
Zephyr
Zephyr Project Meetup
January 30, 2026
2:00 PM - 7:00 PM
Brussels, Belgium

Thank you to our host

Thank you to the organizers for making this possible!

Frederik Van Bogaert

Senior Embedded Software Developer, Mind

Titouan Christophe

Embedded Software Engineer, Mind

Agenda:

2:25 PM	Introduction & Welcome	Susan Remmert, LF
2:30 PM	State of the Zephyr project	Kate Stewart, LF
3:00 PM	Turning the Microbit V2 into a BTLE microphone using Zephyr	Colin Evrard and Javad Rahimi, Mind Software Consultancy
3:30 PM	Break Time	
3:50 PM	Zephyr & LLMs: The Good, The Bad, and the Hallucinated	Benjamin Cabe, Zephyr project
4:30 PM	MIDI Weaver	Titouan Cristophe, Mind Software Consultancy
5:00 PM	Zephyr release engineering	Fabio Baltieri, Google
5:40 PM	Open Discussions	Community
18:00	Closing Note	Susan Remmert, LF

Zephyr Project Meetup

State of Zephyr Project

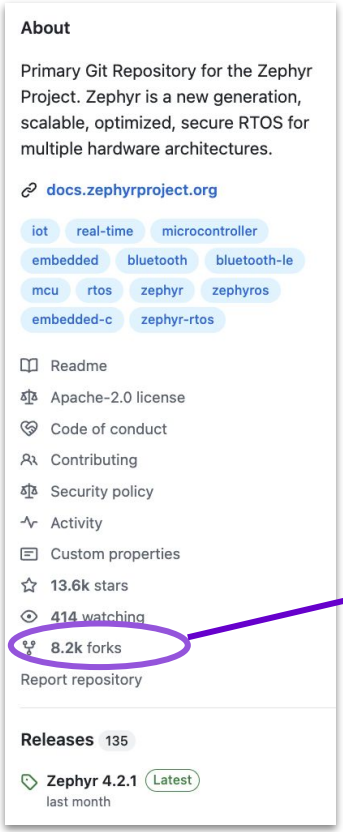
Kate Stewart

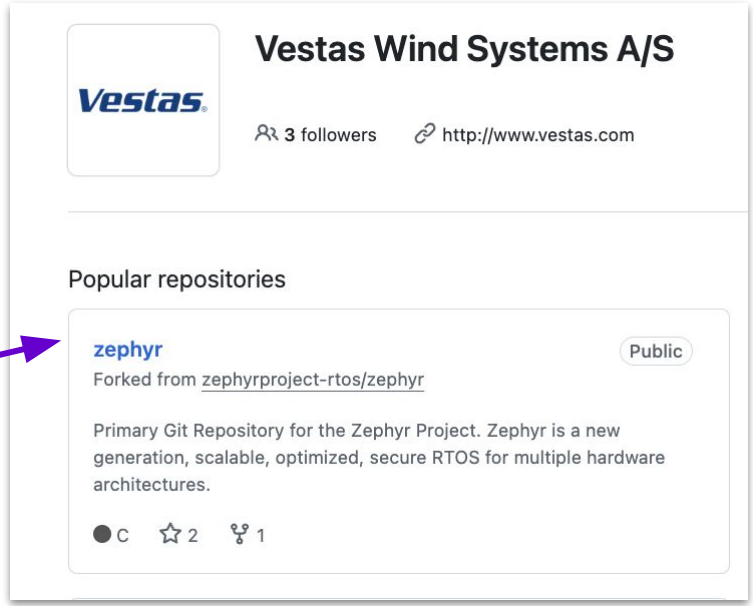
January 30, Brussels, Belgium

Features overview

- **Lightweight kernel & supporting drivers and services**
- **Portable, secure, power-efficient**
- **Highly connected**
  - Bluetooth 5.0 & BLE
  - Wi-Fi, Ethernet, CANbus, ...
  - IoT protocols: CoAP, LwM2M, MQTT, OpenThread, ...
  - USB & USB-C
- **Complete developer environment**
  - Toolchain and HAL management
  - Logging, tracing, debugging
  - Emulation/Simulation
  - Testing framework

Zephyr in the wild… 8K+ Forks!





Source: https://github.com/vestas-wind-systems

Source: https://github.com/zephyrproject-rtos/zephyr

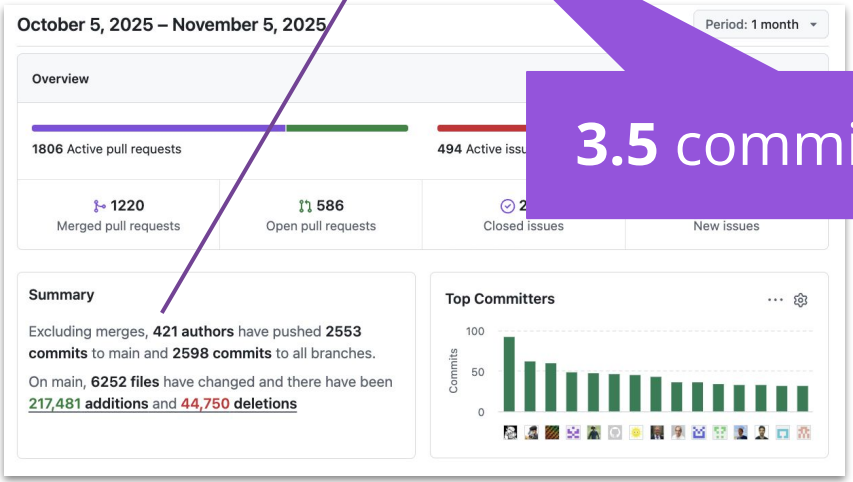
Operating System	First Commit	Controls Commits	Declared License	Total Contributors	Contributors in last month	Total Commits	Commits in last month
Zephyr	2014/11	**community**	**Apache-2.0**	**2955**	**421**	**126,450**	**2,598**
nuttX	2007/?	community	BSD-variant → Apache-2.0	647	30	59,473	174
RT-Thread	2009/06	community	GPL-2.0 → Apache-2.0	773	26	17,535	132
RIOT	2010/09	community	LGPL-2.1	381	20	48,734	140
Tizen RT	2015/04	Samsung	BSD-variant → Apache-2.0	214	10	11,902	33
Ariel-OS	2020/08	community	Apache-2.0 OR MIT	26	8	3,557	202
myNewt	2015/06	community	Apache-2.0	137	6	11,336	28
SeL4	2014/07	community	GPLv2 AND BSD-2-Clause	115	6	4,789	26
FreeRTOS	2004/07	Richard Barry	GPL-2.0 w/ FreeRTOS → MIT	223	4	3,617	3
Contiki-NG	2017/10	community	BSD-3-Clause	218	1	18,091	1
ThreadX	2020/05	MSFT → community	MSL → MIT	25	0	254	0

Data extracted on 2025-11-05 from github

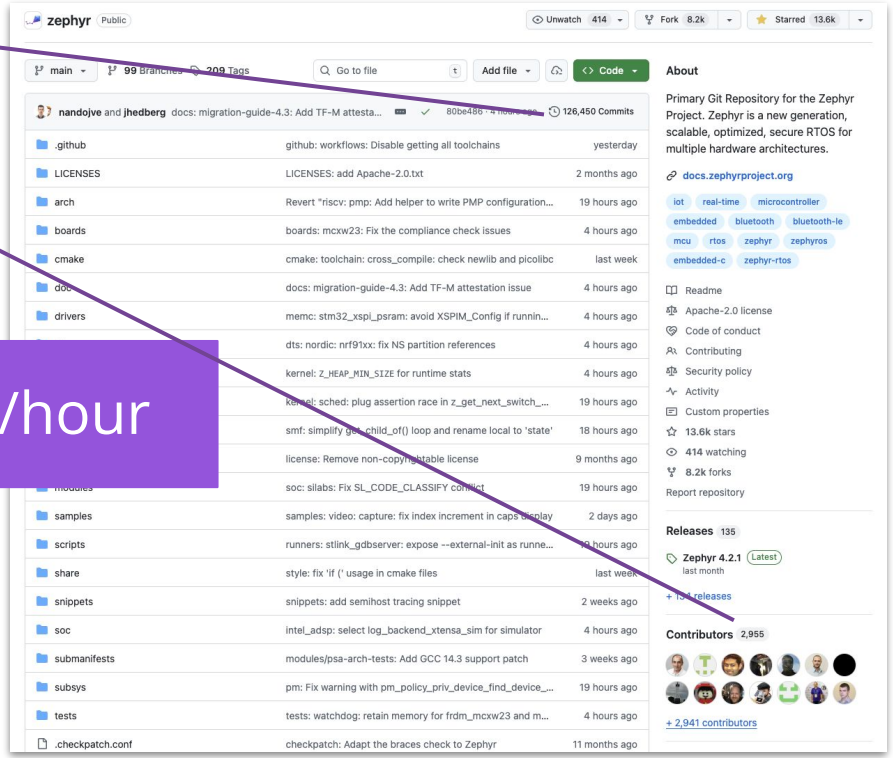
Methodology: Sample from Github

https://github.com/zephyrproject-rtos/zephyr
- Total commits: 126,450
- Total contributors: 2,955

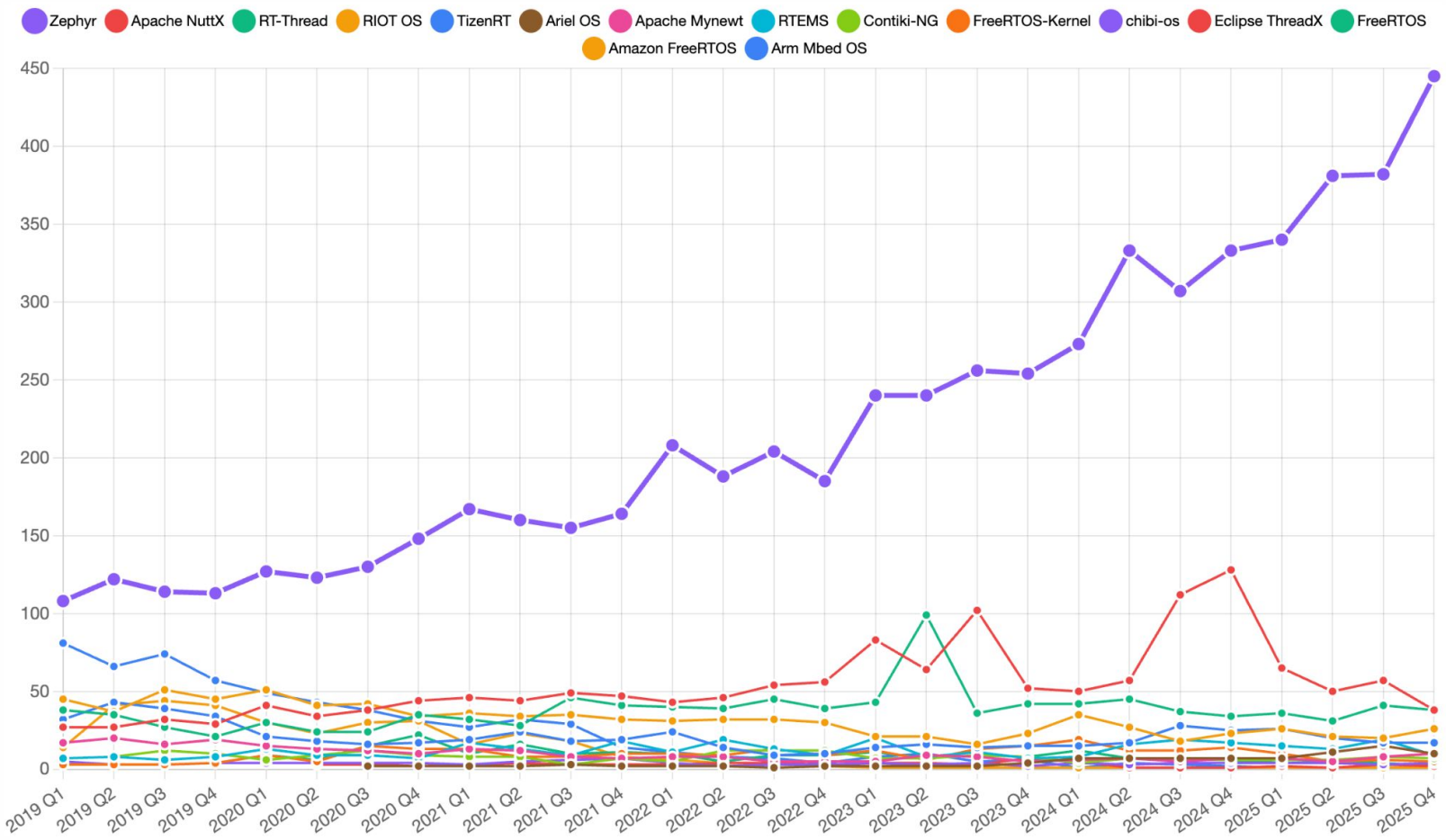
https://github.com/zephyrproject-rtos/zephyr/pulse/monthly
- Monthly contributors: 421
- Monthly commits: 2,598



