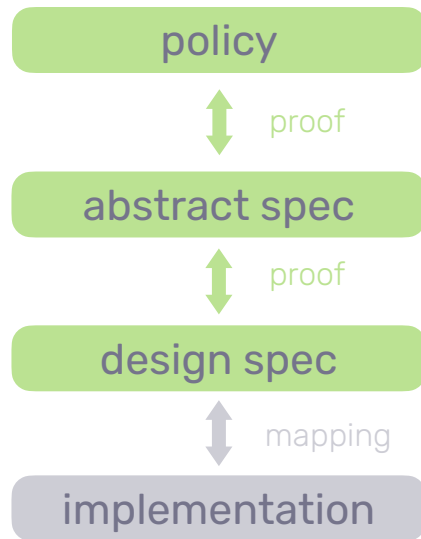
Why



Verification

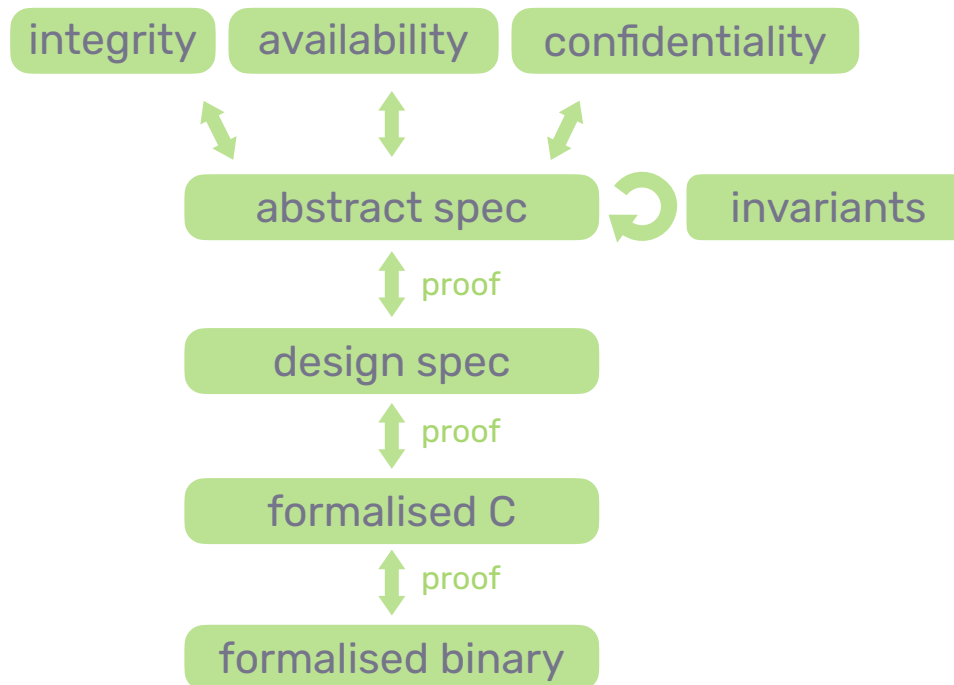
seL4 is the only kernel with inspectable proofs of deep properties down to the implementation