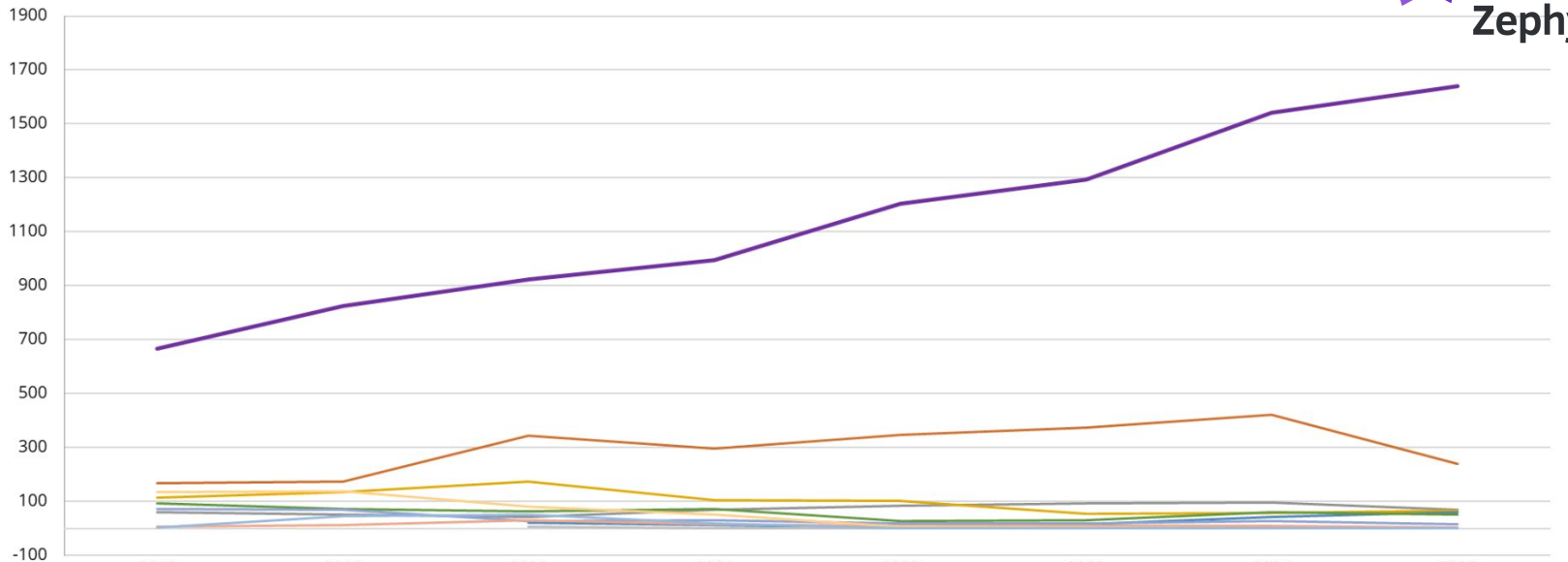
3.5 commits/hour



Unique Contributors per Month



Average Number of Commits per Month



	2018	2019	2020	2021	2022	2023	2024	2025
Zephyr	667	825	924	995	1206	1293	1543	1640
Apache NuttX	169	174	343	297	347	373	423	241
RT-Thread	60	53	43	70	84	93	97	71
RIOT OS	115	136	175	105	103	54	59	66
Ariel OS			23	12	6	16	44	61
TizenRT	93	71	64	74	27	30	60	53
Apache Mynewt	74	70	27	31	18	20	29	16
FreeRTOS	8	13	32	17	11	11	11	4
Eclipse ThreadX			7	1	2	4	1	1
Arm Mbed OS	136	138	82	51	6	5	2	0
Amazon FreeRTOS	4	47	53	20	2	0	0	0

GitHub Clones & Unique Visitors

2025-04-23 → 2025-05–06

~1183 unique clones per day
~1532 unique visitors per day

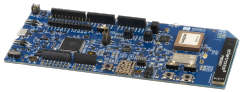
900+ supported boards... and growing

Zephyr®

Arduino Portenta H7

ESP32

Sipeed HiFive1



nRF9160 DK

STM32F746G Disco

M5StickC PLUS

TDK RoboKit 1

BBC micro:bit v2

Blues Swan

Arduino Nano 33 BLE

Intel UP Squared

Dragino LSN50 LoRA Sensor Node

Quicklogic Qomu

Raspberry Pi Pico

Renesas RX130

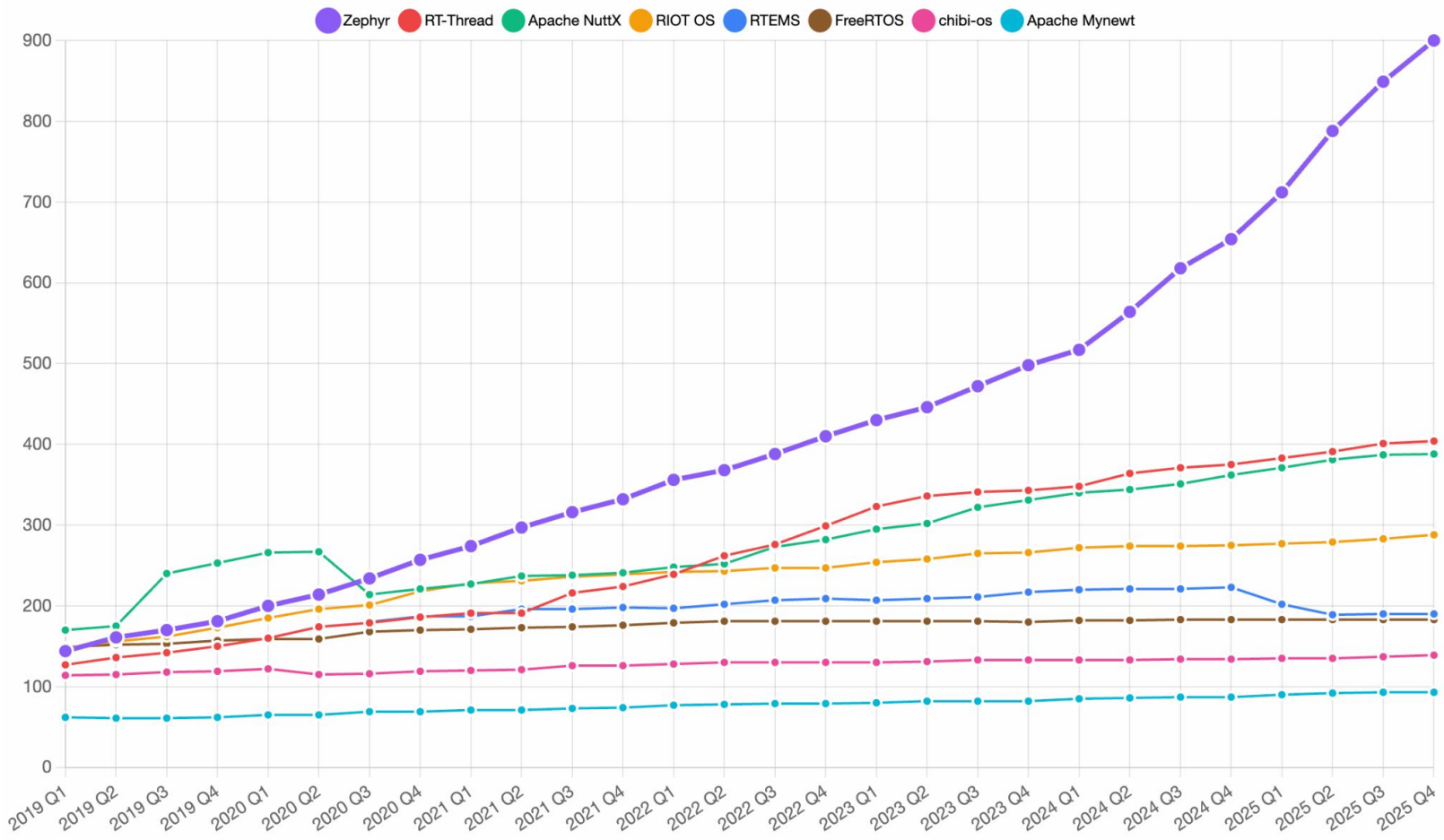
NXP i.MX8MP EVK

Adafruit Feather M0 LoRa

u-blox EVK-NINA-B3

docs.zephyrproject.org/latest/boards/

Supported Boards



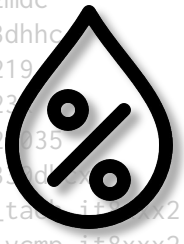
Note: Only the operating systems for which number of supported boards could be easily computed automatically are included on this chart.

280+ Sensors Already Integrated

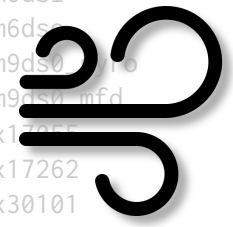
adt7420
adxl345
adxl362
adxl372
ak8975
amg88xx
ams_as5600
ams_iAQcore
apds9960
bma280
bmc150_magn
bme280
bme680
bmg160
bmi160
bmi270
bmm150
bmp388
bq274xx
ccs811

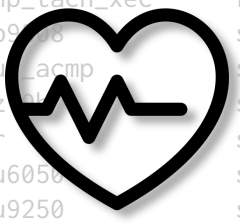
dht
dps310
ds1[illegible]
ens[illegible]
esp[illegible]
fdc[illegible]
fx[illegible]
fx[illegible]
grove
grow_r502a
hmc5883l
hp206c
ht[illegible]221
i[illegible]250d
i[illegible]2605
i[illegible]2670
i[illegible]
icp[illegible]125
iis2dh
iis2dlpc

iis2iclx
iis2mdc
iis3dhhc
ina219
ina23[illegible]
isl2[illegible]35
ism3[illegible]
ite_ta[illegible]x2
ite_vcmp_it8xxx2
lis2dh
lis2ds12
lis2dw12
lis2[illegible]
lis3[illegible]
lm75[illegible]
lm77[illegible]
lps22[illegible]
lps22hh
lps25hb
lsm303dlhc_magn

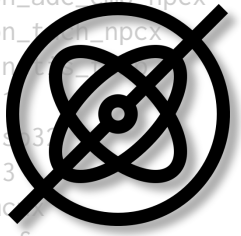


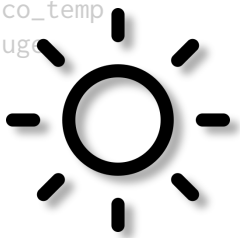
lsm6ds0
lsm6dsl
lsm6ds[illegible]
lsm9ds0[illegible]
lsm9[illegible]mfd
max1[illegible]
max17262
max30101
max31875
max44009
max6675
mchp_tach_xec
mcp9[illegible]
mcu_[illegible]acmp
mhz[illegible]
mpr
mpu6050
mpu9250
ms5607
ms5837





nrf5
nuvoton_adc_cmp_npcx
nuvoton_t[illegible]_npcx
nxp_kin[illegible]
opt300[illegible]
pcnt_es[illegible]
pms7003
qdec_mc[illegible]
qdec_nrfx
qdec_sam
qdec_stm32
rpi_pico_temp
sbs_gaug[illegible]
sgp40
sht3xd
sht4x
shtcx
si7006
si7055
si7060





si7210
sm351lt
stm32_temp
stm32_vbat
stmemsc
stts751
sx9500
th02
ti_hdc
ti_hdc20xx
tmp007
tmp108
tmp112
tmp116
vcnl4040
vl53l0x
wsen_hids
wsen_itds

github.com/zephyrproject-rtos/zephyr/tree/main/drivers/sensor

Supported Hardware Architectures

Cortex-M, Cortex-R
& Cortex-A

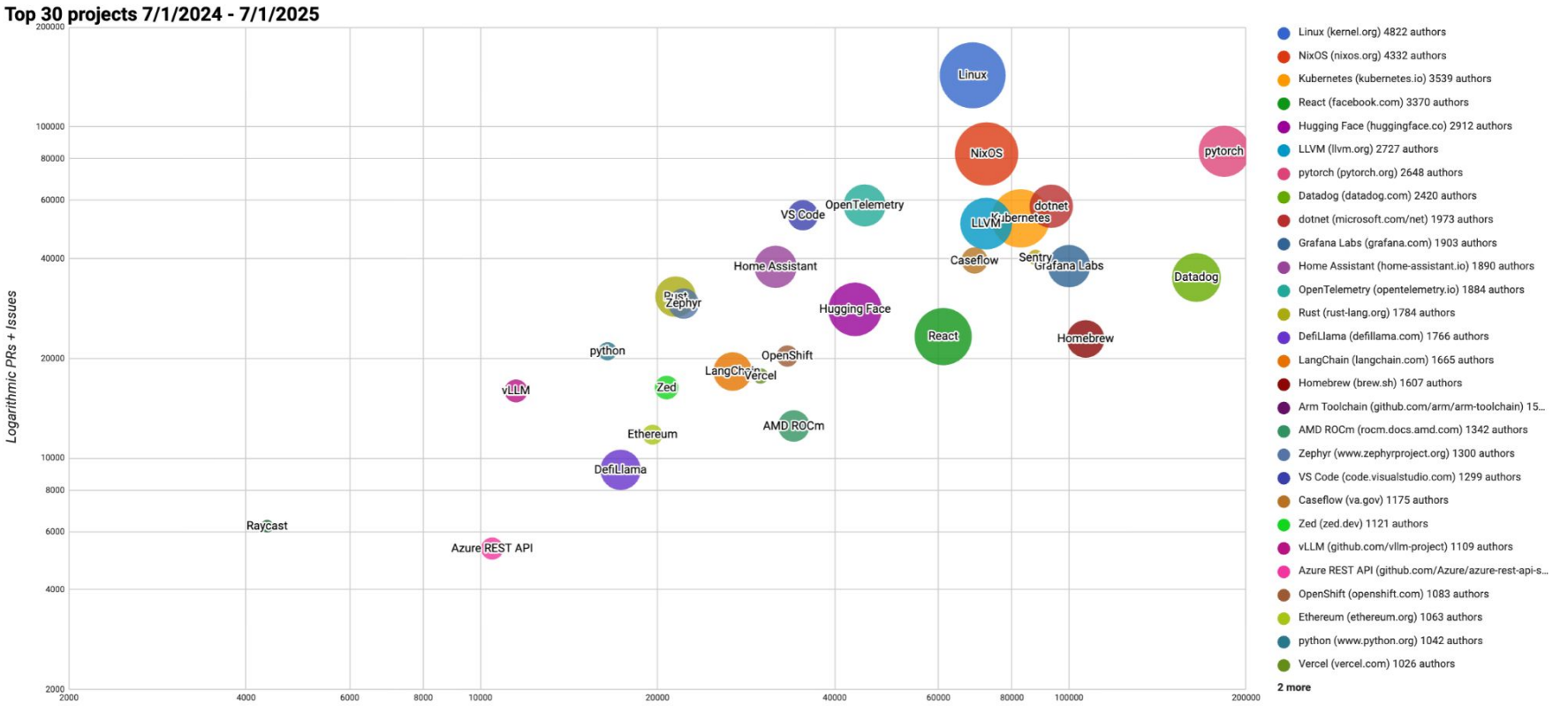
x86 & x86_64

32 & 64 bit

Xtensa

docs.zephyrproject.org/latest/hardware/index.html#hardware-support

All OSS Project Velocity: Zephyr #19!



Source: https://docs.google.com/spreadsheets/d/1KBlQIBOO-i3GuAJd69lAWN5PMA8GxJfj3yKxFLyqGFg/edit

Small Sample of Products Running Zephyr Today

Oticon More Hearing Aid

Lildog & Lilcat Pet Tracker

Livestock Tracker

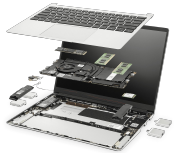
Moto Watch 100

Samsung Galaxy Ring

Proglove

Adhoc Smart Waste

Google Chromebook



Framework laptop

Keeb.io BDN9

Hati-ACE

Blackhole™ PCIe AI Accelerator

BLiXT solid state circuit breaker

Aethero Deimos Satellite

PHYTEC Distancer

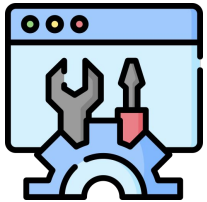
Laird Connectivity sensors & gateways

BeST pump monitoring

Vestas Wind Turbines

zephyrproject.org/products-running-zephyr

Vibrant Ecosystem



Development Tools

Zephyr®

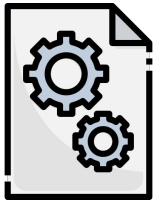
Governing Board

Technical Steering Committee

Contributors

Applications & Middlewares

Training & Consulting

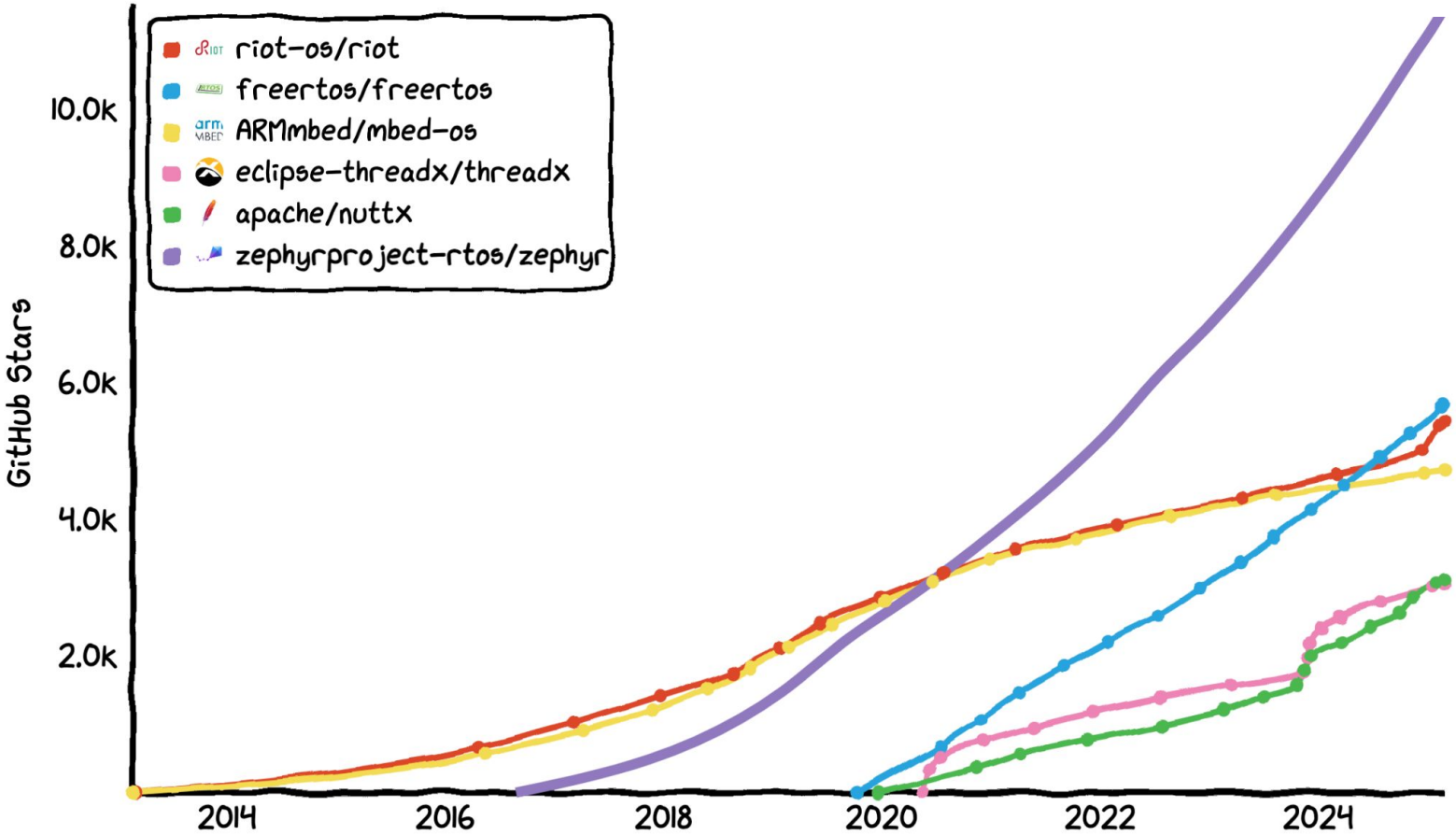


Firmwares & Libraries

Star History

Starred 13.6k

Zephyr®



Ecosystem // Developer Tools

Zephyr®

Development Tools

Training & Consulting

Firmwares & Libraries

Applications & Middlewares

IDE







Compilers



Debuggers / Tracing Tools





Emulation / Simulation



Ecosystem // Training & Consulting

Zephyr®

Development Tools

Training & Consulting

Firmwares & Libraries

Applications & Middlewares

Training

ac6 · DOULOS · Golioth · inovex · NORDIC SEMICONDUCTOR

percepio SENSING SOFTWARE · BENINGO EMBEDDED GROUP · Savoir-faire LINUX · THE LINUX FOUNDATION

Services & Consulting

ANALOG DEVICES · antmicro · AVSYSTEM · Baylibre

ezurio · inovex · NXP · WNDRVR

Ecosystem // Firmwares & Libraries

Zephyr®

Development Tools

Training & Consulting

Firmwares & Libraries

Applications & Middlewares

Security

wolfSSL

psacertified™

Mbed TLS

TrustedFirmware.org

TinyML

TensorFlow Lite

EDGE IMPULSE

emlearn

Language runtimes

C++

JS

Rust

Lua

circuitpython

MicroPython

Others

SOUND OPEN FIRMWARE

zscilib

nRF Connect SDK

Memfault

Zenoh

Ecosystem // Apps & Middlewares

Zephyr®

Development Tools

Training & Consulting

Firmwares & Libraries

Applications & Middlewares

Remote Management

AVSYSTEM · blues · Blynk · Golioth · HERALD · Memfault · STERNUM · MENDER by Northern.tech

Graphical Interfaces

LVGL · MICROEJ · Qt Group · slint

Robotics

ROS · COGNIPILOT · F´

Zephyr 4.3 (Nov. 2025) – What's new?