Common Criteria
EAL7 Certification

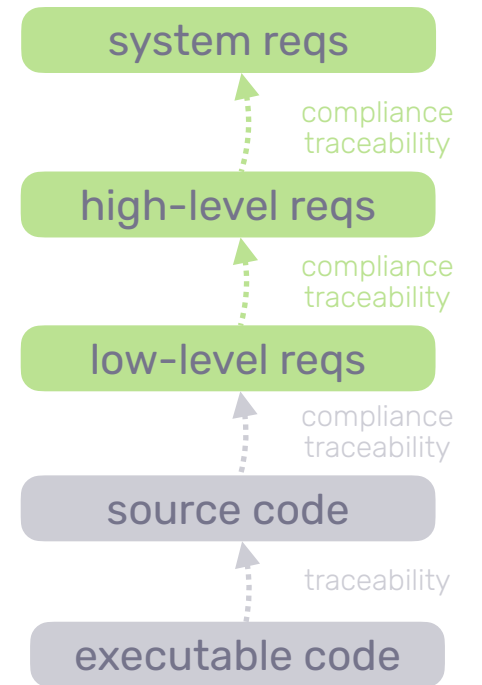


formal

informal



DO178-C Level A
Certification*



Why



Comparison

	QNX	Integrity	CertiKOS	FreeRTOS	seL4
Correctness Proof	—	—	✓	—	✓
Security Proof	—	✓	✓	—	✓
Fast IPC	—	—	—	—	✓
Deployed	✓	✓	—	✓	✓
Fine-grained access control	—	—	—	—	✓
MMU support	✓	✓	✓	—	✓
Virtualisation	✓	✓	✓	—	✓
General purpose	✓	✓	—	—	✓
Open Source	—	—	—	✓	✓

<https://sel4.systems/About/comparison.html>

Why



Platforms

**seL4 is available for a wide range of platforms
on Arm, RISC-V, and Intel architectures**

• Arm:

- Avnet MaaXBoard
- BeagleBoard
- BeagleBone Black
- IMX8MM-EVK
- i.MX8MP-EVK
- i.MX8MQ-EVK
- i.MX93-EVK
- Odroid-C2
- Odroid-C4
- OdroidX
- OdroidXU
- OdroidXU4
- Raspberry Pi 3b
- Raspberry Pi 4B
- Rockpro64
- Rock3b
- Sabre Lite
- TK1
- TK1-SOM
- TQMa8XQP 1GB
- TX1
- TX2
- Ultra96v2
- Zynq ZCU102
- Zynq-7000
- ZCU106
- Zynq-7000

• RISC-V:

- Ariane
- Cheshire
- Banana Pi BPI-F3
- Hifive Premier P550
- HiFive Unleashed
- Microchip PolarFire
- Pine64 Star64
- Rocketchip

• Intel:

- 32 bit PC-99
- 64 bit PC-99

Why



Platforms

**seL4 is available for a wide range of platforms
on Arm, RISC-V, and Intel architectures**

• Arm:

- ✓ Avnet MaaXBoard
- ✓ BeagleBoard
- ✓ BeagleBone Black
- ✓ IMX8MM-EVK
- ✓ i.MX8MP-EVK
- ✓ i.MX8MQ-EVK
- ✓ i.MX93-EVK
- ✓ Odroid-C2
- ✓ Odroid-C4
- ✓ OdroidX
- ✓ OdroidXU
- ✓ OdroidXU4
- ✓ Raspberry Pi 3b
- ✓ Raspberry Pi 4B
- ✓ Rockpro64
- ✓ Rock3b
- ✓ Sabre Lite
- ✓ TK1
- ✓ TK1-SOM
- ✓ TQMa8XQP 1GB
- ✓ TX1
- ✓ TX2
- ✓ Ultra96v2
- ✓ Zynq ZCU102
- ✓ Zynq-7000
- ✓ ZCU106
- ✓ Zynq-7000

• RISC-V:

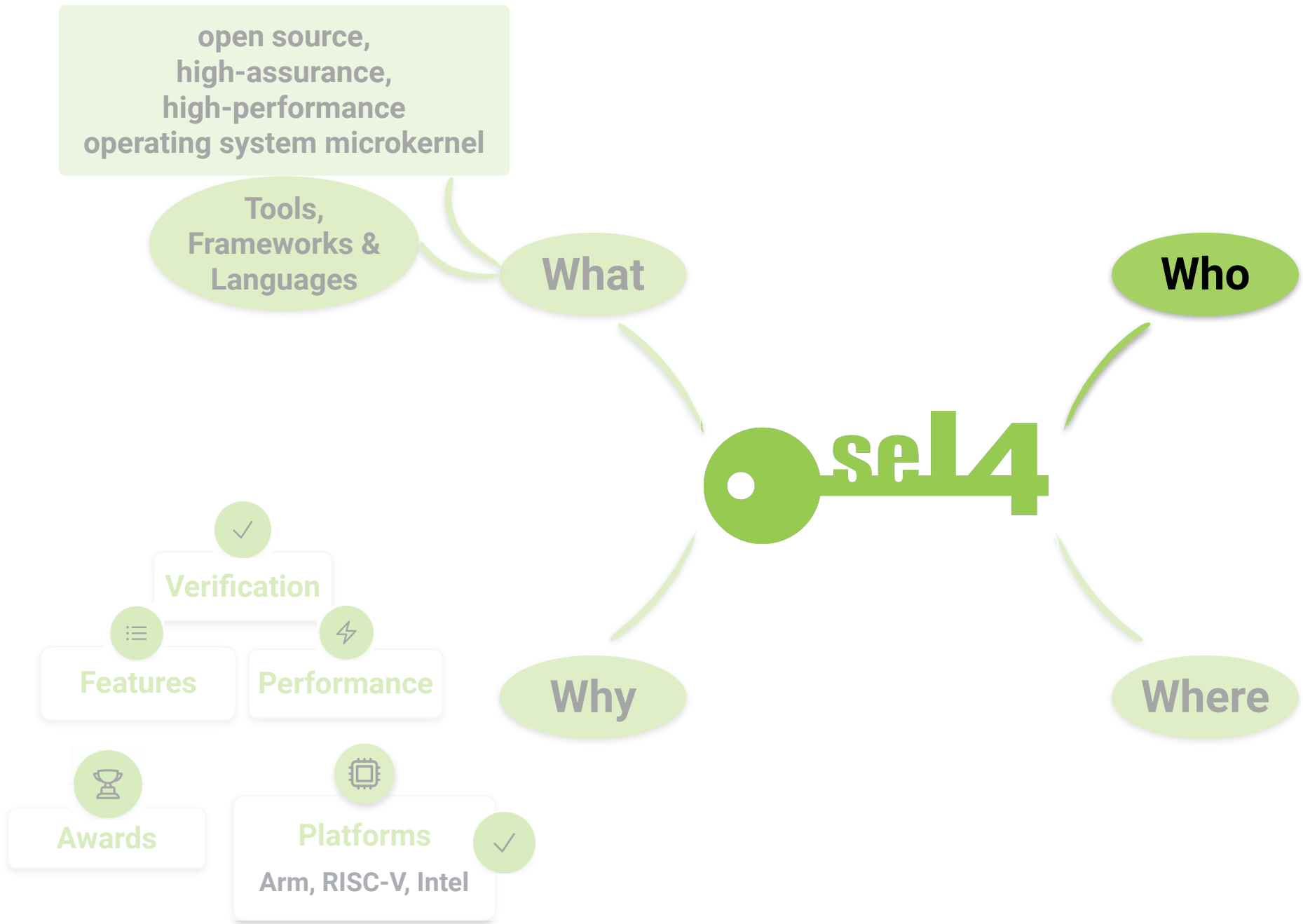
- ✓ Ariane
- ✓ Cheshire
- ✓ Banana Pi BPI-F3
- ✓ Hifive Premier P550
- ✓ HiFive Unleashed
- ✓ Microchip PolarFire
- ✓ Pine64 Star64
- ✓ Rocketchip

• Intel:

- 32 bit PC-99
- ✓ 64 bit PC-99

**and a wide range of configurations
(not all verified)**

<https://docs.sel4.systems/projects/sel4/verified-configurations.html>



Who



developers, users, providers,
customers, supporters, enthusiasts

Who



open-source, non-for-profit organisation
based in Switzerland



developers, users, providers,
customers, supporters, enthusiasts



Who



- ✓ Full set of tests at each code change
- ✓ Code and Proof always in sync
- ✓ Increasing set of hardware boards
- ✓ Hosting of the seL4 website
- ✓ Maintenance of cloud services
- ✓ ...



Continuous Integration



seL4 development



seL4 summit



IT infrastructure



Community Support



Leadership & Coordination



Who



- ✓ Expert advice and guidance
- ✓ Strategic extensions & improvements
 - ✓ Rust support
 - ✓ new seL4 features
 - ✓ new seL4 releases
 - ✓ user-level libraries and frameworks
 - ✓ ...