⚙️ **CPU load monitoring & dynamic frequency scaling**

🔧 **Instrumentation** subsystem

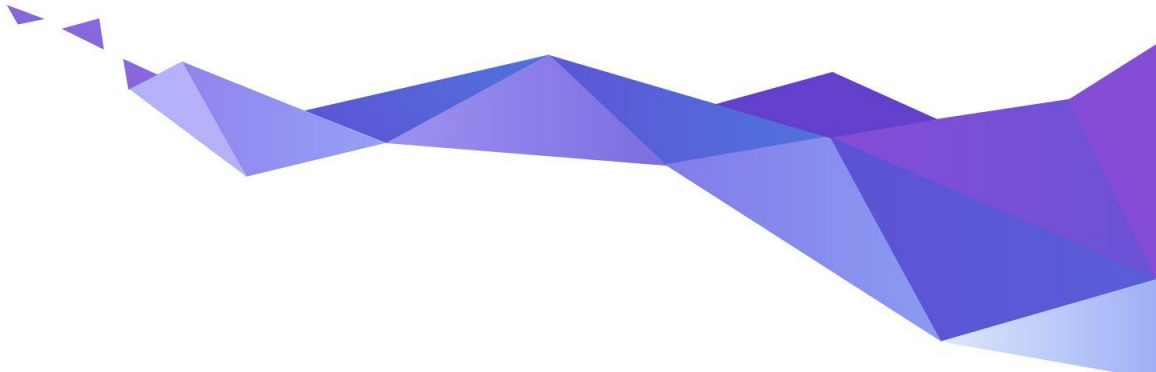
🔋 **OCPP 1.6** support (for EV Charging)

🖥️ **Twister display harness** for automated testing of displays/GUIs

👩‍💻 **Developer Experience improvements** – Several new tools to help with debugging/troubleshooting (DT doctor, traceconfig)

and more, see Release notes 4.3.

Security support in Zephyr



Long Term Support

- **Product Focused**
- Current with latest **Security Updates**
- Compatible with new hardware
  - Functional support for new hardware is regularly backported
- **Tested**: Shorten the development window and extend the Beta cycle to allow for more testing and bug fixing
- **Supported for 2+ years ⇒ 5 years** (as of 2025/3/8)
- ⚠️ **Doesn’t include cutting-edge functionality**

github.com/zephyrproject-rtos/zephyr/releases/tag/zephyr-v2.7.0

LTS Support Windows

Supported Releases

Release	Release date	EOL
Zephyr 4.1.0	2025-03-07	2025-11-14
Zephyr 4.0.0	2024-11-15	2025-07-18
Zephyr 3.7.0 (LTS3)	2024-07-26	2029-07-27

Previous LTS

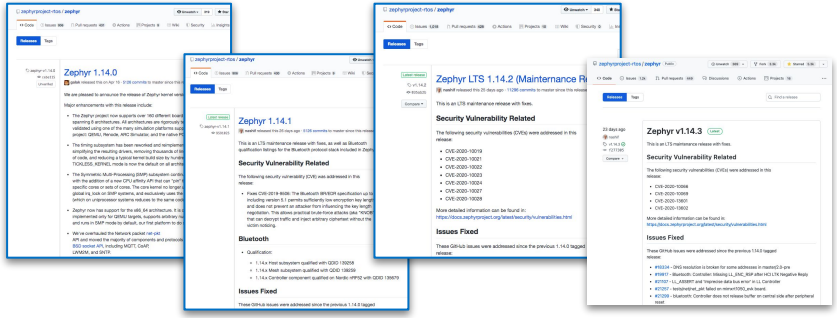
Release	EOL
Zephyr 2.7.6 (LTS2)	2025-01-26
Zephyr 1.14.1 (LTS1)	2022-01-01

Source: https://docs.zephyrproject.org/latest/releases/index.html#supported-releases

Long Term Support (LTS 1 & LTS 2)

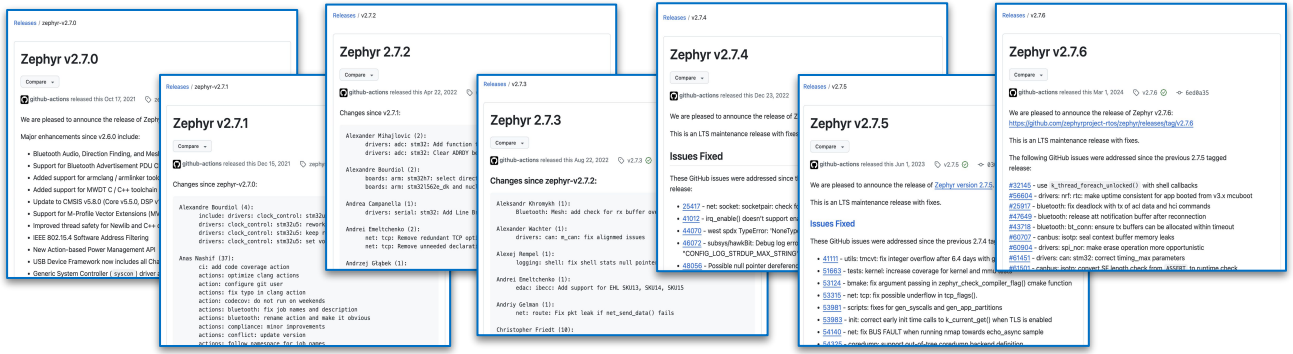
LTS 1

Apr ‘19 → Nov ‘21



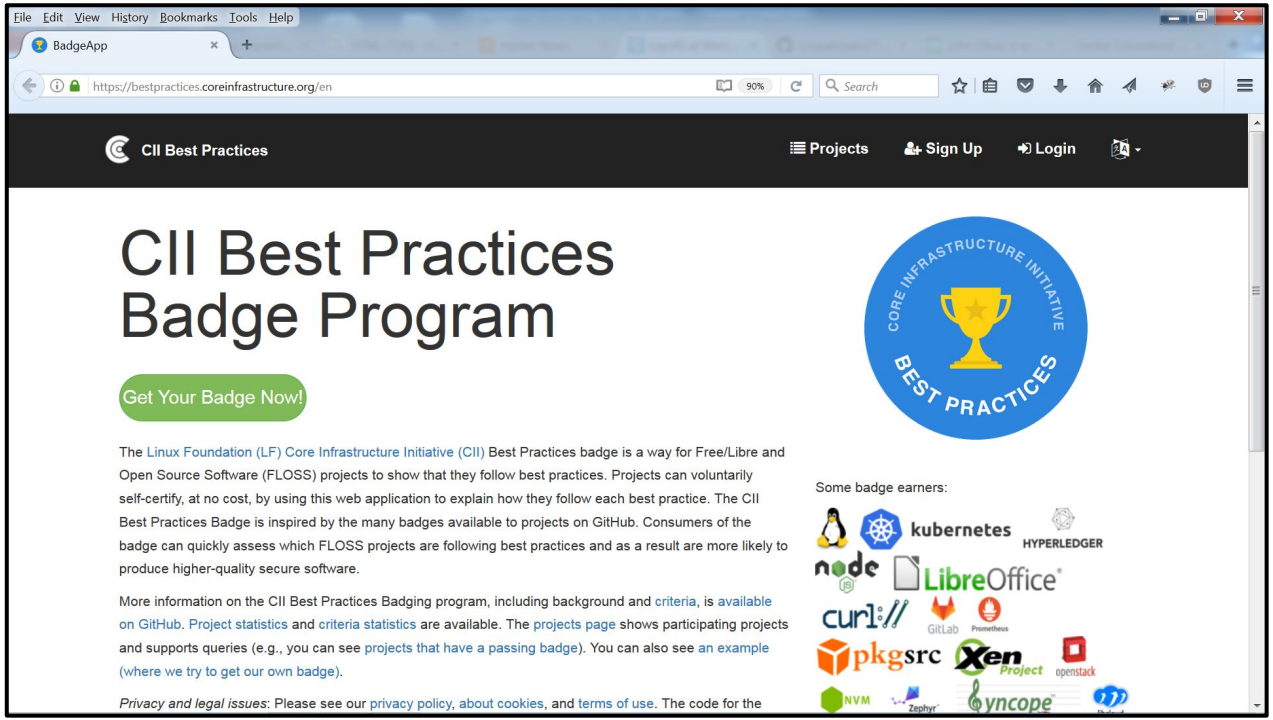
LTS 2

Oct ‘21 → Jan ‘25



Delivered bug fixes and latest security updates for 2+ years!

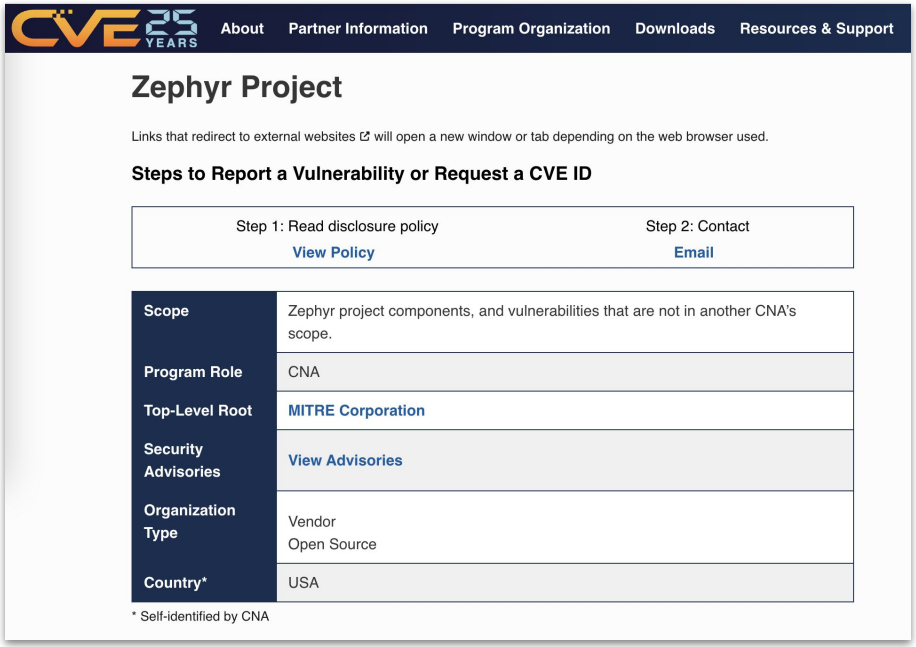
Adopted Known Best Security Practices



https://bestpractices.coreinfrastructure.org

CVE Numbering Authority

- **Registered with MITRE** in 2017
  - Zephyr triages and issue our own CVEs
- **Zephyr Project Security Incident Response Team** (PSIRT)
  - Volunteers from the Security Committee
  - Led by the Zephyr Security Architect.

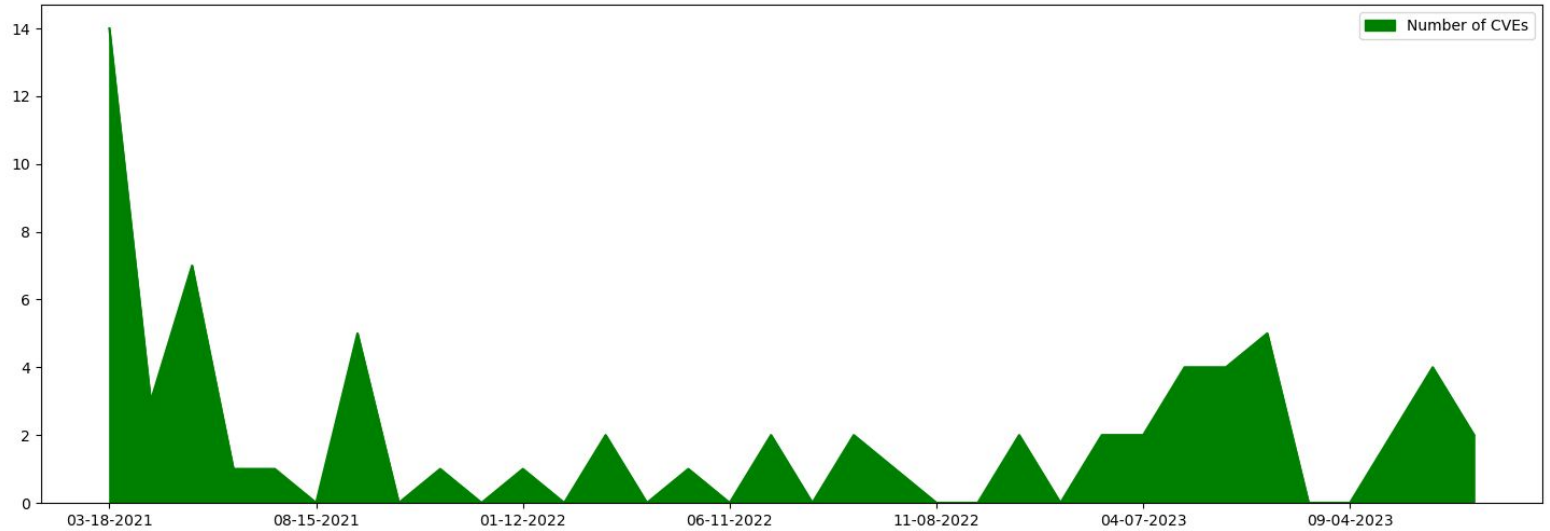


Vulnerability Infrastructure → Github 2021

Why Transition?

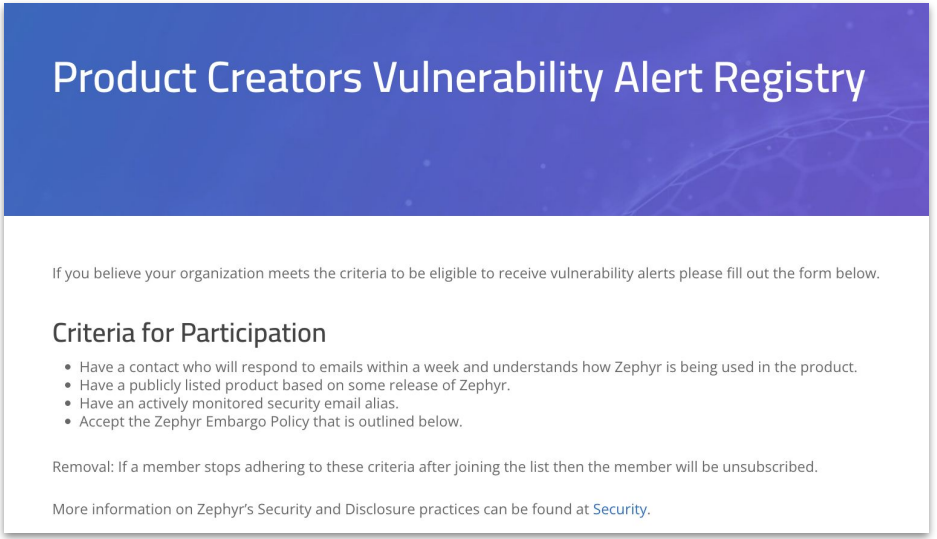
Private repos became available. Better integration with rest of code.
No additional ids to manage. Improved analysis capabilities

Total of CVEs published : 68 (since we started using github)



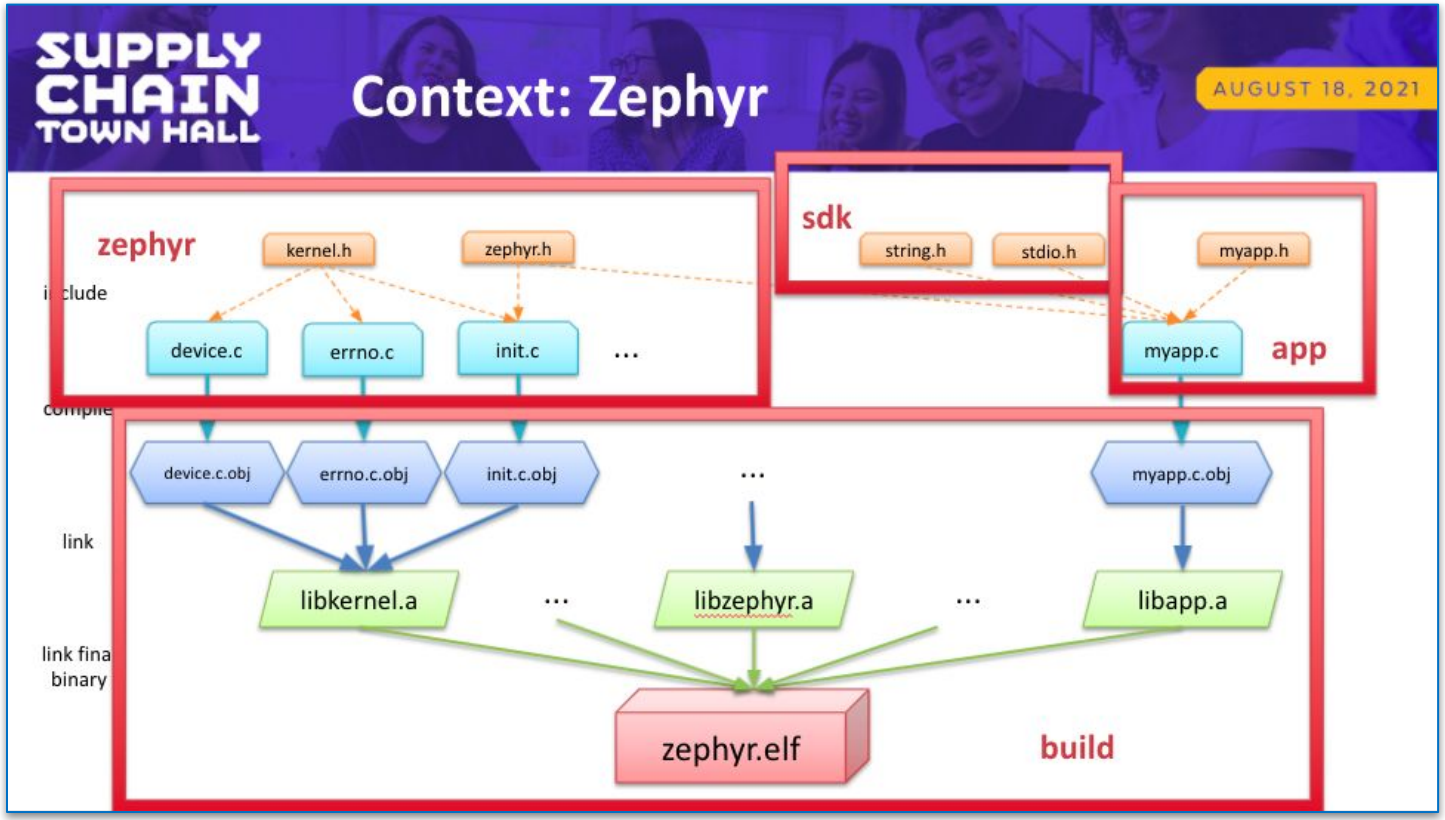
Support for Product Makers

- For an embargo to work, product makers need to be notified early so they can remediate.
- Created Vulnerability Registry for **vendors to register** to receive these alerts for **free**
- **Goal:** Zephyr to **fix issues within 30 days** to give **vendors 60 days** before publication of vulnerability



Source: https://www.zephyrproject.org/vulnerability-registry/

SBOM generation added in 2021



Learn more at: https://www.youtube.com/watch?v=KYC3YpSu9zs

Automated SBOM Generation During Build!

1. Create a build directory with CMake file API enabled
2. Build project with “build metadata” enabled
3. Compute SBOM(s)

```
west spdx --init -d BUILD_DIR
west build -d BUILD_DIR -- -DCONFIG_BUILD_OUTPUT_META=y
west spdx -d BUILD_DIR
```

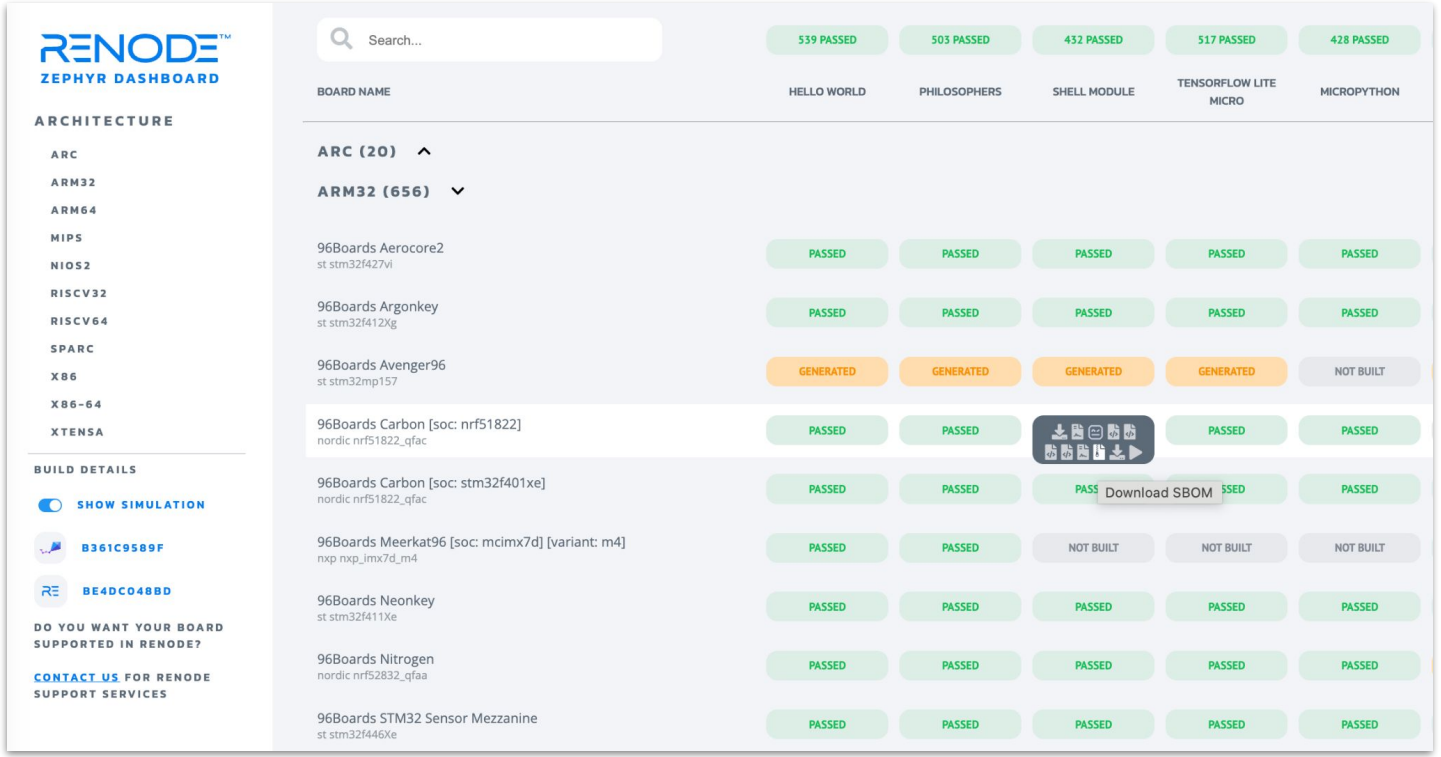
`zephyr.spdx`	SBOM for the **Zephyr source files** actually used by your application
`app.spdx`	SBOM for the source files of your **application**
`build.spdx`	SBOM for **all the build objects**, inc. of course your final image