Indan



Nick



seL4 development



seL4 summit



Community Support



Leadership & Coordination



Who



2026, Vancouver, 75 participants



2025, Prague, 55 participants



2024, Sydney, 89 participants (15y anniversary)



2023, Minneapolis, 65 participants



2022, Munich, 70 participants



seL4 summit



Leadership & Coordination

Who



2026, Vancouver, 74 participants



2025, Prague, 55 participants



2024, Sydney, 89 participants (15y



2023, Minneapolis, 65 participants



2022, Munich, 70 participants

seL4 summit 2027?



Lucy



Martin

Who



Continuous Integration



seL4 development



seL4 summit



IT infrastructure



Community Support



Leadership & Coordination

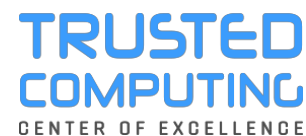


Who



Members







COLLINS AEROSPACE | PRATT & WHITNEY | RAYTHEON



Technical University
of Munich

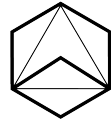


Endorsed
Service
Providers

<https://sel4.systems/Services/>



Australian
National
University



THE
AUTWARE
FOUNDATION



cyberagentur



DORNERWORKS

ETH zürich



Fraunhofer
AISEC

GAPFRUIT

KANSAS STATE
UNIVERSITY



KRYTO

Lewis & Clark




MEP
VOICE COMMUNICATION SYSTEMS



in association with
National Cyber
Security Centre

 neutrality



NIO

 Proofcraft



RTX

COLLINS AEROSPACE | PRATT & WHITNEY | RAYTHEON

 neutrality

Skykraft

Technical University
of Munich

TRUSTED
COMPUTING
CENTER OF EXCELLENCE



INSTITUTE FOR
INFORMATION
SCIENCES
The University of Kansas

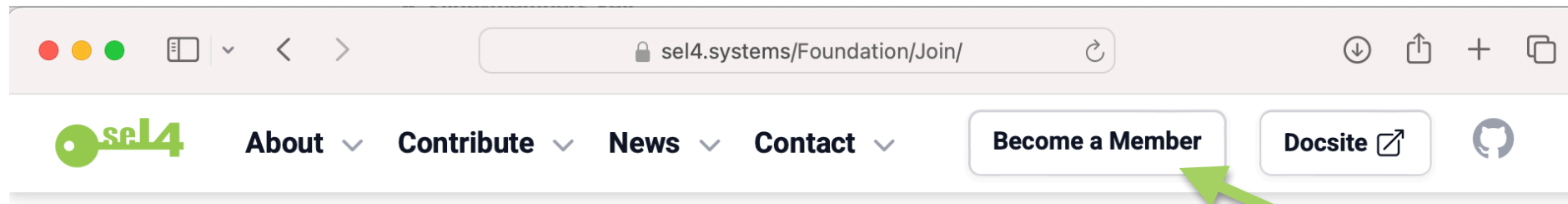


UNSW
SYDNEY

NEW



10% off your 1st year!



Membership Tiers

Premium

Guaranteed board seat

CHF 100k / year

[Join →](#)

General

One board seat as a class

Based on number of employees

CHF	35k / year	(5000+)
CHF	20k / year	(500-4999)
CHF	10k / year	(100-499)
CHF	4k / year	(21-99)
CHF	2.5k / year	(1-20)

[Join →](#)

Associate

No voting rights

Free

For non-profits and government entities.

[Join →](#)

Here
Today:



Raf



Ihor



Kent



Yanyan

Who

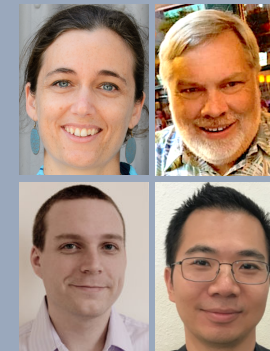
TSC



Members



Board



Here
Today:



David



Gerwin



Gernot



Where



Where



seL4 in mass production in NIO's cars



*NIO's SkyOS
product line*



Yanyan



<https://sel4.systems/use.html>

Where



seL4 in KOS operating system for mission critical connected devices



*OT Network
Guard*



Martin



<https://sel4.systems/use.html>

Where



seL4 in DornerWorks' VM Composer



VM
Composer



Robbie



DORNER**WORKS**

<https://sel4.systems/use.html>

Where



seL4 in Neutrality's Atoll hypervisor



David



<https://sel4.systems/use.html>

Where



seL4 in MEP's SureVoice Solid VCS



<https://sel4.systems/use.html>

Where



You?