SBOM's at Scale...Automatically

875 boards

13 apps

All BUILT, PASSED, GENERATED have **3 SBOM**s available to download & inspect



Source: https://zephyr-dashboard.renode.io/

Dashboard SBOM

blinky-app.spdx

```
SPDXVersion: SPDX-2.3
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: app-sources
DocumentNamespace: http://spdx.org/spdxdocs/zephyr-ab992a5d-47b4-44ee-8357-1b68719b389b/app
Creator: Tool: Zephyr SPDX builder
Created: 2024-06-07T01:12:51Z

Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-app-sources

##### Package: app-sources

PackageName: app-sources
SPDXID: SPDXRef-app-sources
PackageDownloadLocation: NOASSERTION
PackageLicenseConcluded: Apache-2.0
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
PrimaryPackagePurpose: SOURCE
PackageLicenseInfoFromFiles: Apache-2.0
FilesAnalyzed: true
PackageVerificationCode: a5993032fe245294fb73f4ed2f53be33566662f6

FileName: ./src/main.c
SPDXID: SPDXRef-File-main.c
FileChecksum: SHA1: d71a9d7b80f5eac4b749b84c57297614ef8e3899
FileChecksum: SHA256: cdc42b14891c38dfc131eb3dea80906698289496a18c7e76e9945f2e3dd17152
LicenseConcluded: Apache-2.0
LicenseInfoInFile: Apache-2.0
FileCopyrightText: NOASSERTION
```

blinky-zephyr.spdx

```
SPDXVersion: SPDX-2.3
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: zephyr-sources
DocumentNamespace: http://spdx.org/spdxdocs/zephyr-ab992a5d-47b4-44ee-8357-1b68719b389b/zephyr
Creator: Tool: Zephyr SPDX builder
Created: 2024-06-07T01:12:51Z

Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-zephyr-sources

##### Package: zephyr-sources

PackageName: zephyr-sources
SPDXID: SPDXRef-zephyr-sources
PackageDownloadLocation: NOASSERTION
PackageLicenseConcluded: Apache-2.0
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
PackageLicenseInfoFromFiles: Apache-2.0
FilesAnalyzed: true
PackageVerificationCode: f10da9dec03dd29bb556c72963bf33ae9f840643

FileName: ./zephyr/arch/arm/core/cortex_m/__aeabi_read_tp.S
SPDXID: SPDXRef-File---aeabi-read-tp.S
FileChecksum: SHA1: 62d0921844d538be8c28eae5bc4c0b9f87692bd3
FileChecksum: SHA256: 1ba5712dbc2a5d48a57fde5070b2cdc0f6b2bb86a740ae2f55811aaf1bea0aa1
LicenseConcluded: Apache-2.0
LicenseInfoInFile: Apache-2.0
FileCopyrightText: NOASSERTION
```

blinky-build.spdx

```
SPDXVersion: SPDX-2.3
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: build
DocumentNamespace: http://spdx.org/spdxdocs/zephyr-ab992a5d-47b4-44ee-8357-1b68719b389b/build
Creator: Tool: Zephyr SPDX builder
Created: 2024-06-07T01:12:51Z

ExternalDocumentRef: DocumentRef-app http://spdx.org/spdxdocs/zephyr-
ab992a5d-47b4-44ee-8357-1b68719b389b/app SHA1: 594de9d45188c55bdb059a2b0045987bb87e79be
ExternalDocumentRef: DocumentRef-zephyr http://spdx.org/spdxdocs/zephyr-
ab992a5d-47b4-44ee-8357-1b68719b389b/zephyr SHA1: 4ae97af97a0e9fbc050f72ea71ad3bf2f9caffa7

Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-zephyr-final

                ...

FileName: ./zephyr/arch/arch/arm/core/cortex_m/libarch__arm__core__cortex_m.a
SPDXID: SPDXRef-File-libarch--arm--core--cortex-m.a
FileChecksum: SHA1: 310c7abd765821c8e8df8ceb1ac8bae330f371b1
FileChecksum: SHA256: 5efe0a524dd3a48e7cf6d637966a4f6fffa60119f4ab2b2b2f3ec4d924f5ea2a
LicenseConcluded: NOASSERTION
LicenseInfoInFile: NONE
FileCopyrightText: NOASSERTION

Relationship: SPDXRef-File-libarch--arm--core--cortex-m.a GENERATED_FROM DocumentRef-zephyr:SPDXRef-File-exc-exit.c
Relationship: SPDXRef-File-libarch--arm--core--cortex-m.a GENERATED_FROM DocumentRef-zephyr:SPDXRef-File-fault.c
Relationship: SPDXRef-File-libarch--arm--core--cortex-m.a GENERATED_FROM DocumentRef-zephyr:SPDXRef-File-fault-s.S
Relationship: SPDXRef-File-libarch--arm--core--cortex-m.a GENERATED_FROM DocumentRef-zephyr:SPDXRef-File-fpu.c
Relationship: SPDXRef-File-libarch--arm--core--cortex-m.a GENERATED_FROM DocumentRef-zephyr:SPDXRef-File-reset.S
Relationship: SPDXRef-File-libarch--arm--core--cortex-m.a GENERATED_FROM DocumentRef-zephyr:SPDXRef-File-scb.c
Relationship: SPDXRef-File-libarch--arm--core--cortex-m.a GENERATED_FROM DocumentRef-zephyr:SPDXRef-File-thread-abort.c
Relationship: SPDXRef-File-libarch--arm--core--cortex-m.a GENERATED_FROM DocumentRef-zephyr:SPDXRef-File-vector-table.S
Relationship: SPDXRef-File-libarch--arm--core--cortex-m.a GENERATED_FROM DocumentRef-zephyr:SPDXRef-File-swap.c
Relationship: SPDXRef-File-libarch--arm--core--cortex-m.a GENERATED_FROM DocumentRef-zephyr:SPDXRef-File-swap-helper.S
Relationship: SPDXRef-File-libarch--arm--core--cortex-m.a GENERATED_FROM DocumentRef-zephyr:SPDXRef-File-irq-manage.c
Relationship: SPDXRef-File-libarch--arm--core--cortex-m.a GENERATED_FROM DocumentRef-zephyr:SPDXRef-File-prep-c.c
Relationship: SPDXRef-File-libarch--arm--core--cortex-m.a GENERATED_FROM DocumentRef-zephyr:SPDXRef-File-thread.c
Relationship: SPDXRef-File-libarch--arm--core--cortex-m.a GENERATED_FROM DocumentRef-zephyr:SPDXRef-File-cpu-idle.c
Relationship: SPDXRef-File-libarch--arm--core--cortex-m.a GENERATED_FROM DocumentRef-zephyr:SPDXRef-File-irq-init.c

                ...

FileName: ./zephyr/zephyr.elf
SPDXID: SPDXRef-File-zephyr.elf
FileChecksum: SHA1: 2e80741d3c373bd7626bc49625783ea8fd1bcacb
FileChecksum: SHA256: 7a838128652e85835f9167be429d41559701533fbd0d09b6bab9176a289fdc5e
LicenseConcluded: NOASSERTION
LicenseInfoInFile: NONE
FileCopyrightText: NOASSERTION

Relationship: SPDXRef-File-zephyr.elf GENERATED_FROM DocumentRef-zephyr:SPDXRef-File-empty-file.c
Relationship: SPDXRef-File-zephyr.elf GENERATED_FROM SPDXRef-File-isr-tables.c
Relationship: SPDXRef-File-zephyr.elf STATIC_LINK SPDXRef-File-libapp.a
Relationship: SPDXRef-File-zephyr.elf STATIC_LINK SPDXRef-File-libzephyr.a

                ...
```

Security Working Group added March 2022

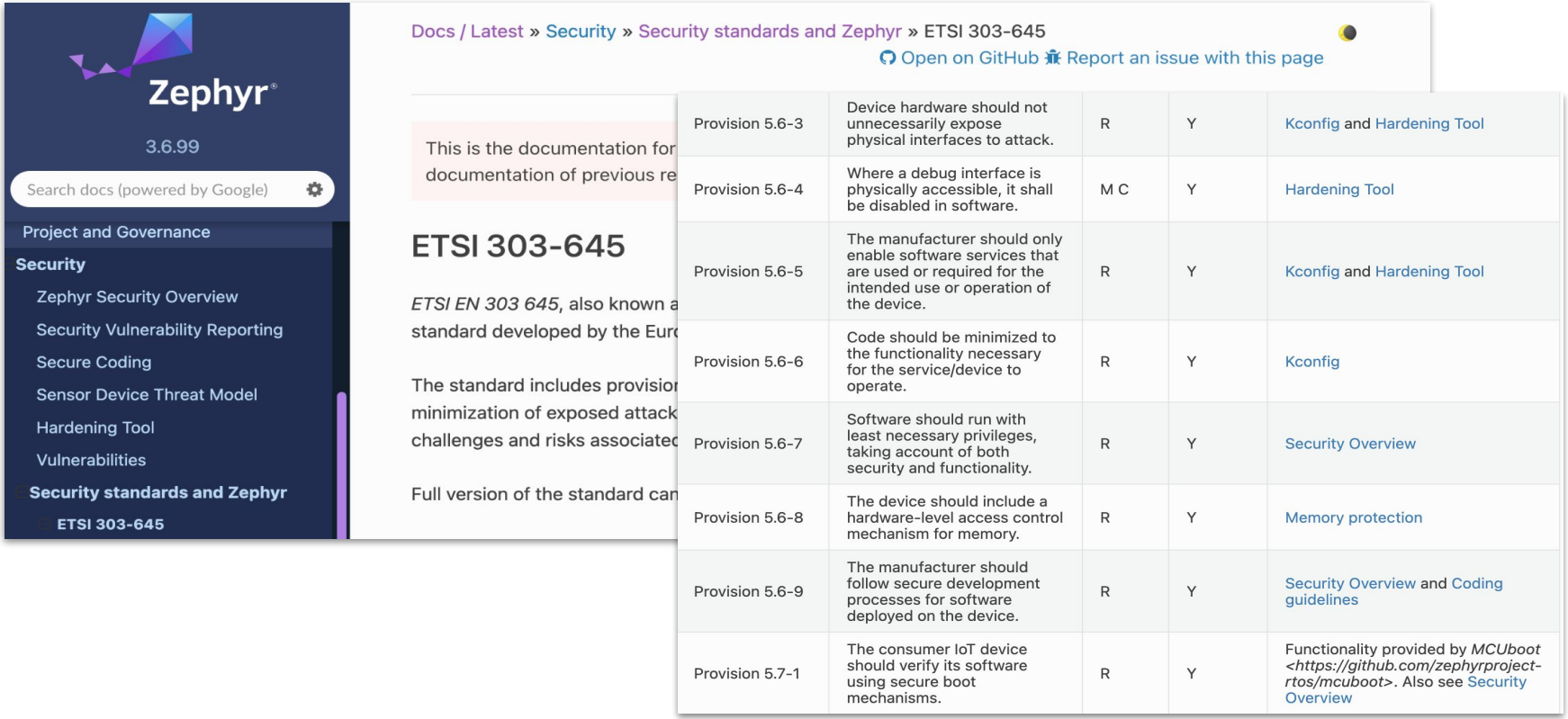
Security Committee

- **Restricted** to one representative from each platinum member, an architect (Flavio Ceolin), and a chair (David Brown)
- Meeting: Every 2 weeks
- Topics:
  - Vulnerabilities
  - PSIRT processes
  - Financial/contracts
  - Other sensitive information

Security Working Group

- **Open** to any participant
- Meeting: Every 2 weeks
- Topics:
  - Security Standards
    - ETSI EN 303-645
    - FIPS 140-3
    - SP 800-128
    - Annex K (C11 standard)
  - Evolving Security Processes
  - Code Analysis Tools
  - Documentation

Work on ETSI EN 303-645 in 2023



Provision 5.6-3	Device hardware should not unnecessarily expose physical interfaces to attack.	R	Y	Kconfig and Hardening Tool
Provision 5.6-4	Where a debug interface is physically accessible, it shall be disabled in software.	M C	Y	Hardening Tool
Provision 5.6-5	The manufacturer should only enable software services that are used or required for the intended use or operation of the device.	R	Y	Kconfig and Hardening Tool
Provision 5.6-6	Code should be minimized to the functionality necessary for the service/device to operate.	R	Y	Kconfig
Provision 5.6-7	Software should run with least necessary privileges, taking account of both security and functionality.	R	Y	Security Overview
Provision 5.6-8	The device should include a hardware-level access control mechanism for memory.	R	Y	Memory protection
Provision 5.6-9	The manufacturer should follow secure development processes for software deployed on the device.	R	Y	Security Overview and Coding guidelines
Provision 5.7-1	The consumer IoT device should verify its software using secure boot mechanisms.	R	Y	Functionality provided by *MCUboot <https://github.com/zephyrproject-rtos/mcuboot>*. Also see Security Overview

Source: https://docs.zephyrproject.org/latest/security/standards/etsi-303645.html#provisions-assessment

2024 Security Audit with NCC Group

Why External Audit?

- Identifying Vulnerabilities
- Independent Assessment
- Best Practices
- Community Trust
- Reputation

Scope Definition

- Security Objectives
- Components
  - Narrow to something doable and that benefits most users
- Depth of Analysis
- Threat Model

Results from NCCGroup

- Target Zephyr 3.6 / 3.7
  - 02/2024 ~ 03/2024
- Three issues found
  - Two low severity caused by integer overflow and TOCTOU
  - One informational caused by integer overflow

Lessons Learned from the Audit

Defining the scope is hard

- Resource Constraints
- Depth and Breadth
- Future-Proofing
- Stakeholder Agreement

Threat model is useful

- Guiding the Audit Process
- Validating Security Controls
- Facilitating Communication

Comprehensive testing importance

- The audit make it clear the importance of comprehensive testing

Outcomes:

- Enhanced Security
  - The identification and subsequent remediation of even low-severity issues contribute to a more secure system
- Increased Confidence
  - Third-party auditor validated the security and quality of the code base increasing confidence among developers, stakeholders, and users
- Recommendations aligned with Zephyr plans
  - Guided Fuzzing of Libraries and Subsystems

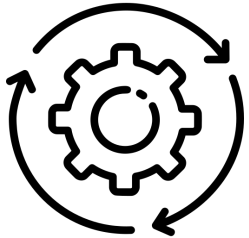
More Details Available...

Details at:
https://www.youtube.com/watch?v=vEG-Owv9TEs&list=PLzRQULb6-ipHnRUuy2UJpqZjTM9FPWtWx&index=22

2025 OS Steward Readiness for CRA

Article	Summary	Zephyr Status
Article 24.1	Security policy & vulnerability reporting process / link	☑ Documented in Project (policy & vulnerability reporting process).
Article 24.2	Cooperate with MSAs to reduce risk	☑ Working already with CVE Authorities as CNA.
Article 14.1	CSIRT Contact established	🕒 Identify CSIRT coordinator for EU
Article 14.3	Notify CSIRT & ENISA of "severe" vulnerabilities	🕒 Determine if processes used with NVD will work or if adjustments required.
Article 14.8	Notify end-consumers of "severe" vulnerabilities	☑ Provide information to manufacturers & integrators signed up on Zephyr Vulnerability Alert Registry
Article 52.3	Stewards found non-compliant must take corrective actions to respect obligations	☑ Doing this today with CVE authorities

Zephyr Security Summary



Weekly Coverity scans

MISRA scans

Automated Code checks per pull request

Documented secure coding practices

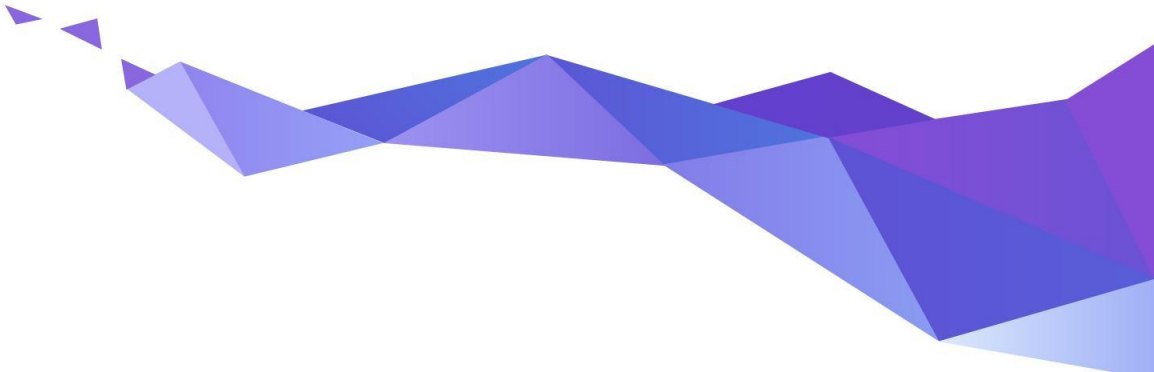
Vulnerability response criteria publicly documented

SBOM generation

per

ISO/IEC 5962:2021

Zephyr approach to safety



So what does Zephyr mean by Safety?

Safety – the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment

Zephyr will focus on "Functional Safety"

- the part of safety that depends on a system or equipment operating correctly in response to its inputs
- Detecting potentially dangerous conditions, resulting either in the activation of a protective or corrective device or mechanisms to prevent hazardous events or in providing mitigation measures to reduce the consequences of the hazardous event.

"depends on a system" ?

Systematic capability is the general assumption, that

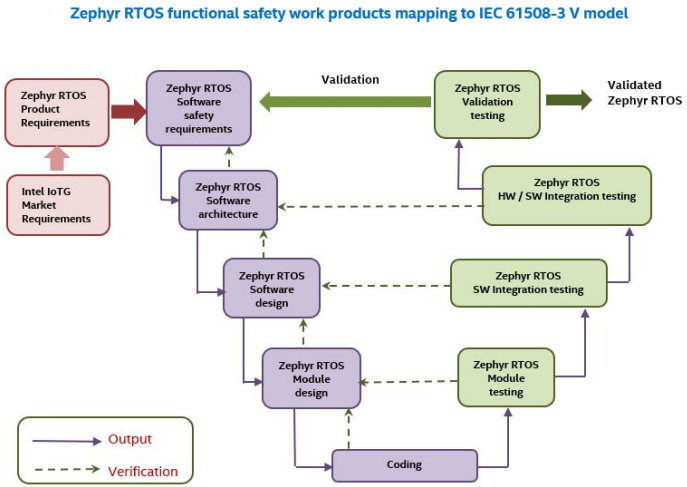
- if development, test and deployment of a system follow a specific set of tasks and
- there is evidence for adherence to these tasks
- (and under the assumption that the system architecture supports safety)

⇒ Software is capable of performing as intended

Compliant Development: V-model

It is difficult to map a stereotypical open-source development to the V-model

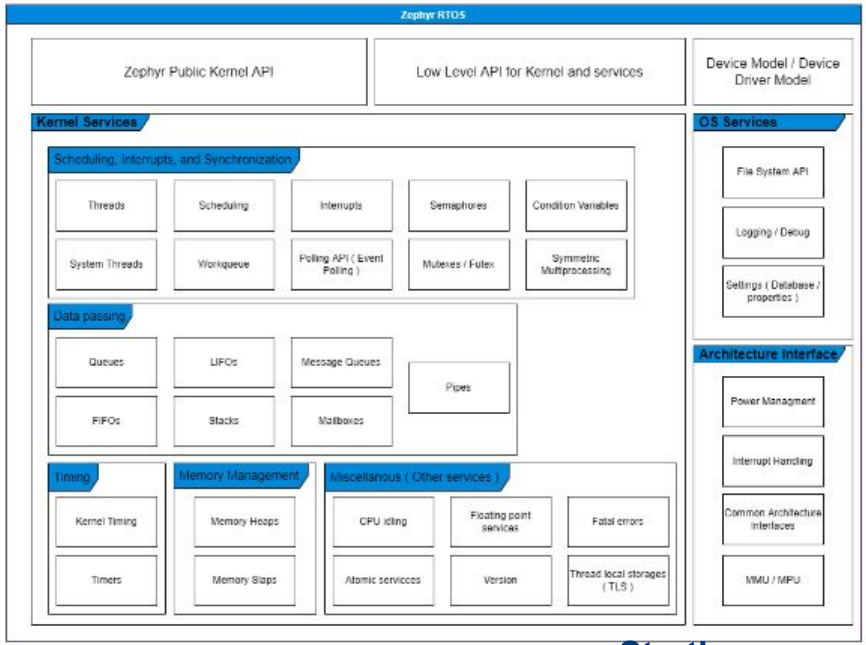
- Specification of features
- Comprehensive documentation
- Traceability from requirements to source code
- Number of committers and information known about them



⇒ Provide the evidences that open source developers can map to compliance and meet all requirements