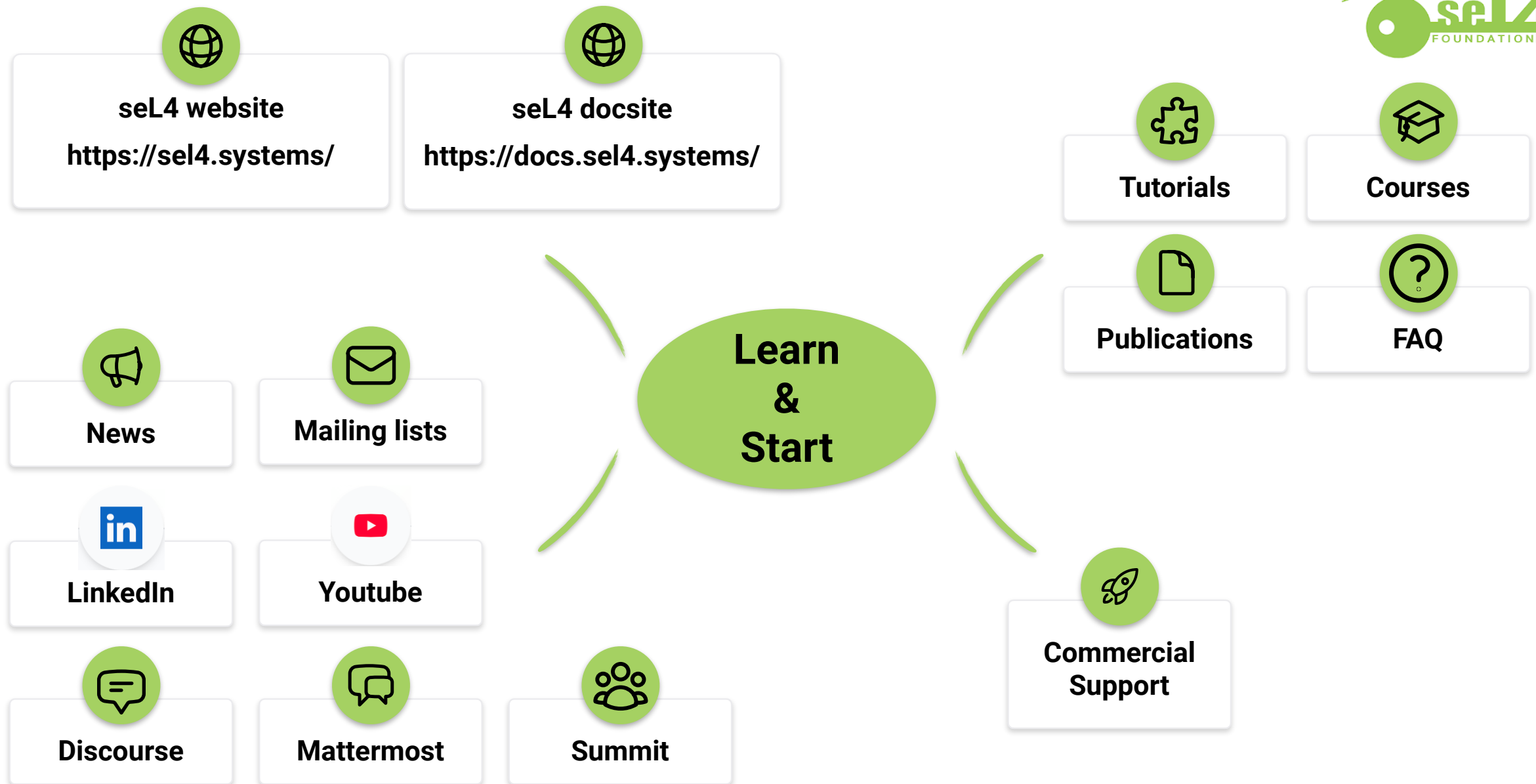




Photo by Gregory DALLEAU on Unsplash