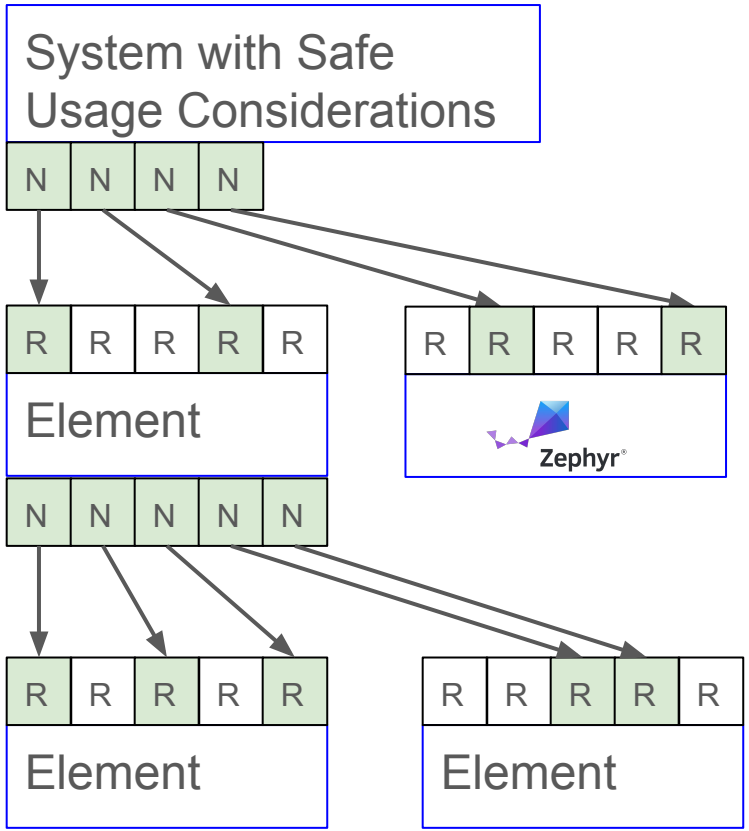
Zephyr Initial Certification Focus

- Start with a limited scope of kernel and interfaces
- Initial target is IEC 61508 SIL 3 / SC 3 (IEC 61508-3, 7.4.2.12, Route 3s)
- Option for 26262 certification has been included in contract with certification authority should there be sufficient member interest



Scope can be **extended** to include **additional components** with associated **requirements** and **traceability** as determined by the safety committee

Safety Element out of Context - SEooC



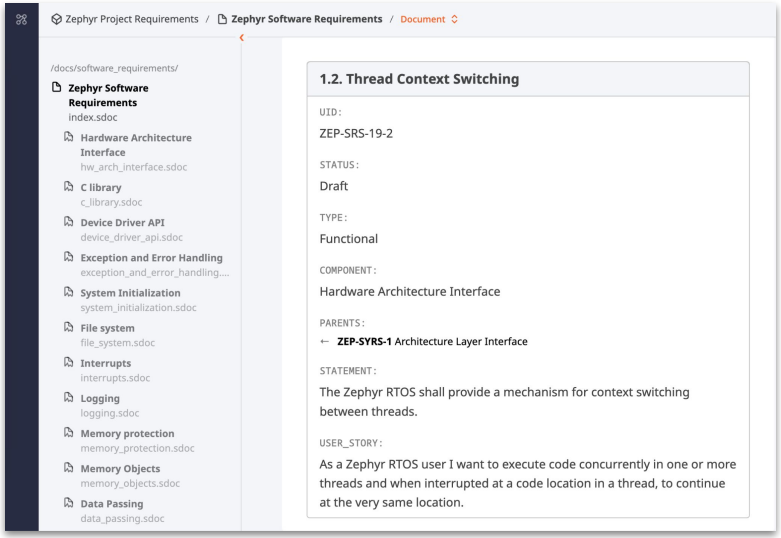
Development and verification independent of a specific context or application

Provides integration and operation information for safe system integration

Comes with sufficient evidence, that it can be integrated to a safety relevant system.

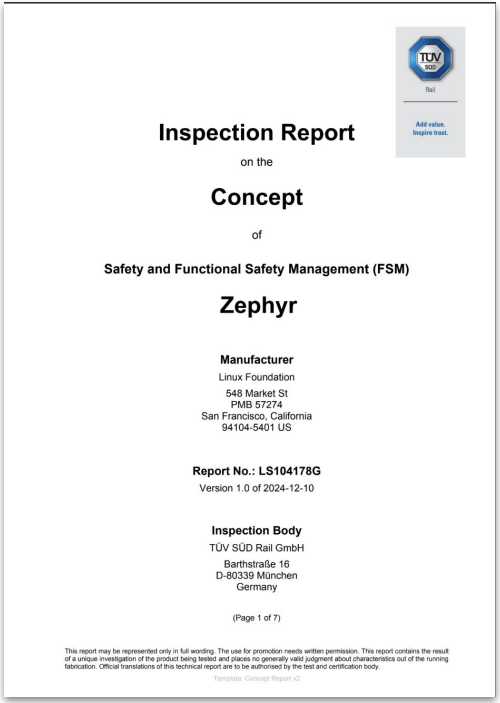
Status Today

- Coding Guidelines established based on MISRA rules and applied
- Static Analysis tooling to check for adherence to Guidelines selected for future contributions
- Reference Requirements and Traceability started in the code base. End to end example by FOSDEM.
- Automatic human readable documentation of requirements from StrictDoc rules is available



Status Today

- Coding Guidelines established based on MISRA rules and applied
- Static Analysis tooling to check for adherence to Guidelines selected for future contributions
- Reference Requirements and Traceability started in the code base
- Automatic human readable documentation of requirements from StrictDoc rules is available
- **Formal concept approval and Phase 1 is complete … on to Phase 2**



Inspection Report

on the

Concept

of

Safety and Functional Safety Management (FSM)

Zephyr

Manufacturer

Linux Foundation

548 Market St
PMB 57274
San Francisco, California
94104-5401 US

Report No.: LS104178G

Version 1.0 of 2024-12-10

Inspection Body

TÜV SÜD Rail GmbH

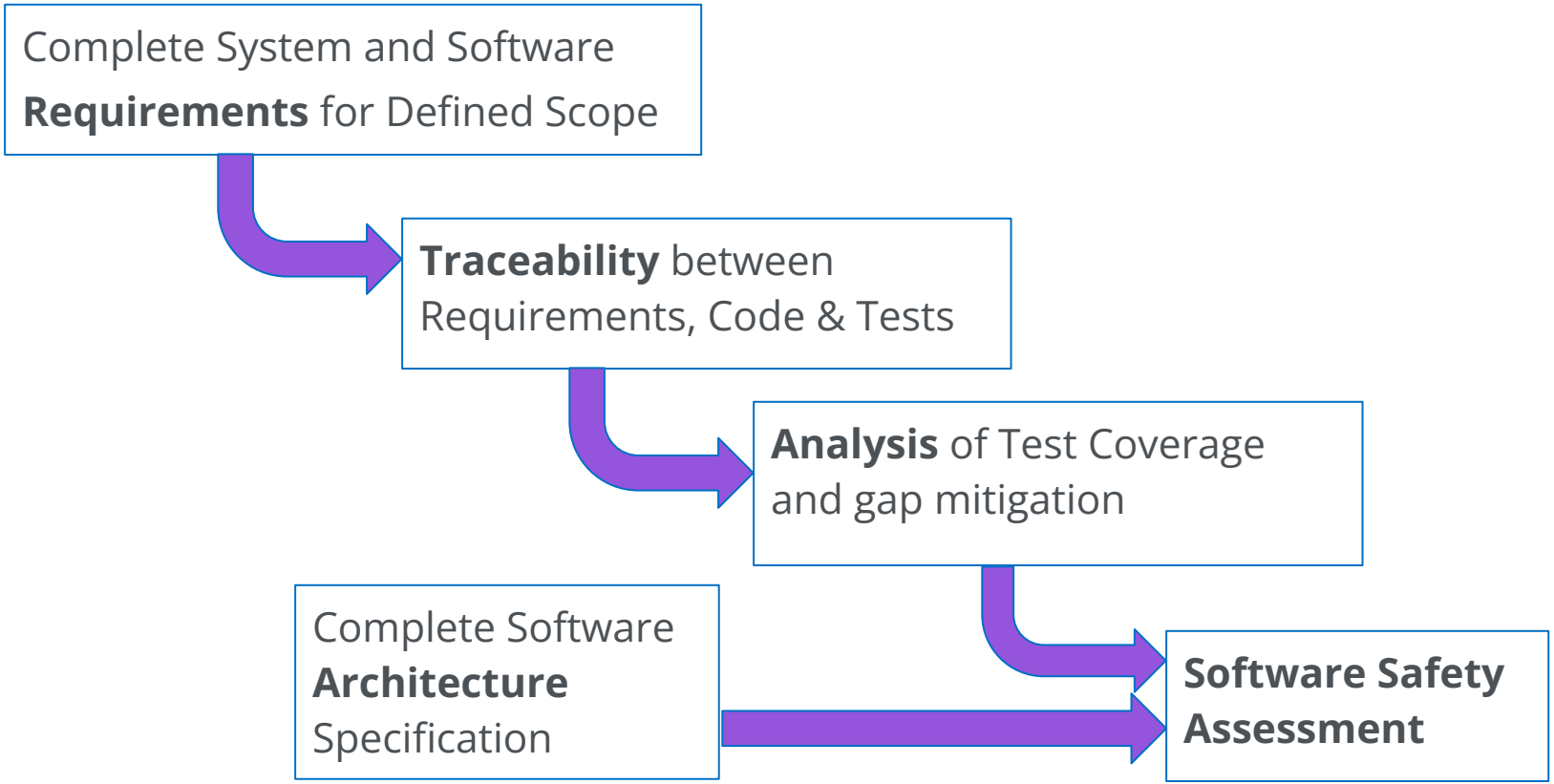
Barthstraße 16
D-80339 München
Germany

(Page 1 of 7)

This report may be represented only in full wording. The use for promotion needs written permission. This report contains the result of a unique investigation of the product being tested and places no generally valid judgment about characteristics out of the running fabrication. Official translations of this technical report are to be authorised by the test and certification body.

Template: Concept Report v2

Critical Path to Phase 2



Member & Community Participation

Safety Committee Role

- Safety Certification strategy decisions
  - Scope of certification
  - Certification standards
  - Certification timeline
- Assessment and audit specific tasks
- Owner of certification artefacts
- **Participation limited** to the project's platinum members, the safety architect, the safety chair, functional safety manager and project staff

Safety Working Group Role

- Creating/deriving and documenting the requirements for project code
- Establishing traceability between requirements, code and relevant tests
- Extending testing coverage as needed
- Setting up requirements management tooling
- Working on the creation of the required documentation and evidence
- **Open to everyone to participate**

Getting started – Important links

- Check out the official **Getting Started Guide**
- Dig into the hundreds of **code samples**
- Check the catalog of 100s of available Devicetree bindings
  - No driver for your HW? Chances are a similar driver already exists and writing one is not as hard or daunting as you would think!
- Reach out to the community on **Discord**

Zephyr Participation Information

zephyrproject.org

github.com/zephyrproject-rtos

lists.zephyrproject.org

chat.zephyrproject.org

Zephyr Project: Platinum Members

Zephyr Project: Silver Members

7/LAB
AC6
ALIF SEMICONDUCTOR
ARDUINO
arm
Baumer
Baylibre Zephyr Member
BENINGO EMBEDDED GROUP
((o)) Blecon
blues
JRLC 菁蓉联创
DOULOS
embedd
Embeint
ezurio
HONDA The Power of Dreams
hubble NETWORK
iar
infineon
inovex
linaro™
MICROCHIP
MICROEJ
oticon life-changing technology
percepio
Qt Group
RAYTAC
Savoir-faire LINUX
Schneider Electric
life.augmented
SYNOPSYS®
tenstorrent
Texas Instruments

Zephyr®

zephyrproject.org